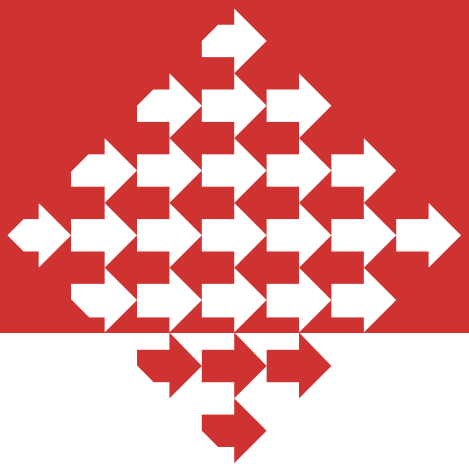


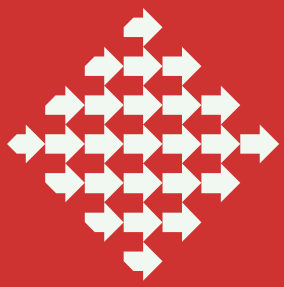
VITEL

Zbornik referatov

Triintrideseta
delavnica o telekomunikacijah

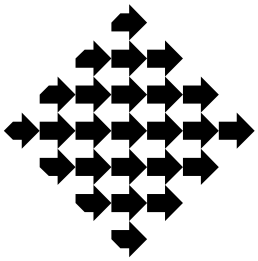
OMREŽJA 5G
ZA DIGITALNO PREOBRAZBO

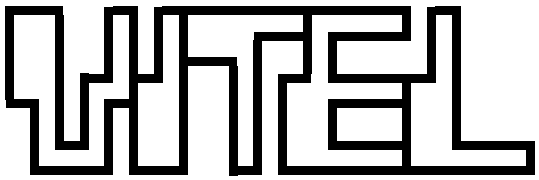
22. in 23. maja 2017 Brdo pri Kranju



Slovensko društvo za elektronske komunikacije
Elektrotehniška zveza Slovenije

SLOVENSKO DRUŠTVO ZA ELEKTRONSKE KOMUNIKACIJE
ELEKTROTEHNIŠKA ZVEZA SLOVENIJE





Triintrideseta delavnica o telekomunikacijah

OMREŽJA 5G
ZA DIGITALNO PREOBRAZBO

ZBORNIK REFERATOV

22. in 23. maja 2017 Brdo pri Kranju, Slovenija

33. delavnica o telekomunikacijah VITEL

ZBORNIK REFERATOV

33 Workshop on Telecommunications VITEL

PROCEEDINGS

Vsi referati v tem zborniku so recenzirani.
All papers in this proceedings have been peer reviewed.

Organizirata / *Organised by*:	Slovensko društvo za elektronske komunikacije
	Elektrotehniška zveza Slovenije
Pokrovitelj / *Sponsored by:*	IEEE Communications Society

Uredila / *Editors*:	Tomi Mlinar, Nikolaj Simič
Priprava za tisk / *Prepress:*	Tomi Mlinar, Nikolaj Simič
Naslovnica / *Cover design:*	Nikolaj Simič, Filip Samo Balan, Aleksander Vreže
Izdajatelj / *Publisher:*	Slovensko društvo za elektronske komunikacije
Tisk / *Printing house:*	DTP, d. o. o., 2017
Število izvodov / *Copies:*	100

ISSN 1581–6737

Programski in organizacijski odbor delavnice

Programme and Organizing Committee

Programski odbor delavnice

Programme Committee

Ana Robnik, predsednica
Alojz Hudobivnik
Ivica Kranjčevič
Tomi Mlinar
Nikolaj Simič
Boštjan Tavčar

Organizacijski odbor delavnice

Organizing Committee

Nikolaj Simič, predsednik
Ivica Kranjčevič
Tomi Mlinar

Zgodovina delavnic o telekomunikacijah VITEL

History of Workshops on Telecommunications VITEL

1993: 1. *ISDN omrežja in storitve v Sloveniji*, Brdo pri Kranju
1994: 2. *Mobilne in brezvrvične telekomunikacije*, Brdo pri Kranju
1995: 3. *Podatkovna omrežja in storitve v Sloveniji*, Brdo pri Kranju
1995: 4. *Načrtovanje, upravljanje in vzdrževanje komunikacijskih omrežij*, Brdo pri Kranju
1997: 5. *Varnost in zaščita v telekomunikacijskih omrežjih*, Brdo pri Kranju
1997: 6. *Zbliževanje fiksnih in mobilnih omrežij ter storitev*, Brdo pri Kranju
1998: 7. *Telekomunikacije in sprejetje Slovenije v Evropsko unijo*, Brdo pri Kranju
1999: 8. *Omrežja IP, internet, intranet, ekstranet*, Brdo pri Kranju
1999: 9. *Upravljanje omrežij in storitev*, Brdo pri Kranju
2000: 10. *Mobilnost v telekomunikacijah*, Brdo pri Kranju
2001: 11. *Dostop do telekomunikacijskih storitev*, Brdo pri Kranju
2002: 12. *Poslovne telekomunikacije*, Ljubljana
2002: 13. *Kakovost storitev*, Brdo pri Kranju
2003: 14. *Varnost v telekomunikacijskih sistemih*, Brdo pri Kranju
2003: 15. *Mobilni internet*, Brdo pri Kranju
2004: 16. *Pametne stavbe*, Brdo pri Kranju
2005: 17. *Telefonija IP (VoIP)*, Brdo pri Kranju
2005: 18. *Storitev trojček = Triple play*, Ljubljana
2007: 19. *Brezžični širokopasovni dostop*, Brdo pri Kranju
2007: 20. *Optična dostopovna omrežja*, Brdo pri Kranju
2008: 21. *Povsem IP–omrežja*, Brdo pri Kranju
2009: 22. *Širokopasovna mobilna omrežja*, Brdo pri Kranju
2009: 23. *Konvergenčne storitve v mobilnih in fiksnih omrežjih*, Brdo pri Kranju
2010: 24. *Prehod na IPv6*, Brdo pri Kranju
2011: 25. *Internet stvari*, Brdo pri Kranju
2011: 26. *Komunikacije in računalništvo v oblaku*, Brdo pri Kranju
2012: 27. *Telekomunikacije in zasebnost*, Brdo pri Kranju
2012: 28. *Pametna mesta*, Brdo pri Kranju
2013: 29. *Infrastruktura za izpolnitev digitalne agende in kaj po tem – primer Slovenije;* Brdo pri Kranju
2014: 30. *Omrežja prihodnosti,* Brdo pri Kranju
2015: 31. *Kritična infrastruktura in IKT,* Brdo pri Kranju
2016: 32. *Pametna omrežja informacijske družbe,* Brdo pri Kranju

Zgodovina mednarodnih simpozijev VITEL

History of International Telecommunication Symposium VITEL

1992: *VITEL*, Ljubljana
1994: *Subscriber Access*, Ljubljana
1996: *Broadband Communications Prospects and Applications*, Ljubljana
1998: *Mobility and Convergence Communication Technologies*, Ljubljana
2000: *Technologies and Communication Services for the Online Society*, Ljubljana
2002: *NGN and Beyond*, Portorož
2004: *Next Generation User*, Maribor
2006: *Content and Networking*, Ljubljana
2008: *DVB–T and MPEG4*, Bled
2010: *Digital Television Switchover Process*, Brdo pri Kranju

Uvodnik

Foreword

Področje komunikacij zadnjih trideset let vsako dekado doživlja tektonske premike v vrstah in načinih prikaza vsebine, nudenja storitev in povezovanja nasploh. Živimo v času informacijsko-komunikacijskih, računalniških in operativnih integracij v domačem okolju, na poti in na delovnem mestu. Z novimi in zlitimi tehnologijami, infrastrukturnimi rešitvami, inovativnimi storitvami in spremenjenimi poslovnimi modeli te integracije ponujajo številne nove priložnosti partnerskim ekosistemom v podaljšanih in prenovljenih verigah vrednosti.

Omrežja pete generacije – ali krajše omrežja 5G – so ključni in temeljni gradnik takih integracij in digitalne preobrazbe gospodarskih sektorjev, javnega sektorja in družbe kot celote. Omrežja 5G so del sistemov 5G, ki vključujejo tako naprave z vgrajeno inteligenco kot naslednjo stopnjo pametnih naprav kot tudi množice stvari za domačo in industrijsko rabo. Ti sistemi ponujajo vrsto aplikacij in storitev na zahtevo in v realnem času za spremenjeno in novo doživljanje sveta okrog nas in v nas s pomočjo umetne inteligence in strojnega učenja ter nov modus vivendi z močno izboljšano uporabniško izkušnjo.

Omrežja 5G so zasnovana na raznolikih primerih uporabe, ki dopolnjujejo komunikacijo med ljudmi s komunikacijo med napravami in stvarmi, jo obogatijo s širokopasovno video komunikacijo in vsebinami aplikacij ter ob tem zahtevajo odzivni čas 1 ms (Tactile Internet) in manj, v kombinaciji z odpornostjo na izredna stanja, zanesljivostjo, energetsko varčnostjo ter varnostjo in zasebnostjo. Naj omenimo le nekatere: samovozeča vozila z inteligentnim prometom in logistiko, zdravstvene storitve in oddaljeni medicinski procesi, virtualna, oplemenitena in razširjena resničnost, zagotavljanje varnosti ob različnih množičnih dogodkih, energetska oskrba. Iz omenjenih primerov uporabe so razvidna tudi varnostna razsežja in razsežja zasebnosti, ki postavljajo visoke zahteve za obe področji.

Omrežja 5G s svojimi bistveno izboljšanimi karakternimi lastnostmi, ki se merijo v mnogokratnikih izboljšav, združujejo končne naprave, fiksna, mobilna in brezžična dostopovna, prenosna in jedrna omrežja ter aplikacije orkestracije in upravljanja. Omrežja 5G niso več množica med seboj standardno in kompleksno povezljivih omrežnih elementov, ampak postajajo vse bolj programje inteligentno krmiljenih virtualnih omrežnih funkcij. Ponudnik omrežij 5G mora imeti torej dinamično porazdeljeno računsko, hrambeno in visoko razpoložljivostno zmogljivost na celotni poti, od dostopa do roba omrežja, preko prenosnega do jedrnega omrežja. Vse bolj se dozdeva, da se bo prva in največja sprememba dogajala prav na robu, kjer bo tudi največ prostora za inovativne storitve in zadovoljstvo uporabnikov ter na podlagi tega za ustvarjanje novih prihodkov. Prve implementacije omrežij 5G pa se na podlagi poročil predvidevajo v transportnem omrežju z integriranim zalednim in robnim sistemom z optimalnimi zaključitvami prometnih tokov.

Nova tehnološka gradnika sta programsko opredeljena omrežja na vsej poti in virtualizacija omrežnih funkcij (SDN/VNF), ki omogočata gibko arhitekturno shemo omrežij ter učinkovito dobavo in uporabo storitev. Omogočata gradnjo virtualnih omrežnih poti in rezin omrežij, ki jih lahko pojmujemo kot omrežja na zahtevo z zagotovljeno kakovostjo storitev in so gradnik v nudenju omrežij kot storitev. Na tem mestu še posebej omenimo naslednjo generacijo radijskih dostopovnih tehnologij, ki so povezana z virtualizacijo (C-RAN, elastični RAN, virtualiziran RAN).

Odprtost omrežnih funkcij preko aplikativnih programskih vmesnikov ter dinamično pridobivanje virtualnih in fizičnih virov centralizirane ali danes vse bolj porazdeljene oblačne infrastrukture omogočata optimalno izvajanje omrežnih funkcij glede na zahteve aplikacij in storitev. Z uporabo vgrajene inteligence za povezovanje vseh plasti omrežja in principov »self-« (self-configuration, self-optimization, self-healing, self-protection) za potrebe upravljanja, nadzora in orkestracije na podlagi rezultatov analitičnih orodij, dobimo v skoraj realnem času vedno bogatejše nabore informacijskih in operativnih storitev, kjer je človek vključen vse pogosteje le še kot kritičen opazovalec in pomemben odločevalec.

Ne glede na vse različne oblike in sloje nudenja virov pa imajo še vedno zadnjo besedo fizične omejitve. Radiofrekvenčni spekter je izjemno pomemben omejen naravni vir, zato je z njim potrebno delati zelo tenkočutno, da bodo frekvence na voljo za tako obsežno področje delovanja. Njegovo namembnost in uporabo bodo določili na svetovni radijski konferenci (WRC) leta 2019. Pričakujemo, da bodo regulativni organi izpeljali dodeljevanje frekvenc preko avkcij, kar se že dogaja po svetu. Pomanjkanje sodelovanja pri določanju licenčnega spektra za 4G je lahko dober razlog za izboljšanje v omrežjih 5G.

Ker postaja omrežje vse bolj programje in vse manj strojna oprema, na tem področju izjemno intenzivno delajo v okviru odprtokodnih skupnosti. Posamezna podjetja usmerjajo svoj raziskovalno-razvojni potencial v segmente, kjer so najboljši, razvoj tehnoloških gradnikov pa prepuščajo tem skupnostim. Pomembna je tudi prihajajoča standardizacija omrežij 5G ter združljivost standardov pod okriljem različnih standardizacijskih organizacij in stanovskih združenj (ITU-R, ITU-T, ETSI,

IEEE, IETF, ONF, ...) ter sodelovanje odprtokodnih skupnosti z njimi. Zahteve in koncepti za omrežja 5G so že po večini znani, prvi standardi 5G pa bodo na voljo leta 2018.

Omrežja 5G kot nova razvojna in poslovna priložnost so izjemnega pomena tudi za Slovenijo. Strategija Komisije za enotni digitalni trg, ki vključuje tudi Akcijski načrt za 5G v Evropi (COM(2016)588), poudarja pomen uvedbe zelo visoko zmogljivih omrežij 5G v vsaki državi, saj so ključna za evropsko konkurenčnost na globalnem trgu. Investicije v omrežja 5G ne bodo majhne, stroški vzdrževanja pa bodo odvisni od posameznih postavitev in migracijskih scenarijev. Omrežja 5G lahko namreč delujejo v sozvočju z omrežji 4G ali pa so povsem samostojna, vmesniki za medsebojno povezovanje so prav tako v fazi standardizacije. Prav zaradi velikih stroškov pri gradnji omrežij 5G in kompleksnih postavitev zaradi raznorodne uporabe morajo biti jasni potenciali za znatno povpraševanje in regulativni pogoji, ki omogočijo, da se ta naložba izplača. Industrijski sektorji, ki jih zanima uporaba omrežij 5G za postopek njihove digitalizacije, bodo morda tudi želeli počakati, dokler ne bodo omrežja 5G preskušena in pripravljena. S tem namenom se ponudniki komunikacijskih storitev 5G povezujejo z industrijskimi sektorji ali sami postajajo vse bolj ponudniki digitalnih storitev zasebnim, poslovnim in industrijskim uporabnikom.

Za omrežja 5G z vso strokovno utemeljenostjo lahko trdimo, da so ključni element za digitalno preobrazbo industrije in družbe. Digitalizacija evropske industrije se že začenja danes na podlagi razpoložljivih virov (zlasti 4G/LTE, Wi-Fi ali satelita), še dodatno pa jo bo pospešilo postopno uvajanje 5G od leta 2018 dalje. Zato so še kako pomembne pilotske postavitve in preskušanja omrežij 5G, ki jih bomo izvedli tudi v Sloveniji v tem in prihodnjih letih. Leto 2020 pa je leto napovedanih prvih resnih komercialnih postavitev.

Uporaba omrežij 5G in z njimi povezana digitalna preobrazba bo imela v prihodnjem desetletju izrazit vpliv tudi na socialne modele življenja in zaposlovanja. Nekateri strokovnjaki opozarjajo, da bo ta preobrazba prinesla tudi negativne posledice prav na področjih (samo)zaposlovanja, kar bo še povečevalo razkorak v razvitosti posameznih delov družbe in regij ter tako potencialno še poglobilo razliko v e-vključenosti ranljivih skupin prebivalstva. Zato je uspeh zelo odvisen od vsakega posameznika in od naše pripravljenosti na soočenje z novo stvarnostjo.

Zahvaljujem se avtorjem za vse članke v zborniku, ki s strokovnega gledišča osvetljujejo različne zgoraj omenjene vidike omrežij 5G in njihovo uporabno vrednost. Želim, da bralci v njih najdete dovolj uporabnih informacij in prepotrebnih znanj s tega področja za vaše uspešno in učinkovito delo ter strokovno pomoč pri vaših morebitnih strateških odločitvah s tega področja.

Brdo pri Kranju, 22. maja 2017

mag. Ana Robnik,
vodja programskega odbora

Kazalo prispevkov

Table of contents

22. 5. 2017

23. 5. 2017

Towards 5G Software-Defined Ecosystems

Antonio Manzalini, Telecom Italia Mobile, Italy
Alojz Hudobivnik, AH.TS, Slovenia

Abstract — Techno-economic drivers are creating the conditions for a radical change of paradigm in the design and operation of future telecommunications infrastructures. In fact, SDN, NFV, Cloud and Edge-Fog Computing are converging together into a single systemic transformation termed "Softwarization" that will find concrete exploitations in 5G systems. The IEEE SDN Initiative has elaborated a vision, an evolutionary path and some techno-economic scenarios of this transformation: specifically, the major technical challenges, business sustainability and policy issues have been investigated. This paper presents: an overview on the main techno-economic drivers steering the "Softwarization" of telecommunications, an introduction to the Open Mobile Edge Cloud vision, the main technical challenges in terms of operations, security and policy, an analysis of the potential role of open source software, some use case proposals for proof-of-concepts, and a short description of the main socio-economic impacts being produced by "Softwarization".

Keywords — SDN, NFV, 5G, Open Mobile Edge Cloud

Povzetek —Tehnološki in ekonomski faktorji ustvarjajo pogoje za korenito spremembo paradigme o zasnovi in delovanju prihodnjih telekomunikacijskih infrastruktur. Dejstvo je, da se SDN, NFV, oblakovno (ang. Cloud) in megleno računalništvo na robu (ang. Edge-Fog Computing) zbližujejo in predstavljajo sistemsko preobrazbo imenovano programanje (ang. Softwarization), ki se bo uporabljala v sistemih 5G. Pobuda IEEE SDN je izdelala vizijo, evolucijske poti in podala nekaj tehnološko-ekonomskih scenarijev te preobrazbe. Izpostavljeni so bili glavni tehnični izzivi, trajnostna poslovna naravnanost in politike. Ta članek podaja: pregled glavnih tehnoloških in ekonomskih faktorjev telekomunikacijskega programanja, uvod v vizijo o odprtem oblaku na mobilnem robu (ang. Open Mobile Edge Cloud), glavne tehnične izzive na področju operacij, varnosti in politike, analizo potencialne vloge odprtokodne programske opreme, nekaj primerov uporabe za potrditev koncepta izvedbe in kratek opis glavnih družbeno-ekonomskih učinkov, ki jih prinaša programanje. Naj navedeva, da pobuda IEEE SDN razvija tudi odprt katalog programskih platform, orodij in funkcionalnosti s ciljem postopnega razvoja in združevanje testnih/pilotskih preskusov na področju SDN-NFV-5G. To bo osnova za razvoj novih ekosistemov IKT, s čimer se bo izboljšala kakovost življenja in spodbujal razvoj novega digitalnega gospodarstva.

Ključne besede — SDN, NFV, 5G, Softwarization

I. INTRODUCTION

A number of techno-economic drivers are converging to create the conditions for a paradigm change in the design and operations of future telecommunications networks and services. These drivers include progress in Information Technologies (IT), pervasive diffusion of ultra-broadband (fixed and radio) access, the falling costs of hardware, the maturity of virtualization techniques, a wider and wider availability of open source software and, eventually, ever more powerful terminals.

Software-Defined Networks (SDNs) [1], Network Function Virtualization (NFV) [2], Cloud [13] and Edge-Fog computing [12] can be seen as different dimensions of an overall trend that has been named by the IEEE SDN Initiative as the "Softwarization" of telecommunications (Figure 1).

"Softwarization" is an overall techno-economic transformation impacting the design, implementation, deployment and operations of infrastructures, deeply integrating network nodes and IT systems. It fully exploits the nature of software, such as flexibility and rapidity, for both network functions and services. This transformation will enable new architectural models, in turn implementing automated operation processes (e.g., self-management) while opening innovative Information and Communications Technology (ICT) service paradigms 0.

It is very likely that this transformation will find first concrete expression in the 5G (Fifth Generation) of network and services infrastructure, which will be much more than a direct evolution of current LTE-4G networks. It is expected that 5G will handle 1000 times the current wireless area capacity, radically reduce the average service provisioning time, and meet significantly more stringent performance targets for reliability (packet error probability) and latency.

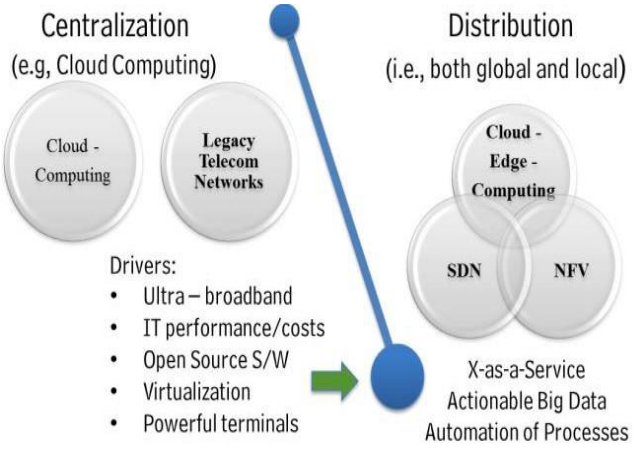


Figure 1: Softwarization of Telecommunications

The 5G infrastructure will also enable a wide variety of new applications and ICT services. In fact, the huge amount of data collected by sensors – embedded in all sorts of terminals, machines, and things – will be networked with low latency fixed-radio connections, elaborated in the Cloud and Edge- Fog Computing facilities, to eventually be actioned into a variety of ICT services.

This enormous amount of data will create new service scenarios such as the Internet of Things, Tactile Internet, Immersive Communications, and, in general, X-as-a-Service. For example, 5G will enable remote the radio control and programmability (via Application Program Interfaces) of advanced robotic systems, with various applications for both

industry (e.g., Industry 4.0) and agriculture (e.g., Precision Agriculture).

5G systems will therefore assume the characteristics of a powerful networking-computing-storage infrastructure. Its functions will be partly distributed and partly centralized, supporting pervasive connections (both wired and mobile) characterized by both high capacity and very low latency (of only a few milliseconds).

This techno-economic transformation of telecommunications is currently under the spotlight, not only in academic research communities but also in several industrial initiatives. This is clearly evident in forums and bodies like ONF, IETF, ITU-T, and ETSI that are developing reference architectures for SDN, NFV, Cloud and Edge-Fog Computing. At the same time, there is still a fragmentation in these efforts, which is delaying, if not jeopardizing, an effective exploitation of this techno-economic transformation worldwide. The IEEE SDN Initiative[1], established in 2013 by the IEEE Future Directions Committee, is a cross-society IEEE program with the goal of contributing to overcoming such fragmentation by proposing a leading effort and vision for Softwarization which includes not only technological aspects but also business sustainability and policy issues.

In 2016 IEEE SDN Initiative published white paper with the following topics:

- An overview of the main techno- economic drivers steering the "Softwarization" of telecommunications;
- An introduction to the Open Mobile Edge Cloud vision;
- The main technical challenges concerning operations, security and policy;
- An analysis of the potential role of open source software;
- Some use case proposals for proof-of-concepts; and
- A short description of the main socio-economic impacts being produced by "Softwarization".

II. TOWARDS THE 5G ERA

A. C-RAN: Softwarization of the RAN

The Radio Access Network (RAN) is the most important asset for operators: base stations outnumber the nodes in the core networks and are closer to and directly perceived by end users. The significance of softwarization on the RAN is self-evident.

As an essential element for 5G systems, the centralized, collaborative, cloud and clean RAN (C-RAN) [3] was proposed as early as 2010.

A C-RAN system centralizes different processing resources together to form a cloud in which the resources could be managed and dynamically allocated on demand. With virtualization implemented, standard IT servers are used as the general platform with computation and storage as the common resources, on which run different kinds of applications. The indispensable applications in C-RAN are those to realize different radio access technologies including 2G, 3G, 4G and future 5G. In addition, the C-RAN platform could provide a set of standard APIs opening the opportunity for new service provision and deployment.

In the era of 5G, C-RAN itself needs to evolve to accommodate new features, new use cases and new requirements to better support 5G. On the way towards C-RAN softwarization in 5G, there exist several challenges.

First, the C-RAN architecture itself needs to evolve. Although C-RAN embodied the softwarization spirit from the very beginning, it used to be thought more as a means of network implementation (e.g., using Commercial-Off-The-Shelf (COTS) platforms rather than proprietary platforms). It does not change the network architecture of 2G, 3G and 4G defined in 3GPP. However, for 5G with many more requirements such as ultra-low latency, network slicing, and extreme flexibility, the design of the 5G architecture requires co-design of the C-RAN architecture to support such features. Examples include how to support control/user plane separation, and how to incorporate SDN controller and multi-RAT controller.

The fronthaul issue comes next. A fronthaul (FH) link is typically a connection between the baseband unit (BBU) and a remote radio head (RRH). As traditional FH protocols such as Common Public Radio Interface (CPRI) [4] process any shortcomings as constant high data rate without taking account of dynamic wireless traffic, low transmission efficiency, poor scalability, etc., there are increasing concerns that they are not suitable for large-scale C-RAN deployment in 5G networks, especially when massive multiple-input multiple-output (MIMO) is introduced. Several schemes have been proposed to either improve CPRI itself or even redefine the fronthaul interface. One such scheme is the Next Generation Fronthaul Interface (NGFI) concept proposed by China Mobile [5][6]. The essence of NGFI is to redesign the fronthaul interface to make the FH data stream traffic-dependent (therefore dynamic) and antenna-independent. Based on this the underlined transport networks could be designed more efficiently. The key ways towards NGFI include redesign of the BBU-RRH function split and packetization of FH data. By decoupling the FH bandwidth from the antenna number, NGFI can better support large antenna technologies. In addition, the cell-processing functions should be decoupled from the UE- processing functions to make NGFI traffic-aware, which can exploit the statistical multiplexing gain to improve efficiency and further reduce power consumption. It is also suggested that the function split schemes for downlink and uplink could be different to improve flexibility and efficiency. The use of Ethernet for NGFI transmission brings the benefits of improved reliability and flexibility due to the packet-switching nature of Ethernet. In the meantime, jitter, latency and accurate timing distribution mechanisms remain the key difficulties to overcome to realize NGFI transportation.

Virtualization implementation to realize resource cloudification is another challenge. Due to the characteristics of intensive computation and extremely strict real-time requirements on wireless communications, especially on the physical layer process, implementing virtualization technology to realize radio access technologies such as LTE is not an easy task, not to mention the future 5G new radio technologies. Fortunately there has been extensive pioneering work on this front. For example, China Mobile has successfully demonstrated a virtual machine-based LTE implementation running on COTS platforms in field trials. Despite the demonstrated functionality and desirable performance, there is still much room for improvement,

[1] Manzalini, A., et all, IEEE SDN Initiative SDN4FNS white paper "Software- Defined Networks for Future Networks and Services – Main Technical Challenges and Business Implications", January 2014, http://sdn.ieee.org/publications

including further enhancement of real-time performance, seamless live migration for the sake of energy saving, and standardizing the interface. In addition to the virtual machine-based virtualization technology, there are many other new promising technologies such as container which are also worth further investigation.

Software architecture is another important aspect for C-RAN softwarization in 5G. Traditional wireless network design follows "cell-centric" principles, i.e., resource allocation, mobility management, cell planning and optimization, etc. are on a cell basis. In 5G, there is a paradigm shift from cell- centric towards "user-centric". The user-centric design depends on several key technologies including data/control plane separation, UL/DL decoupling and C-RAN is deemed to facilitate the realization of user-centric networks [7].

However, in traditional base stations, the system software architecture is designed based on traditional vendors' proprietary platforms consisting of Digital Signal Processing (DSP), Application Specific Integrated Circuits (ASICs), etc. to meet the cell-centric purpose. In C-RAN in 5G, the systems would operate based on COTS platforms consisting of standardized IT servers, switches, and storage. All the resources are in the cloud and allocated on demand according to user needs. Thanks to the difference between the COTS platforms and traditional DSP-constituted platforms, and more importantly, due to the difference in the design principles from cell-centric to user-centric, the whole software system architecture in C-RAN needs to be reconsidered to exploit the cloud computing features and capabilities of COTS platforms as much as possible. The idea could be strengthened as far as the 5G requirements such as high agility, flexibility and scalability are concerned. In addition, network slicing, which is one of the key features of network softwarization, requires the cloud resources be reconfigured in a fast, agile, dynamic and cost-effective way. This also imposes requirements on careful software architecture design. In this sense, software architecture redesign is a critical issue for future study.

Last but not least, the introduction of SDN in C-RAN should not be neglected. Traditionally the concept of SDN mainly applies in the transport/routing area with the basic idea of control/data plane decoupling to realize the programmability of the control plane. With FH transport networks, in particular when NGFI is introduced, it is natural to extend the SDN concept to C-RAN. There should be an SDN controller located in the C-RAN cloud, deciding on the optimal FH routing path. This work could be coordinated with the management system or orchestrator in the cloud. The system architecture, the interface, the data flow and the coordination among the SDN controller and other control units are all worth further study.

In summary, as the essential element of 5G, the concept of C-RAN is firmly in line with the essence of "Softwarization" of telecommunications. On the one hand, C-RAN claims benefits such as facilitation of signal joint processing, deployment of mobile edge computing, multi-RAT coordination, and user-centric network realization. On the other hand, to achieve these benefits requires careful and optimal design of C-RAN from various aspects, including the architecture, FH transportation, virtualization technologies, software architecture redesign, SDN, management, and orchestration.

B. An end-to-end vision for 5G

5G era is aiming at an End-to-End (E2E) vision that includes the evolution of the RAN, the Next Generation (NG) core, and a management/control plane that extends User Equipment (UE) to the core and beyond.

As mentioned 5G is much more than an air interface beyond current LTE-4G. 5G will include evolutionary components of current generations of mobile networks (under a unifying umbrella). It also includes revolutionary components that will enable energy and spectral efficiency, a new resilient framework (i.e., responsive, auto-manageable QoS/QoE, secure, survivable, traffic and disruption tolerant) for services to everyone and everything (applications and machines).

5G requires a complete revamping of the E2E architecture, new service capabilities, rethinking of interfaces, management and control frameworks, access and non-access protocols and related procedures, functions, and advanced algorithms (e.g., Authentication, Authorization and Accounting (AAA), auto- maintenance and management of services) and any resource types (both physical and virtual).

Several challenges are still in the process of being addressed to meet stringent performance targets set out by the 5G community. These include 1000 times higher mobile data volume per area, 10 times to 100 times higher typical user data rate, 10 times to 100 times greater number of connected devices, 10 times longer battery life for low power devices, and five times reduced E2E latency. Moreover, the infrastructure needs to be highly flexible and scalable thus meeting foreseen and unknown requirements. Resiliency and responsiveness must be built into the design. Complexity is a big issue that needs to be measured and evaluated as part of this comprehensive redesign.

Service Providers (SPs) and network operators are currently deploying transformative approaches to provide network functions in appropriate infrastructures (using both centralized and distributed flexible architectural concepts) and thus providing flexible and scalable capabilities according to required use cases and their traffic demands. This flexibility will be achieved using a software-defined ecosystem and NFV technologies as well as data path programmability. The target architecture has to be cost and resource efficient as well as auto-managed and flexible for new innovations.

Significant adoption of Cloud Edge-Fog computing, SDN, NFV demands new thinking in various key areas to be able to fully utilize and monetize the capabilities presented: e.g., distributed system architecture, provide minimum "state" information, elastic and scalable systems in a consistent way, loose coupling and necessary event handling. Auto- management and control of mobile networks using new and innovative paradigms will be crucial.

IEEE SDN argues that any aspects require new and innovative work. These include context management (e.g., related to service, network, and device information); a Control, Orchestration, Management and Policy (COMP)[2]

[2] COMP: many SPs have example implementations of Control, Orchestration, Management and Policy frameworks that are part of a larger ecosystem that specifies standardized abstractions and interfaces that enable efficient interoperation of the ecosystem components. They are collections of software components which collectively are responsible for the efficient control, operation and management of capabilities and functions.

details related to eRAN; spectrum management; E2E resilient service composition; mobility management; low power-long range and various Machine-Type Communications (MTC); Device- to-Device (D2D) services; Radio Resource Management (RRM); and modular radio interfaces and a new protocol independent layering. Similarly, a new set of devices would also have modular capabilities developed around context, interference and Radio Access Technology (RAT) management, since end devices would be an integral part of RAN.

Most of the research and innovation efforts need to be in place in the next few years so that large field trials and testing can occur for early deployments to happen in 2020. This can be realized only through global collaboration and investment in key technologies and related fields. Since the required set of capabilities is very broad, mobile and wireline ecosystems need to be established that will allow global participation through open frameworks.

C. Open Mobile Edge Cloud

Various efforts are in progress in the RAN and core areas to address the architectural principles outlined above. In the RAN space, one of the promising architectures was identified as Cloud RAN (C-RAN, various flavours) as it provides a transition path to the cloud computing-based architecture. C-RAN architectures have been in trials in various countries and research labs for the past few years to determine the major benefits, challenges and solutions. The major challenges are fronthaul requirements (e.g., delay, jitter, cost, technology) and the ability of centralized baseband units (BBUs) to provide adequate signal processing in performance targets which basically determine the required spectral and energy efficiencies.

Several variants of C-RAN are proposed to address the fronthaul restrictions; one of the promising architectural directions is to decouple user and control planes and progress using the SDN strategy. This also allows a major rethink of the mobility edge (and subsequently the converged wireline/wireless edge). In this framework, a deconstruction of basic functions of RAN and core networks is followed by the definition of new architectural elements using the deconstructed functions.

IEEE SDN argues that one key area of this exercise is the introduction of a new functional node as an intersection point of these functions in order to create a future proof architecture.

This functional node, called Open Mobile Edge Cloud (OMEC) node, will be deployed to provide seamless coverage and execute various control plane functions as well as some of the "core functions" currently placed in various nodes of the Evolved Packet Core (EPC). More functionality related to compute and storage will be added to enable true cloud capabilities in closer proximities. Since many location-based applications are on the rise (social, analytics, video, etc.) fronthaul load will be considerably higher in the future. Requirements on local storage, compute and networking processing of "edge" services almost forces a new architectural direction.

ETSI's Mobile-Edge Computing (MEC) Industry Specification Group[3] and "Fog computing[4]" are efforts in this direction; trying to address similar issues and identifying that a substantial amount of storage, communication, control, configuration, measurement and management should be placed at the "edge" of a network, in addition to the current cloud paradigms. This idea is based on the premise of certain extensions of Cloud computing architectures to the network edge, up to the Users' equipment/terminals.

Figure 2 shows an example of functional decomposition of NG UE, RAN and core functions for an E2E architecture of mobile networks in the 5G era. All these are related approaches but much more needs to be done.

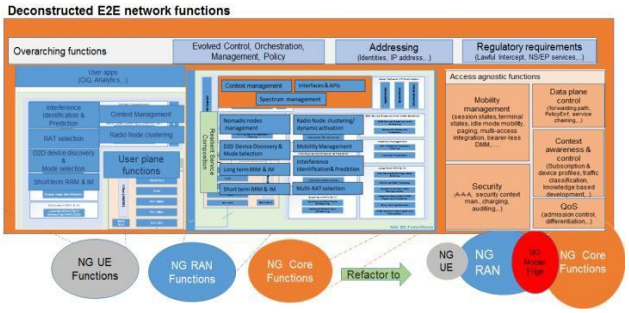


Figure 2: The Functional Decomposition of NG UE, RAN, Core and End-to-End Functions

The deconstruction of functions is a prelude to reconstruction and optimal placement of functionalities, much more than networking, to refactored nodes to address all the considerations outlined above. It is envisioned that NG Mobile edge (subsequently converged edge) will be the center of all 5G era networks with compute and storage functionalities attached. OMEC is an architectural paradigm based on this framework.

There are multiple variants of this key idea that essentially pushes some applications, analytics and computing, content and storage to the edge (including the edge devices). What is being done in the networking space should converge with similar ideas in the compute and storage dimensions. To include the UEs and other Customer Premise Equipment's (CPEs) in this methodology requires many new collaboration capabilities to be developed to execute traditional RAN functions (e.g., RRM) along with others such as mobility management and security in this architectural framework as well as content delivery, storage and compute functionalities.

Given the vision outlined above, and the strategic role it would play as an intersection of NG Core and RAN functions, the edge needs to be properly defined. In the IEEE SDN workshop that took place in November 2015[5] on OMEC, it was defined as:

An open cloud platform that uses some end-user clients and located at the "mobile edge" to carry out a substantial amount of storage (rather than stored primarily in cloud data centers) and computation (including edge analytics, rather than relying on cloud data centers) in real-time, communication (rather than routed over backbone networks), and control, policy and management (rather than controlled primarily by network gateways such as those in the LTE core).

[3] http://www.etsi.org/technologies-clusters/technologies/mobile-edge-computing

[4] http://www.openfogconsortium.org/

[5] http://sdn.ieee.org/pre-industrial

Note that this definition substantially re-architects the whole network. Key components are an application delivery framework on a cloud-based system with key functionalities refactored from NG RAN and Core.

The broad set of use cases outlined in various research and standards bodies points to a new set of applications that are limited by human physiology and psychology[6].

What differentiates the 5G era networks is the ability to address varying degrees of requirements (in delay, throughput, types and quantities of devices, etc.) concurrently with a unified framework. This almost dictates a new architectural component that is in close proximity to end users/devices with at most 10km distance to provide the new control and steering applications brought by new use cases.

These requirements are already very well known within the industry and there are approaches within the 5G community to address them.

All architectural work should be based on a set of Non-Functional Requirements (NFRs) on technology, business, and quality. These are the high level requirements and constraints that determine the evolution direction. Then the architecture[7] becomes the functional implementation of these requirements based on these constraints.

A key question that needs to be answered for the OMEC architecture is to determine how to merge various activities at the edge on a common platform based on the NFR constraints.

III. Security, Policy and Regulatory Issues

SDN and NFV have much to learn from existing security best practices in enterprise and the cloud, but there are specific challenges that arise with large-scale "softwarization" projects, particularly in the telecommunications industry.

Rather than attempt an exhaustive survey of the issues that arise, three specific areas are examined to give an overview of some of the key issues facing service providers: "Planning, Policy and Regulation", "Infrastructure" and "Operations".

A. Planning, Policy and Regulation

In a traditional, non-virtualized environment, the domains of control of various entities are generally fairly clear: network administrators manage the network, systems administrators manage the hardware systems, OS stacks and patching, storage administrators manage the storage, and so on. With the advent of widespread virtualization of all the various components of the data center, the separation between different components becomes less clear. However, the importance of maintaining appropriate authorities and responsibilities does not diminish, even if the sets of components managed by different administrators changes. It is a key security requirement that trust domains are defined between, for instance, the various components – virtual machines, containers or non-virtualized hardware – of a Virtual Network Function (VNF), and that the administrators of this trust domain are not confused with – nor have control over – separate trust domains such as the hardware and software infrastructure on which the virtualized components execute.

It is not only virtual network functions which are being virtualized, of course: service providers are also enjoying the benefits of the softwarization of Management and Orchestration (MANO) components. Trust domains need to be considered not only for the MANO components, but also for the infrastructure – physical and virtual – that underpins them. SDN controllers fall firmly within this category, as compromise of an SDN controller may mean loss of control of significant portions of a service provider's network.

The complexity of managing the network at various different layers opens another issue: that of network topology. Network topologies should be an expression of operational – and security – policy, but in a world where routing rules can change on a second-by-second basis, there are three specific challenges:

1. The creation of a resilient policy;
2. The mapping and application of the policy to real hardware and software;
3. The visualization and enforcement of the policy, typically through visualization and enforcement tools.

In fact, once any trust domain has been defined, establishing and maintaining it will require use of a variety of monitoring and enforcement tools, including attestation, Intrusion Defense Systems (IDS) and Network Domain Security (NDS), and careful management of software (including vendor-provided image) provenance and integrity. Definition – and the mapping and enforcement – of these trust domains is not simple, and is further complicated by the need for some trust domains which span others. Security monitoring, management and application of policy, for instance, will need to cross multiple trust domains. Added to this complication is the fact that some will span geographical boundaries. This includes components which reside outside the data center, in the case of vCPE and base station equipment, for instance, but also across legislative and judicial boundaries.

The issue of legislative and judicial boundaries raises the question of regulatory bodies. There are various requirements that are placed on service providers. Examples from the USA include requirements associated with Personal Identifiable Information Protection, the Payment Card Industry Data Security Standard (PCI-DSS), the Health Insurance Portability and Accountability Act (HIPAA), Critical National Infrastructure and Lawful Interception. Many of these have significant impact on the types of trust domain and the controls between them, a particularly notable example being the requirement to keep data in virtualized resources – whether parts of VNF or MANO components – confidential from non- authorized entities, as well as integrity-protected. In the short to medium term, technical controls will not be sufficient to provide all the required protections, reliance will continue to be placed on human and physical controls.

B. Infrastructure

The provisioning of appropriately secure infrastructure is a keystone to any securely-managed deployment. With open source software making up a significant part of many deployments, it is important to have a good view of the security of such software. The first point that should be made is that, for many service providers and operators, the

[6] http://eandt.theiet.org/magazine/2015/03/tactile-internet-5g.cfm

[7] See for example Architecture, constraints, and behavior, John C. Doyle and Marie Csete (http://www.pnas.org/content/108/Supplement_3/15624.abstract)

provision of open source software will not be directly by them, but by a vendor who will undertake to support it. To some extent, then, liability for the security of the software will lie with another party. A firm understanding of the liability and support arrangements behind the use of open source software is important in any deployment, but where that software has particular security functions, it is even more vital. It should be stressed, of course, that no system – either software or hardware – should be considered completely secure. Many of the security functions required for full softwarization – virtualization, containers, vSwitches, cryptographic libraries, etc. – are very complex, and seemingly minor mistakes in implementation may have major and far-reaching impacts on the service offering. What is more, the worldwide security community has shown time and time again that "security through obscurity" as practiced by some commercial vendors can be next to worthless. This does not mean, however, that the openness of open source software necessarily guarantees its security. There have been several examples of key security functions being shown to be incorrectly implemented, and even some cases of the public repositories in which such software is stored having been compromised, leading to concerns about the trustworthiness of the available code. The most robust code comes not from "many eyes", but from multiple expert eyes.

Operators planning to deploy open source software have both the opportunity and a responsibility to ensure that sufficient due diligence has been performed over that software, particularly when it supports core security functions.

One approach to mitigate security-related implementation errors or bugs in software that can be applied to either open source software or proprietary software is the provision of heterogeneous systems within a single deployment. Although this may be considered to increase the attack surface of a deployment, by introducing more systems, in reality it can reduce the impact of a single vulnerability in a key piece of widely-deployed software. There is, of course, a trade-off between manageability and security, but even when proprietary software is being used, when that software implements open interfaces or protocols, opportunity exists for consolidated management of the different systems – though this, in itself, may introduce a single point of failure which is unacceptable to service providers.

It has become clear, given the various vulnerabilities that software inevitably introduces, and whether proprietary or open source software is employed, that an approach rooted in hardware measures is required to provide sufficient defence in depth to satisfy a number of the requirements for a secure platform for both VNF and MANO components. Use of hardware-based attestation mechanisms can improve the trust in particular platform instantiations and agglomerations of systems, but run-time protection is more complex. Hypervisors already make use of chip-level hardware instructions to provide memory and process isolation between virtual machines, but protection of the administration layer from malicious or compromised workloads, and of the workloads from a malicious or compromised administration layer, will require further hardware measures. Containers in their standard Linux implementation currently make little use of hardware isolation. Hardware-mediated execution environments are expected to provide capabilities to allow isolation between layers of execution such as the hypervisor, vSwitch and virtualization components.

C. Operations

As noted above, management and maintenance of a deployment with multiple trust domains is a complex undertaking. A set of security policies, management capabilities and monitoring capabilities to support them is vital. Monitoring must be able to detect a variety of issues, of which reaction to malicious attacks is the most obvious. In order to do this, telemetry, agents and probes will be required in various positions (logical and physical) within the network and infrastructure: without aggregation across various layers, these inputs will be of significantly less utility. Malicious attacks are not, however, the only type of event to which operational reactions must be made. Probing – passive or active – of parts of the network or infrastructure may be the precursor to a full-out attack, and may occur at various levels: again, without aggregation and pattern-matching, such probing may not be detected.

An actual failure may occur for one of several reasons – one of which is a malicious attack – and may or may not have an impact on the security posture of the deployment. One of the opportunities offered by SDN is the ability, at least in some cases, to reconfigure the network to mitigate against such failures. Such reconfigurations should be in line with topology policies. NFV also offers opportunities for mitigation of failures, as VNFs – or their components – may be redeployable to nodes and hosts which are not affected – or less affected – by the failure.

In all these cases, there are likely to be options for different mitigation strategies. In some cases, the most secure is to "fail safe" – which may involve closing down a service. However, one alternative model – well supported by the SDN and NFV approaches noted above – is to accept a degradation of service, balancing impacts in various metrics such as security, performance and reliability whilst maintaining some levels of service. Although a common approach in the enterprise, reconciling this sort of degradation with the Service Level Agreements (SLAs) usually associated with telecommunications services will be a challenge. Another alternative may be to embrace the ability to sacrifice certain services (or degrade them to a larger degree) to maintain other, more critical services. These choices are enabled by softwarization, and require careful preparation and policy design.

One final point is the importance of managing trust models once they have been established. By default, trust relationships should be assumed to degrade over time. Neither can it be assumed that a trust relationship in one direction should be mirrored in the other direction: trust relationships are rarely symmetric. To give one example, the level of security controls implemented for an SDN controller will typically be higher than for the switches that it manages. It is therefore quite feasible – even probable – that vSwitches will fail or be compromised, and the SDN controller should expect these events and any trust model should take them into account when policies are being designed and implemented. The failure – or worse still, compromise – of an SDN controller is an altogether more complex problem to detect, let alone manage, and the ability of vSwitches to cope with such an event is likely to be much lower.

In summary, there are a number of areas where softwarization brings new challenges, or at least complexities, to security planning, operations and management. Some of these areas can be addressed with existing techniques whereas others – the use of hardware-mediated execution environments, for example – require new mechanisms and approaches. There are also opportunities: increased telemetry from NFV hosts and infrastructure will allow for mitigations as more traffic (North- South and East-West) is recorded, alongside performance and state metrics from various components of the deployment. The scale of these benefits and the challenges are yet to be discovered: security is still an area of very active research within both SDN and NFV.

IV. Strategic Role of Open Source Software

"Softwarization" of telecommunications opens up different strategies: vendor proprietary software, in-house operator development or open source software, and often a mix of these. But with cloud, NFV and SDN the number of open source initiatives is increasing. They typically leverage upon relatively mature IT projects such as Linux, KVM, libvirt, OVS and OpenStack [8] but also enterprise SDN with OpenDaylight, OpenContrail, ONOS [9] and expand towards specific needs of telecom operators, with Data Plane Development Kit (DPDK) for instance. The Open Platform for NFV Project (OPNFV) federates multiple upstream projects into one reference implementation for telecom networks. These projects, initially focused on the virtualized SDN enabled infrastructure, in line with corresponding standards, essentially ETSI NFV for NFV and ONF for SDN, are now evolving to the management stack. As the technology and the market progress, parallel and sometimes concurrent projects have also appeared, such as OpenMANO, Tacker or Open Baton for implementing the ETSI NFV MANO stack (Figure 3).

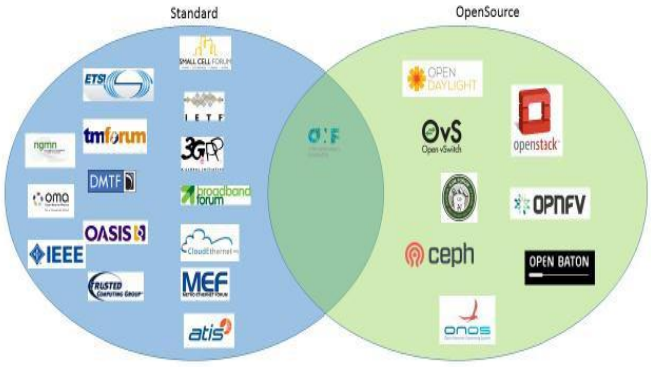


Figure 3: SDN-NFV Standards and Open Source Software

Some are driven by a very large community, and robust implementation platforms and processes, typically with OpenStack or Linux Foundation OPNFV, and OpenDaylight. Most of the code of these open source projects is released under Apache 2.0 license, a non-copyleft license, which opens up to different business models. These projects lead to software releases that are expected to be robust enough to support commercial deployment. But other projects have different objectives. They may be led by a much smaller ecosystem, with a less mature continuous integration mechanism and target different goals, more experimental. Open source can be interesting as collaboration projects to design some tests, or data models. Some standard organizations, such as IETF or ONF, look into open source projects as a way to validate specification with a reference implementation. Open source can also be initiated by a given vendor that decides to change business model, move from closed software to open software, and share his asset under a free open source license. More recently, an operator, Telefonica, released the Open MANO NFV orchestrator of his testing platform under free license and initiated action to aggregate external actors to this community. Open source is a way to drive innovation by granting easy access to the code and creating an open ecosystem

The benefits of open source for the telecom market are numerous: first it is a unique tool for a broad community, with operators, vendors, universities, to agree on requirements, use cases and prototype a solution quickly. Full consensus is often not necessary to start coding, as the open source model is based on an iterative approach (Figure 4). Experimentation and community expansion bring new requirements, and more robustness.

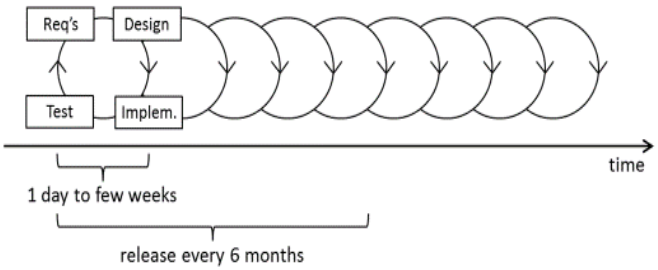


Figure 4: Open Source Iterative Model

Second, it is a great tool for research and universities: with software and open source, the entry barrier to build an experimental telecom network is getting lower and lower.

Third, it brings a common baseline across the industry and fosters better interoperability across vendors that adopt this technology and de facto across operators.

However the concern is that even now few operators adopt open source. Not only do operators have very few resources skilled to produce code and contribute to open source, but they are also very cautious of software coming from a community that does not aim to provide SLAs and standard assurance as proprietary solutions do, nor a clear roadmap as it is built iteratively from a kernel of subprojects. They would rather ask vendors to package open source software into a robust solution they can commit to deploy and support. Liability and risk remain key showstoppers to open source versus vendor proprietary software. Moreover open source is not only a question of technology; it becomes more and more a question of organization. As open source software is transforming the industry, it is difficult for non-native software companies to adopt its paradigms.

Nevertheless, open source is now clearly identified as complementary to standards to validate specifications with real neutral community-driven implementation. Open source is also the easiest and fastest way to fuel innovation across a broad ecosystem. With all-IP networks and 5G networks, more and more actors in the value chain become consumers and producers, including producers of open source code that

is live tested with a few virtual machines and enhanced on the fly by the community. Of course security is a big topic, but many studies and much work are also underway to cope with this.

V. SCENARIOS AND USE CASES

Multiple scenarios and use cases can be envisioned around softwarization of the network. Software-based solutions include the use of different types of virtualization, typically hypervisor or Linux container-based, NFV architecture, SDN control plane, and open APIs. They enable decomposition of the network and service layers into subcomponents that allow modular and multi-vendor architecture and software as service models. These allow service providers, infrastructure providers, and application vendors, to share services on the fly and expand towards new business models, as described in Figure 5.

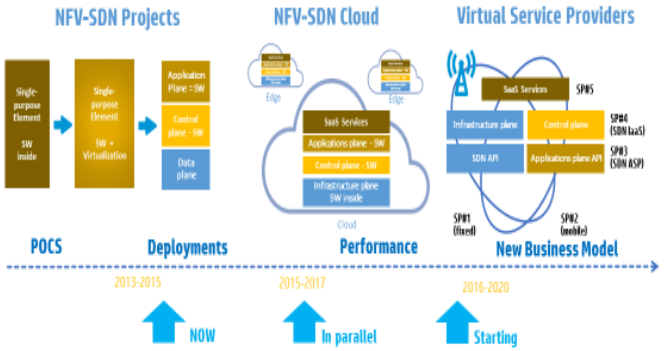


Figure 5: Softwarization, a Phased Approach

ETSI NFV defined nine use cases [10] mainly focused on the evolution of existing typical architectures for broadband or mobile networks towards virtualization, without disrupting the current status quo, i.e., 3GPP and some more specific SDN- NFV ones. But the industry is already exploring beyond this model, expanding into a combination of SDN and NFV, decomposition of the network functions, hybrid deployments with edge and cloud set-up, cross domain – multi operator environments, open management and service APIs including SLAs and monetization, etc.

A. *Cloudification Scenario: from Core Network Optimization to VNFaaS Use Case*

NFV is about virtualizing network functions, from residential customer set-top box to enterprise CPE, and network core functions such as Evolved Packet Core (EPC) and IP Multimedia Subsystem (IMS), and deploying them in a carrier grade NFV enabled cloud (Network Function Virtualization Infrastructure (NFVI) across multiple data centers. On top of that SDN is implemented on the connectivity layer decoupling data and control planes and bringing extra flexibility at the packet forwarding level, all in all to reduce cost and adapt quickly to market dynamics as shown in case#1 Figure 6.

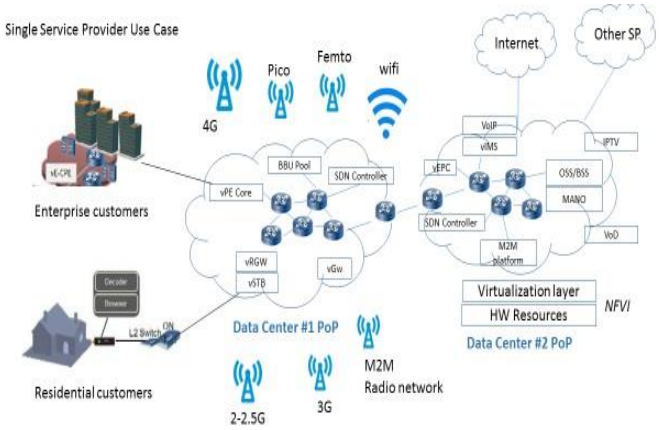


Figure 6: NFV and SDN to Optimize a SP Network

Further use cases define some VNFs that will be dedicated to certain enterprise customers. This is ETSI NFV VNFaaS use case to enterprise. But VNFaaS can also be provided to other SPs. SP#1 may have a virtualized infrastructure and VNFs, and offer some functions to a 3rd party SP#2 such as vHSS (Home Subscriber Server) for a Mobile Virtual Network Operator (MVNO), or functions such as virtual media service function for voice mail, audio-video conference or transcoding, for other SP, MVNO or Over-The-Top (OTT) service providers. The VNF can be deployed on shared or dedicated resources and capabilities offered to SP#2 are up to the multi-tenancy capabilities of SP#1: configuration, scalability, monitoring, usage-based charging, etc. (Figure 7).

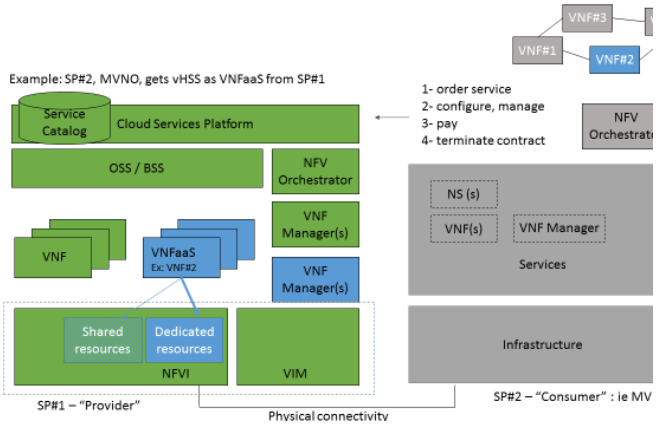


Figure 7: Virtual Network Function as a Service across SPs

B. *"NFV-SDN Decomposition" Scenario: Virtual Mobile Core*

Given the traffic growth on mobile networks and the impact of Machine-to-Machine (M2M) devices, virtualization of the mobile core is one of the top NFV use cases to deploy in small instances, for example dedicated to certain businesses such as M2M, or to bring flexibility to adapt to traffic variations and scale up and down programmatically and rapidly. But SDN is also being explored: not only for cost reduction but also to introduce granular programmability at the data plane level to bring new capabilities, such as dynamic routing of traffic per user or application, Openflow-based Wi-Fi offload, or reducing the Signal to Noise plus Interference Ratio (SNIR) by dynamically selecting base stations. Leveraging SDN and NFV can optimize low or ultra-low latency providing

placement of the SDN and virtual functions is designed properly (Figure 8).

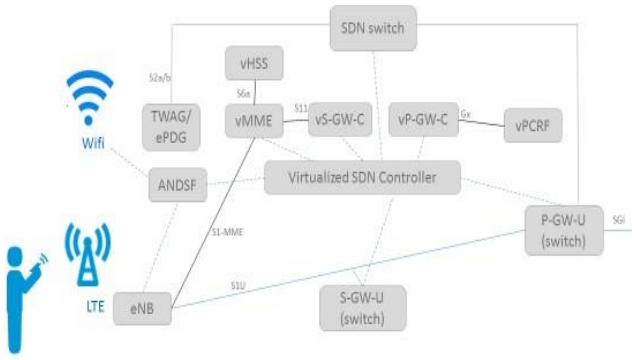


Figure 8: Virtualization and SDN in the Mobile Core

C. *"Edgification" Scenario: vCDN*

Virtualization of base stations and vCDN introduces virtualization to elements that are deployed at the edge of the network. While cloudification is a big trend to leverage cloud infrastructure and mutualization of resources, edge resources remain of high interest for services that require low latency or repeatable content to be distributed to end users, typically streaming blockbuster movies. Virtualizing end points such as CDN edge caching or mobile base stations to host some OTT or M2M vendor applications offers new capabilities to service providers and opens up new business models. It also processes some data at the edge and reduces the traffic being carried to the back end data centers (Figure 9).

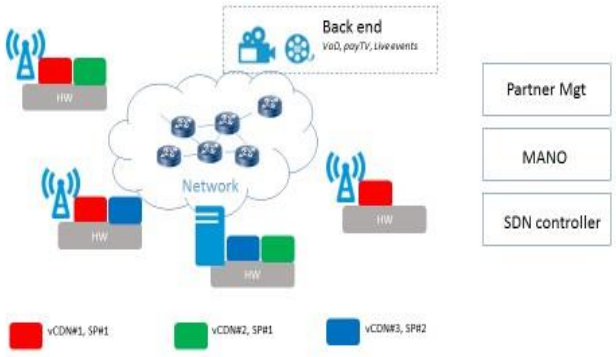


Figure 9: Virtualization of CDNs and Edge Deployment

D. *"Autonomous Machines"*

Robots, drones, autonomous machines, and Artificial Intelligence (AI) interfaces will be the 5G terminals of the future (Figure 10). The development of more and more complex cognitive capabilities through advanced terminals (increasingly powerful and sophisticated) attached at the edges of the 5G infrastructure, offers interesting opportunities not only to automate processes and optimize costs, but also to develop new service scenarios (Cognition as-a-Service). This will pose challenging requirements for ensuring ultra-low latencies in closing the interaction "loop".

Today, the local computing power of a robot is not enough (for reasons of consumption, space, dissipation, etc.) to implement strong cognitive characteristics of autonomy.

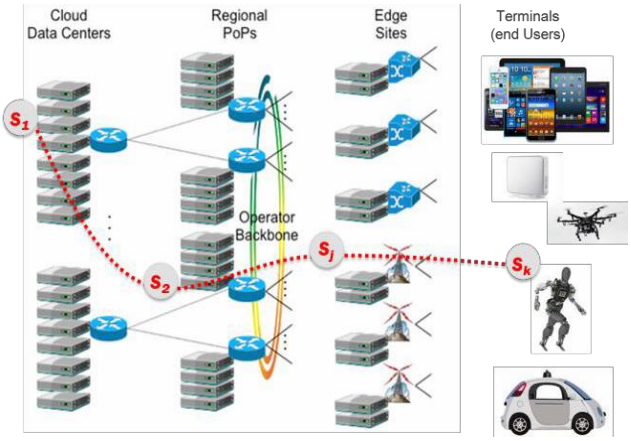


Figure 10: Robots, Drones, Self-Driving Vehicles becoming the "Terminals of the Future"

Tomorrow, thanks to 5G, it will be possible to make use of cloud robotics solutions which offer a huge amount of resources at low cost through cloud/edge computing. In fact, with 5G, the data collected from the several sensors of robotic systems, thanks to high bandwidth connections with very low latency, will be transmitted to destinations where there are adequate computing power and memory resources – with an appropriate centralization/distribution balance. These data will then be transformed quickly into cognitive "decisions", transferred back locally and actuated by the robot within a few milliseconds. It will be possible, for example, to perform highly accurate operations at a distance, to optimize real-time control of any transportation system, and to manage business processes in a highly dynamic and flexible fashion.

An example of an application use case is the radio remote control of an industrial robot or any Autonomous Machine (AM). It implies actuating the orchestration of the service logic execution of the AM. A user wishes to control a remote AM performing a certain service (X-as-a-Service) in a certain area (e.g., a museum or a firm). The AM is equipped with sensors and actuators and has some local (but limited) processing and storage capabilities. The AM is connected to a low latency radio network, the area (where the AM is acting) also has radio access to processing and storage capabilities (both in edge points of presence and in the cloud), which might be required to execute complicated tasks.

In agriculture, for example, AMs can be used for tasks like crop inspection, targeted use of water and pesticides, actions and monitoring to assist farmers, as well as in data gathering, exchange and processing for optimizing the production and distribution processes. Cloud robotics and Industry 4.0 paradigms are full of other potential use cases. In general, these are ideal contexts where an OS can control and operate AMs in real-time (as they were nodes) for a number of different applications. Interestingly, APIs can be opened to end users and third parties to develop new types of services.

Besides agriculture and industry, it is likely that we'll see robotic applications also in the domestic environment: It is estimated that by 2050-2060 one third of people in Europe will be over 65. The cost of the combined pension and health care system will be over 29% of the European gross domestic product (GDP). Remotely controlled and operated robots will enable remote medicine and open up a new world of domestic applications which may be available to the entire

population (e.g., cleaning, cooking, playing, and communicating).

E. Autonomous and Self-Driving Vehicles

The automotive sector is expected to pose very challenging requirements for 5G, with several use cases based on vehicle- to-vehicle communications and vehicle-to-cloud/edge. Other use cases concern services based on augmented reality dashboards installed in the vehicles: for example, displays that overlay information on top of what a driver is seeing through the front window and can identify objects in the dark or in fog by showing the distances and movements of objects.

Many car manufacturers are already adding driver assistance systems based on 3D imaging and built-in sensors and the first prototypes of self-driving vehicles are being tested. The technical requirements for self-driving cars call for ultra-low latencies and ultra-high reliability.

In fact, at the end of the day, a self-driving vehicle is a sort of complex robotic system equipped with sensors, actuators and ICT capabilities. Driving a car in real traffic is a very challenging task for machine intelligence: reaction times in milliseconds are required to avoid sudden and unpredictable obstacles, and maybe some form of "common sense" is also necessary. This demands considerable computing power (to minimize the application latencies) and very low network latencies.

Today, the local computing power that can be embedded in a vehicle is limited for reasons of space, dissipation, and cost. It is not enough for executing machine learning, heuristics or AI methods required to exploit such levels of autonomy. But the availability of enormous computing and storage power in the cloud encourages us to consider locating the "cognition" of the vehicle in the cloud.

VI. SOCIO-ECONOMIC IMPACT ON THE VALUE CHAINS

Technology trends are pushing the competition to move towards OPEX-based business models (e.g., Pay as you go), radically changing the current value chains. This will be reflected in a general convergence process of IT systems and networks and (in the medium to long term) in the gradual disappearance of the distinction between the network and what connects to it, i.e., terminals, machines, smart things, etc.

Technology is going to become accessible to all enterprises in any part of the world on an equal basis, further reducing any competitive advantage due to location. Hence, the real differentiator will be the capacity to innovate continuously. More and more the economics will shift from the economics of resources (becoming commodities) to the economics of data/information (and its related context). This will result in lower barriers to entry and thus lead to a larger number of players.

The impact of softwarization on the telecommunications industry can be seen as a substantial reinforcement of this general convergence process into converged infrastructure for all services (e.g., voice, internet access, and 'over the top' typical services). The emerging paradigm will be X-as-a-Service.

There is likely to be a split between Infrastructure Providers owning and operating the converged infrastructure, and the Service Enablers which offer the connectivity and network and service functions that enable Service Providers to develop and provision end-user services (e.g., retailing services). This split is also likely to drive a separation in the vendors supplying the infrastructure providers, the service enablers and the service providers.

The most likely merger will be between wholesale telecoms supply and data center hosting. In particular, the capital investment required to enter the data center hosting sector is likely to remain lower than that required to enter the access connectivity industry sector. In fact, many players offering global connectivity services are already also significant players in data center hosting.

The converged infrastructure can host a wide variety of network and service functions. Some of these services may not need to be executed in data centers and could instead be run in the middle of the network, involving virtualized functions to carry out intermediate information processing.

Some examples of these functions include:

- Content distribution networks;
- Content repurposing/recoding;
- Authentication, authorization, and access control;
- Content policing and filtering, content-based routing, content-based QoS management (e.g., Deep Packet Inspection (DPI));
- Intrusion detection;
- Firewall; and
- Content-based performance acceleration and bandwidth optimization (WAN acceleration).

These functions and others can be dynamically combined into complete services by constructing a specific chaining of functions – called service function chains. The orchestrator can be seen as a key system of such infrastructure. It would manage the different steps involved in the provisioning of virtual functions and services, such as creating and removing logical resources as well as installing, configuring, monitoring, running and stopping software processes in the logical resources. In this sense, the orchestration of these network and service functions is more linear (chaining) than traditional service orchestration which is based on a more articulated combination of service logics.

It seems likely that the retailing of traditional telecommunications services as a separate industry sector is going to disappear. Traditional telecommunications services will become packaged with other services such as voice with internet access and premium TV. Telecommunications retailing is likely to join with OTT service providers as voice becomes just another OTT service.

At the same time, there will be some merging in the supply of hardware between traditional telecommunications equipment suppliers and IT equipment suppliers. Some telecommunications equipment suppliers will reposition themselves as principally software supply companies. This will require a significant shift in the business model.

Many of the OTT service providers have no practical restrictions, be they technical, legal, or commercial, which means that they do not have to focus on a local national market. Many of these companies are truly global. The marginal cost of entering a new country is very low, assuming infrastructure is in place and is available to the OTT service provider. The introduction of SDNs and NFV enhances this situation, making the marginal cost of

geographical extension even lower. Indeed, softwarization makes it possible to be present in a geography without having to have any physical infrastructure at all, neither people nor physical equipment.

VII. CONCLUSIONS

Techno-economic drivers are creating the conditions for a change of paradigm in the design and operations of future telecommunications networks and services. SDN, NFV, Cloud and Edge-Fog Computing can be seen as different dimensions of a systemic transformation termed the "Softwarization" of Telecommunications.

This transformation will likely find concrete expression in the 5G network and services infrastructure, which will be much more than a direct evolution of current 4G networks (i.e., beyond merely an increase of bandwidth and reduced latency): 5G will be the "nervous system" of the digital society and economy.

This paper reiterates the text and conclusions of IEEE SDN Initiative white paper that describe:

1. an overview of the major techno-economic drivers steering the "Softwarization" of Telecommunications;
2. an introduction to the Open Mobile Edge Cloud vision;
3. the key challenges concerning security, policy and regulation;
4. the potential role of open source software;
5. some probable use cases; and
6. the main socio-economic impacts being produced by "Softwarization" [11].

The IEEE SDN initiative is also detailing the progress in the development of an open catalogue of software platforms, toolkits, and functionalities, aiming at a step-by-step development and aggregation of test-beds/field-trials on SDN- NFV-5G. This will prepare the ground for developing new ICT ecosystems, improving the quality of life and facilitating the development of the new digital economy.

ACKNOWLEDGMENTS

We would like to kindly acknowledge also the previous co-authors of IEEE SDN White paper[8], all members of IEEE SDN Initiative: Cagatay Buyukkoc (AT&T Labs, USA), Prosper Chemouil (Orange, France), Sławomir Kuklinski (Orange, France), Franco Callegati (University of Bologna, Italy), Alex Galis (University College London, UK), Marie-Paule Odini (HPE, France), Chih-Lin I (China Mobile, China), Jinri Huang (China Mobile, China), Mike Bursell (Intel, UK), Noel Crespi (Telecom Sud Paris, France), Eileen Healy (pdv Wireless, USA) and Stuart Sharrock (Telemates, UK).

REFERENCES

[1] White paper on "Software-Defined Networking: The New Norm for Networks" https://www.opennetworking.org/;
[2] White paper on "Network Functions Virtualisation" http://portal.etsi.org/NFV/NFV_White_Paper.pdf;
[3] C. M. R. Institute (2014) C-RAN: The road towards green ran. [Online]. Available: labs.chinamobile.com/cran
[4] CPRI, "Common Public Radio Interface (CPRI) Specification (V6.0)", Tech. Rep. Aug. 2013. Online: http://www.cpri.info.
[5] C. M. R. Institute (2015) White Paper of Next Generation Fronthaul Interface. [Online]. Available: labs.chinamobile.com/cran
[6] Chih-Lin I, Yannan Yuan, Jinri Huang, Shijia Ma, Ran Duan and Chunfeng Cui, "Rethink Fronthaul for Soft RAN", IEEE Commun. Mag. 53(9): 82-88
[7] Chih-Lin I, Rowell, C., Shuangfeng Han, Zhikun Xu, Gang Li and Zhengang Pan (2014) Toward green and soft: a 5G perspective. IEEE Commun. Mag. 52(2): 66-73
[8] Openstack: http://www.openstack.org/;
[9] ONOS: http://onosproject.org/;
[10] ETSI NFV Use Cases GS NFV 001.
[11] IEEE SDN Initiative http://sdn.ieee.org
[12] Ahmed, A., Ahmed, E., A Survey on Mobile Edge Computing - 10th IEEE International Conference on Intelligent Systems and Control, (ISCO 2016), DOI: 10.13140/RG.2.1.3254.7925
[13] Heilig, L., Voss, S., A Scientometric Analysis of Cloud Computing Literature, IEEE Transactions on Cloud Computing, Vol 2, Issue 3, April 2014, DOI: 10.1109/TCC.2014.2321168

[8] Manzalini A., et all, IEEE SDN Initiative white paper »Towards 5G Software-Defined Ecosystems: Technical Challenges, Business Sustainability and Policy Issues, July 2016, http://sdn.ieee.org/publications

GLOSSARY

3GPP	3rd Generation Partnership Project
5G	Fifth Generation
AI	Artificial Intelligence
AAA	Authentication, Authorization and Accounting
AM	Autonomous Machine
API	Application Program Interface
ASIC	Application Specific Integrated Circuit
BBU	Baseband Unit
CDN	Content Delivery Network
COMP	Control, Orchestration, Management and Policy
COTS	Commercial-off-the-shelf
CPE	Customer Premise Equipment
CPRI	Common Public Radio Interface
C-RAN	Cloud RAN
D2D	Device-to-Device
DPDK	Data Plane Development Kit
DPI	Deep Packet Inspection
DSP	Digital Signal Processing
E2E	End-to-End
EPC	Evolved Packet Core
eRAN	evolved RAN
ETSI	European Telecommunications Standards Institute
FH	Fronthaul
GDP	Gross Domestic Product
HIPAA	Health Insurance Portability and Accountability Act
HSS	Home Subscriber Server
ICT	Information and Communications Technology
IDS	Intrusion Defense Systems
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IMT	International Mobile Telecommunication
IT	Information Technologies

ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
KVM	Kernel-based Virtual Machine
LTE	Long Term Evolution
M2M	Machine-to-Machine
MANO	Management and Orchestration
MEC	Mobile-Edge Computing
MIMO	Multiple-Input Multiple-Output
MME	Mobility Management Entity
MTC	Machine-Type Communications
MVNO	Mobile Virtual Network Operator
NDS	Network Domain Security
NFR	Non-Functional Requirement
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NG	Next Generation
NGFI	Next Generation Fronthaul Interface
OMEC	Open Mobile Edge Cloud
ONF	Open Networking Foundation
ONOS	Open Network Operating System
OPEX	Operational Expenditure
OPNFV	Open Platform for NFV Project
OS	Operating System
OTT	Over-The-Top
OVS	Open vSwitch
PCI-DSS	Payment Card Industry Data Security Standard
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RAT	Radio Access Technology
RRH	Remote Radio Head
RRM	Radio Resource Management
SDN	Software-Defined Networking
SETI	Search for ExtraTerrestrial Intelligence
SLA	Service Level Agreement
SNIR	Signal to Noise plus Interference Ratio
SP	Service Provider
UE	User Equipment
UL/DL	Uplink/Downlink ratio
VNF	Virtual Network Function
WAN	Wide Area Network

BIOGRAPHY

Antonio Manzalini received the M. Sc. degree in electronic engineering from the Politecnico of Turin (Italy) and the Ph.D on Computer Networks from Télécom SudParis and Université Pierre & Marie Curie – Sorbonne Universités (France). In 1990 he joined CSELT, which then became part of Telecom Italia. He is the author of a book on network synchronization (for SDH), and his RT&D achievements have been published in more than 100 papers. He was active in ITU as Chair of ITU-T Questions, leading standards developments on transport networks. Since 2000 he has had leading roles in several EURESCOM and European Projects. In 2008 he was awarded with the International Certification of Project Manager by PMI. In 2013 and 2015 he led two projects on software defined networks (SDN) funded by EIT – Digital. He is currently a senior manager in the Strategy & Innovation Dept. (Future Centre) of Telecom Italia. His main interests are innovative architectures and services enabled by SDN and NFV, primarily for 5G. He is General Chair of the IEEE initiative on SDN. (antonio.manzalini@telecomitalia.it)

Alojz Hudobivnik received a B.Sc. and M.Sc. in computer science from University in Ljubljana, in Slovenia, 1983 and 1989, respectively. From 1990-2013 he worked in Iskratel, Kranj, Slovenia in area of telecommunication. He held a number of positions and was involved in product development of No.7 signaling, implementation of broadband access Slovenia, product management and corporate knowledge management. Later he was an independent telecommunication consultant and researcher (AH.TS s.p.) and is now Quality Manager (EuroPlus/NiceLabel). He has been active in telecoms standardization in ETSI (contributing to IMS standardization), FTTH Council Europe (accelerating the implementation of fiber-based, ultra-high-speed access networks for consumers and businesses) and has been a part of ITU-T for almost 20 years, dealing with such topics as the standardization of telecommunication architectures, including NGN and the upcoming Future Networks. He managed work of ITU-T FG Future Networks and was Ass. Rapporteur of ITU-T Q.21/13 Future networks, Vice-Chairman of ITU-T SG13 WP3 (SDN and Networks of Future) and Rapporteur of Q15/13 Data-aware networking in FN. He is Chair of Technical Standardization Board for the areas of electrical technology, IT and telecommunications by Slovenian NSO SIST and permanent delegate by CENELEC BT. He is Chair of Publicity Committee of IEEE SDN Initiative, Chair of Symposium and Workshops VITEL (since 2005) and Vice Chair of Slovenian Society for Electronic Communications (SIKOM). He is member of SOMTA and IEEE Senior Member. (alojz.hudobivnik@gmail.com)

Shifting radio access layers towards 5G
The 5G radio access basic principles and challenges

Srđan Knežević, Ericsson Slovenia

Abstract — This article presents Ericsson view on 5G Radio Access low layer challenges such as NX/Legacy interworking, key 5G radio access challenges (data rates, latency, traffic volume density, energy efficiency, reliability, massive antenna transmission, device density) in shifting towards 5G and usage of "existing" and new spectrums in 5G radio access.

Keywords —5G main enablers, 5G RAN design principles, 5G key RAN technology components, Massive MIMO, Mobility, 5G Spectrum

I. INTRODUCTION

Mobile communication has evolved significantly from early voice systems to today's highly sophisticated integrated communication platforms that provide numerous services, and support countless applications used by billions of people around the world. In addition to that future wireless access will extend beyond people, to support connectivity for anything that may benefit from being connected. Due to that reason, the earlier generation's one-size-fits-all radio access approach will not work for 5G.

Nowadays 5G topic can be covered from many aspects including things like what are 5G networks, requirements for early deployment, business cases, 5G security, migration, interoperability, spectrum usage, spectrum efficiency, radio access and core evolution... The document presents Ericsson view on 5G Radio Access low layer challenges such as NX/Legacy interworking, key 5G radio access challenges (data rates, latency, traffic volume density, energy efficiency, reliability, massive antenna transmission, device density) in shifting towards 5G and usage of "existing" and new spectrums in 5G radio access.

II. THE 5G SYSTEM CONCEPT

The rapid growth of mobile communication and equally massive advances in technology are moving technology evolution and the world toward a fully connected networked society – where access to information and data sharing are possible anywhere, anytime, by anyone or anything.

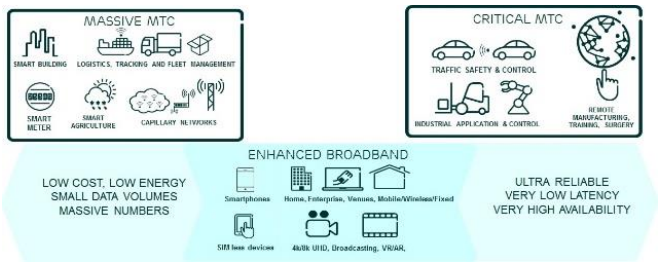


Figure 1: 5G – more than just enhance mobile broadband

To achieve such ambitions goals 5G system has to meet certain specific requirement which can be generalized into three generic 5G services and four enablers [1]

The three generic 5G services are:

- Extreme Mobile Broadband (xMBB):
  - Capacity, Coverage and Latency
- Massive Machine-Type Communication (mMTC):
  - 50 B devices and coverage including deep indoor
- Ultra-reliable Machine-Type Communication (uMTC):
  - Reliable, Resilient and latency

Most likely due to end user needs (and operator urges to serve such demands) first 5G release (Rel-15) will cover most of xMBB requirements. Extreme Mobile Broadband will provide extreme high data-rate, lower latency and more uniform user experience in a form of offering extreme coverage and virtual reality 4K support.

Machine-Type communication will provide wireless connectivity for tens of billions of network enabled devices together with efficient transmission, scalable connectivity and ultra-reliable low-latency communication links.

The four main enablers are:

- Dynamic Radio Access Network,
- Lean System Control Plane,
- Localized Contest and Traffic Flows,
- Spectrum Toolbox.

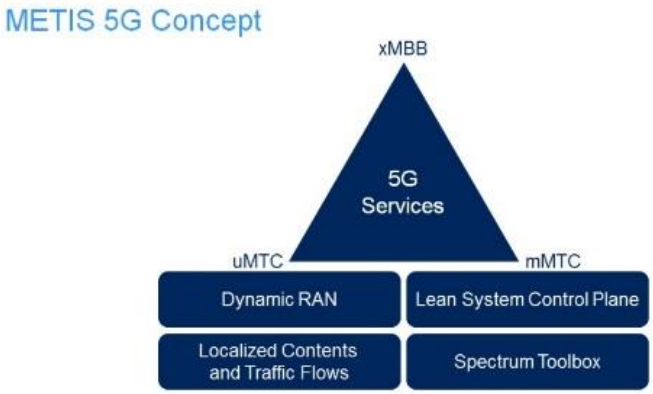


Figure 2: METIS- Main enablers and generic services

Dynamic RAN includes elements such as: antenna beams, device to device communication (D2D), ultra-dense network and device acting as temporary access nodes. Lean System provides lean control signaling with idea that communication will happen only when it is necessary by supporting spectrum flexibility, separation user from control data and supports large variety of devices with different capabilities. Localized

Contest and Traffic flows allows computing power to be placed closer to the end-user by enabling offloading, distribution of content close to physical layer. The Spectrum toolbox provides a set of enablers which will support a wide range of use cases with different requirements on the employed spectrum, signal bandwidth and authorization schemes. Depending on final 3GPP decision some overlapping functionality can end up in any of above mentioned category and it is desirable to make common as many functions as possible.

III. THE 5G FUNCTIONAL ARCHITECTURE AND FLEXIBILITY

Nowadays operator networks include a large variate od HW equipment in a form of different component nodes. To launch a new service often requires lengthy time to marker complex integration procedures on dedicated hardware. For the 5G networks to minimize negative complexity aspects important concepts are Network Function Virtualization (NFV) and Software Defined Network. Both concept will serve as key enablers to provide the needed scalability, flexibility and service-oriented management [2]

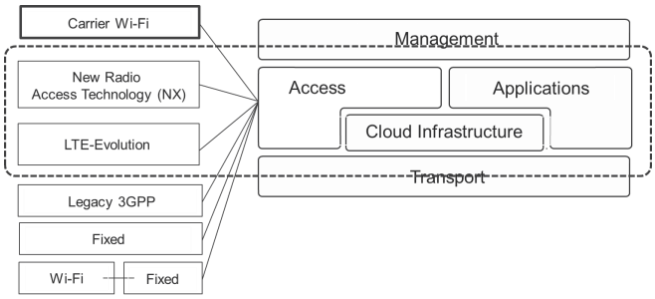


Figure 3: Vision of Network beyond 2020

At the end of 2012, network operators initiated concept similar to IT virtualization concept known as Network Function Virtualization [3]. The main NFV goal is to consolidate variety of the network equipment onto industry standard high-volume servers by giving to operators freedom that servers can be located at the different network nodes and premises. NFV may consist of one or more virtual machines running different software and process in order to replace dedicated HW.

While NFV principle brings benefits of decreased time to market and reduction of capital and operational expenditures, SDN bring concept of logical planes separation. The basic principles of SDN are separation of control and data planes, logical centralization of network intelligence and abstraction of physical networks from the applications and services by standard interfaces [4] . It is worth to mention that NFV and SDN do not rely on each other since NFV is providing flexible infrastructure for SDN while SDN concept enables virtual modularity of network functions.

Based on NFV and SDN concepts recent 5G researches addressed the logical architecture design by defining Network Functions (NFs) and inter-function interfaces instead of Network Elements (NEs) and inter-node interfaces [5][[6]. Further, the logical architecture design allows mapping of NFs to a protocol layers and placing such layers within different NEs. This logical design has been recognized as “functional split”. The functional split is characterized by the flexibility to place any NF at any location within NW topology.

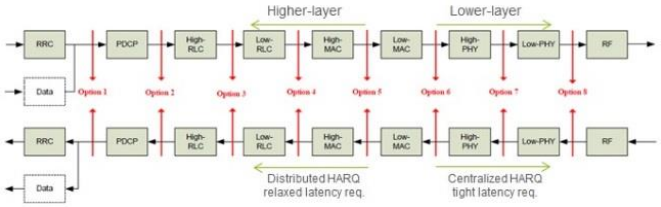


Figure 4: RAN split proposals

The approach of functional split brings freedom and flexibility to architecture design however potential challenge could be complexity of such systems especially in multi-vendor environments. In this moment it is hard to estimate what will be potential trade-off between complexity and flexibility.

IV. 5G NX RADIO ACCESS NETWORK

There are still a lot of uncertainties regarding 5G radio access specifications. According to the latest 3GPP acceleration agreement (March 2017) the idea is to have Non StandAlone specification done till the end of year 2017. Based on current commercial demand early 5G radio deployment will have mainly focus on evolved Mobile Broadband which is Non StandAlone solution.

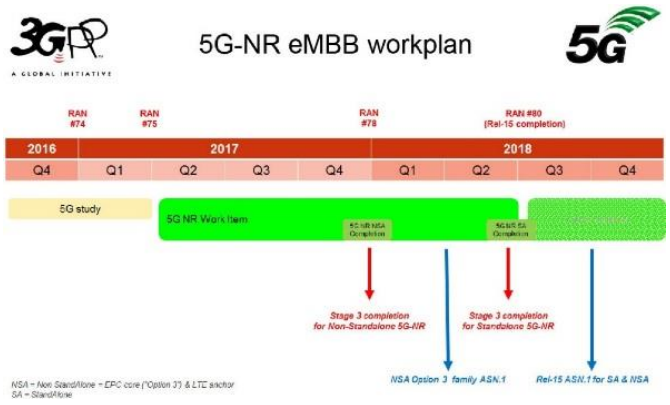


Figure 5: March 2017, 3GPP work plan for 5G NR Release 15

V. OVERVIEW 5G LOGICAL ARCHITECTURE

The 5G architecture should support both stand-alone deployments and deployments integrated with LTE (known as non-stand-alone deployment).

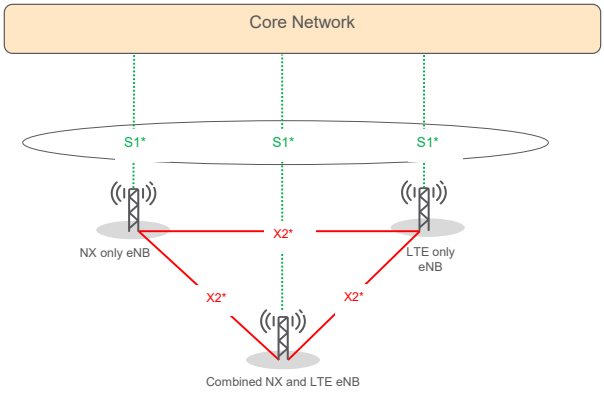


Figure 6: High level logical architecture for NX and LTE

Figure above shows the high level logical architecture for a system supporting both NX and LTE. The logical architecture includes both NX and LTE only eNBs as well as eNBs supporting both NX and LTE. It is assumed that the eNBs are connected to each other with the X2* interface and to the core network with the S1* interface. The current assumption is that there will be a CN/RAN split for 5G. [7]

It should also be mentioned that S1* and X2* are initially assumed as the only open RAN related network interfaces to be standardized It is initially envisioned that these should be an evolution of the existing S1 and X2 in order to facilitate the integration of NX with LTE. It is likely that these interfaces would need to be enhanced to support multi-RAT features for NX and LTE Dual Connectivity (DC), potentially new services (IoT or other 5G services) and features such as network slicing (where e.g. different slices and CN functions may require a different CN design), on demand activation of mobility reference signals, new multi-connectivity solutions, potentially new UP/CP splits in the CN, support for a new connected dormant state etc. A detail discussion about potential enhancements of these interfaces can be found in [8].

A. Spectrum and Propagation Challenges

The requirements for 5G services have implications for new spectrum. Peak rates of about 10 Gbps or higher, will require bandwidths of 1 GHz or more using state of the art technology. Such bandwidths will most likely not be made available at lower frequencies (e.g., below 6GHz). Millimeter wave spectrum bands (i.e., near and above 30 GHz) will play a role in some deployments to reach the envisioned peak rates. Given the propagation characteristics (of these bands), peak rates of over 10 Gbps may only be available within small hot spots.

5G MBB services will require a range of different bandwidths. At the low end of the scale, support for massive machine connectivity with relatively low bandwidths will be driven by total energy consumption at the user equipment. In contrast, very wide bandwidths may be needed for high capacity scenarios, e.g., 4K video and future media [9].

The NX air interface will primarily focus on high bandwidth services, and is designed around availability of large and preferably contiguous spectrum allocations. [10]

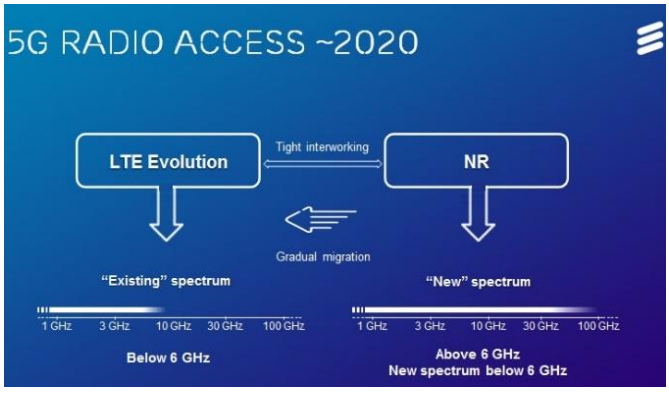


Figure 7: Ericsson view on 5G Radio Access in 2020 time frame

Propagation in the 6-100 GHz is currently extensively investigated worldwide by stakeholders in the telecom industry as well as by academy. The crucial question is what different kinds of technology and deployment solutions will be possible conditioned by the different propagation properties in different frequency bands. For free space transmission using fixed types of antennas (fixed antenna gains at TX and RX) the loss increases as 20 log(f), where f is the carrier frequency. This is purely an effect of the receive antenna aperture which is proportional to λ^2where λ is the wavelength. The radiated power flux density is independent of frequency. For a fixed available receive antenna area the increase in loss with frequency may however exactly be compensated for by utilizing array antennas (e.g. array gain). For free space transmission it is even possible to achieve a 20 log(f) gain if directive antennas are used in both ends of the link. In the case of NLOS propagation the same kind of compensation may be achieved to the extent the directivity of the channel is higher than the directivity of the antenna. It is likely that this often is the case at the access point in macro and microcell scenarios. For small cell and indoor scenarios, however, it is likely that the angle spread is substantial and that the gain of beam forming therefore is reduced. Further it is presently not assessed to what extent propagation into NLOS regions is governed by diffraction or by scattering by objects (buildings, cars, people etc.) in the environment. If diffraction is the main mechanism for propagation from LOS areas into NLOS areas substantially higher loss is expected for higher frequencies. However, both published [11] and [12] and internal results from urban microcell scenarios indicate that scattering by objects might be dominant as only minor frequency effects are observed.

As most users are located indoors it is very important to know the frequency behavior of building radio wave penetration as well as indoor radio wave propagation.

Last (and not the least) challenge on spectrum will be compliance with current regulative regarding EMF exposure. For frequencies above 6 GHz (North American market) and 10 GHz (Europe and most other countries in the world), basic restrictions are given in terms of free space power density. Studies have shown that the currently used exposure limits are more restrictive (up to 10 dB) in terms of allowed handheld UE transmit power above 6 GHz compared with the frequency bands used by existing cellular technologies. [13]

VI. LOW LAYER DESIGN PRINCIPLES AND CHALLENGES

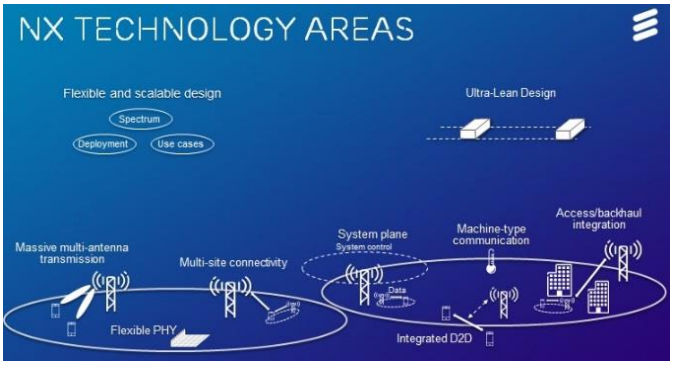


Figure 8: NX Key technology areas

Every new generation is a good opportunity to fix a long list of mostly minor problems that have been observed in previous generation over the years. The same principle is valid also for NX. There are quite a large number of areas where improvements can be made: LTE uses a fixed HARQ feedback timing which is a problem in some implementation

scenarios (e.g. with centralized baseband deployment or non-ideal backhaul) and when operating in unlicensed spectrum (e.g. where listen-before-talk sometimes prevents UEs from sending HARQ feedback) ; the LTE UL and DL L1 control channels can be improved for better support of high gain beamforming, the switches between transmission modes and configurations is unnecessarily hard and slow; there is a rather long latency coming from the UL scheduling; the DRX behavior is not always optimal; the design of the scheduling request channel is not very flexible or efficient; etc.

In particular there are some areas where the backwards-compatible requirements of LTE may be limiting: Support for reciprocal massive MIMO transmission and Massive MIMO beamforming can likely be made to work better in NX than in LTE. Other improvement areas are dynamic TDD; unlicensed band operation; contention based access; multi-connectivity; multi-hop; D2D etc. These are areas that have increased significantly in importance since LTE Rel-8 was finalized and we now have an opportunity to enable enhanced support for these features in NX already from the start instead of patching in solutions to an existing standard. The situation now is somewhat similar to when WCDMA was developed and MIMO support was not part of the first Rel-99 release but was added later while for LTE the use of MIMO has always been an integral part of the system from day one. With NX we can ensure native and optimized support for increasingly important use-cases such as multi-X (multi-connectivity, multi-RAT, multi-hop, multi-carrier, multi-node, multi-beam), UL/DL decoupling etc. from the start.

One key lesson from previous generations is that they continue to evolve after the initial release. Therefore, the NX standardization challenge will be to have both a RAT evolution strategy as well as a migration story and exit strategy for services in place from the very beginning.

By influencing design of NX L2, Ericsson is using a few key design principles such as:

– Service agnostic design allowing flexible service centric configurations

  The NX standard should provide a large set of service agnostic features which the network may configure and enable to fulfill the service specific requirements. This is supposed to enable co-existence of multiple services while maintaining low complexity and high efficiency for each service

– Stay in the box

  A key feature of LTE is that all traffic is mapped dynamically to a single pair of shared channels (PDSCH/PUSCH). This maximizes statistical multiplexing and allows a single UE to get instantaneous access to all radio resources of a carrier or even multiple carriers. Appropriate RLC configurations and scheduling policies ensure that QoS requirements are met. While NX should maintain this fundamental principle some services just cannot be multiplexed. For example, it is not acceptable if a breaking command in a traffic junction is interfered by a packet from the entertainment system in a nearby car. Hence for some critical use cases (e.g. intelligent transport system, public safety, industrial automation, etc.) it may not be acceptable to coexist on the same radio resources with any other service.

– Flexibility

  NX shall have a lean and scalable design that is able to cope with various latencies on the transport and radio interface as well as with different processing capabilities on UE and network side. To ensure this, one should for example avoid fixed timing relations between control messages such as HARQ (MAC), ARQ (RLC) and RRC signaling

– Design for flows

  For NX we want to optimize the control signaling by utilizing correlations in traffic. By doing this we can avoid hard and slow reconfigurations. Whenever we can predict a future behavior (e.g. if we sent something in the downlink there will be uplink traffic a short while later) we shall try to take advantage of that: E.g. start with open-loop transmission and do a seamless switch to a closed-loop transmission format once the channel state information becomes available at the transmitter end

– Layers of coordination

  When the cost of observation and control becomes too high, e.g. in terms of delay or overhead, we are better off delegating scheduling decisions to nodes and UEs for the time it takes to collect sufficient information and enforce a suitable coordination. The centralized resource scheduler still owns and controls the right to use radio resources but in situations where observation and control is easier and more efficient to maintain in another node (e.g. in multi-hop relaying or D2D) the momentary decisions on how to assign resources should be distributed.

– Lean and thereby future-proof

  The mandatory transmissions to be done by an NX eNB at specific times should be sparse in time and frequency. For example, the NX terminal should not expect control messages at specific time/frequency resources (as is the case today for HARQ feedback in LTE). The configurability will enable forward compatibility as the network can assign resources freely to other (newer) terminals without having to send a massive amount of legacy signals for legacy terminals. In particular when operating in unlicensed spectrum, the NX radio interface needs to be able to send control information at dynamic time instances. In addition to containing all signals in a bounded resourced slice a user shall be capable of ignoring any “un-defined resources” within the resource slice unless explicitly instructed otherwise. “Un-defined resources” may be dynamically configured as a set of periodic patterns in time, and/or in frequency.

VII. MASSIVE MULTI-ANTENNA TRANSMISSION

Massive Multiple-Input Multiple-Output systems are considered essential in contribution to support 5G requests for larger capacity, data rate and coverage as massive MIMO provides substantial increase spectral efficiency per cell. A massive MIMO system is typically defined as a system that utilizes a large number of individually controllable antenna elements (in general on base station side) [14]. Such systems exploit spatial multiplexing by providing multiplex messages for several users on the same time-frequency resource and minimizing intra-cell and inter-cell interference. Focusing of

radiating signals in particular direction is possible by transmitting the same signal from multiple antennas using different phase shift per each antenna. Key challenges which have to be overcome are following: [15]

– The need of accurate Channel State Information (CSI) at the transmitter side

  The basic principle is that the CSI may be obtained through the transmission of reference signals from each transmit antenna element. The drawback is that the pilot signal overhead in terms of required CSI grows linearly with the number of transmit antennas. Another approach is to utilize channel reciprocity like in TDD systems. The cost of utilizing reciprocity is that it requires array calibration in order to take the differences in radio frequency (RF) chains of different antenna elements. In time varying channels, the delay between pilot transmission, channel estimation, channel feedback, beamform calculation and actual beamform data transmission will degrade the performance of massive MIMO

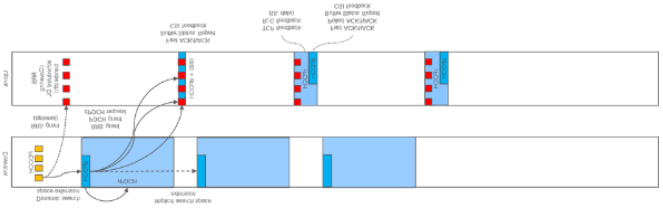


Figure 9: Usage example of downlink data transmission supporting reciprocal massive MIMO beamforming

– Impact of Pilot contamination

  In multi-cell multi-user massive MIMO system the pilot data resource allocation trade-off is interwined with the management of inter-cell interference both on pilot and data signals

– The exploitation of Massive MIMO in a network with an ultra-dense deployment of small cells

  At lower frequencies, the size of the antenna arrays is limited factor. At higher frequencies (millimeter Wave – mmW) the size is not an issue.

Ideally, the signals from/to all antenna elements should be digitally processed in the baseband domain so that all the degrees of freedom are available for the transmitting side. This gives total flexibility in the spatial and frequency domains for post-processing signals at reception and for precoding at transmission; thus, enabling full potential of massive MIMO features such as frequency-selective precoding and MU-MIMO.

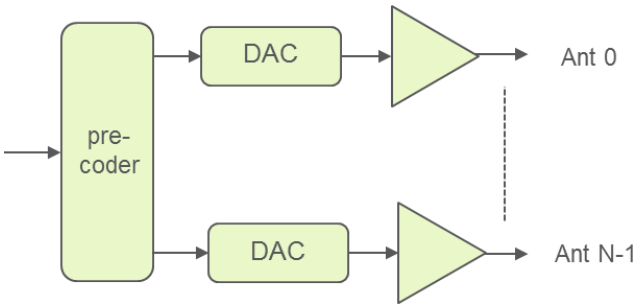


Figure 10: Digital beamforming

Nowadays due to practical limitation such as real-time computing, power per element and cost of architecture beamforming is done in the analog (time) domain. Note, since beamforming is done after converter is frequency independent and applies to the entire spectrum.

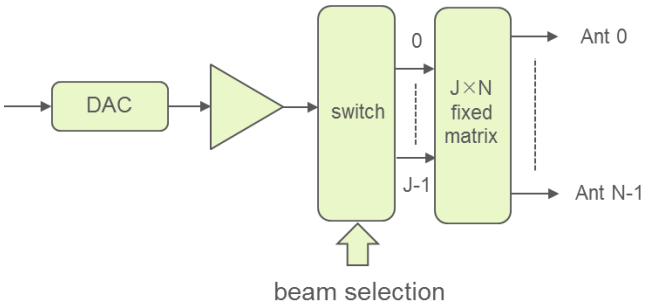


Figure 11: Analog beamforming

Much of the feasibility of using very large antenna systems will be dictated by the required hardware quality and trade-offs regarding:

– Data converters resolution,
– Non-linear, efficient power-amplifiers and mutual coupling,
– Oscillator phase-noise,
– Centralized or distributed processing,

VIII. MULTI-SITE CONNECTIVITY

NX is likely to be deployed in bands higher than those of current commercial RANs. At higher frequencies, shadowing of radio paths is much more severe as compared to radio shadowing at lower frequencies. Especially for high frequencies, line-of-sight may be needed for successful transmission. In such radio conditions, multi-point connectivity can be used to reduce interruptions in traffic. Capacity and user throughput improvements can also be achieved when multiple connection points can be maintained simultaneously. The NX concept supports multi-point connectivity as an integral part of the concept. It is important to emphasize that the DL mobility concept of NX is beam based. From a UE point of view, the mobility procedures are the same independently on how many eNBs that are involved. A consequence of this is that the UE does not have to care about which eNB is transmitting beams or not; sometimes we refer to this as the UE being node agnostic and the mobility being UE centric. For mobility to work efficiently, the involved eNBs need to maintain beam neighbor lists, exchange beam information, and coordinate MRS usage. Fast switching of beams in a multi-point connectivity scenario requires fast communication between eNBs and may also require pre-caching and duplication of data; in many cases the data need to be duplicated and distributed to, and from, multiple eNBs. This requirement challenges the capability of backhaul connection in terms of capacity and delay. One option is to put a certain data splitting agency at EPC side so as to remove the loop at anchor-eNB S1 connection.

Different transmission/reception modes can be considered depending on the channel conditions, network deployment, available backhaul capacity and delay, and type of traffic. In the NX context, we prefer to talk about multi-point diversity (MPD), traffic aggregation and distributed MIMO. Traffic

aggregation usually refers to multi-connectivity operations at lower layers being independent and distinct in terms of resources and/or RATs, such as carrier aggregation or IP layer aggregations. Distributed MIMO involves multiple transmission points and assumes joint coding over the branches. Typically, it requires a backhaul with high capacity and low delay to deliver the expected performance.

Coordinated multi-point (CoMP) is a term that is used to describe a set of specific LTE features used for intra LTE multi-point connectivity. Usually, CoMP features tight coordination on MAC level. MAC coordination is needed when co-channel radio resources are used for the different transmission points. The term CoMP is intentionally avoided in the NX context to avoid confusion.

Alongside measurement acquisition, the main challenge associated with multi-point connectivity lies in limitations on capacity and delay in the backhaul links carrying the inter node interfaces. In many deployments, backhaul with limited capacity and large latency is the only option due to high cost involved in deploying fast backhaul. For example, in some cases, X2 connections are made available by an ordinary internet data link.

Relevant concept to multi-connectivity for NX is DC concept in LTE [16] and cluster concept in mmW [17] [18]. The scope of DC in LTE is to support one UE connect to two eNBs using different frequencies and the scope of cluster in mmW is to support one UE connect to more than one eNBs sharing a carrier.

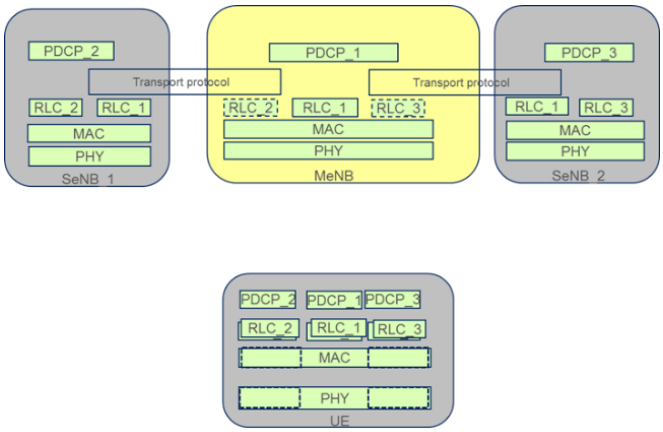


Figure 12: Example of User Plane protocol architecture

Multi-point connectivity on the user plane can operate at different layers. The integration layer for multi-point connectivity can be either PHY layer, MAC layer (which corresponds to Carrier Aggregation in the LTE context), or PDCP layer (which corresponds to Dual Connectivity in LTE).

For the Control Plane the focus is whether to have one centralized RRC entity in MeNB (Master eNB) or multiple RRC entities distributed in both MeNB and each SeNB in multi-point connectivity. The advantage of centralized RRC entity is that it is simple compared to multiple RRC entities and follow the same architecture as LTE DC. UE only needs to maintain one RRC connection with MeNB and it is not impacted by DL and UL decoupling. The disadvantage is that the response to some radio resource configuration at SeNB, e.g. UE beam switching within SeNB, may be slow and when MeNB crashes the procedure to recover the whole multi-point connectivity could also relatively time consuming.

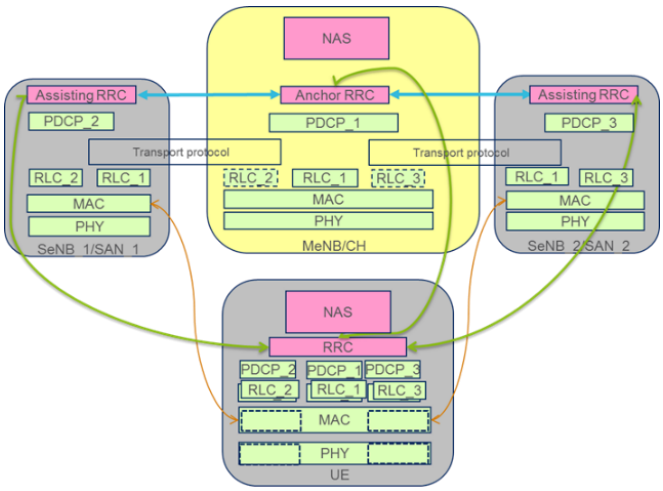


Figure 13: Multiple RRC entities at both MeNB and SeNB

IX. ERICSSON CONCLUSION

NX is Ericsson's non-backwards compatible RAT concept for 5G. NX targets vast range of new use cases based on MTC as well as Extreme Mobile Broadband, and may be deployed in a wide range of spectrum bands, calling for high degree of flexibility. A wide range of frequency bands are supported, from below 1 GHz to almost 100 GHz. It is of principal interest to ensure that NX can be deployed in a variety of frequency bands, some targeting coverage at lower frequency regions below 6 GHz, some providing a balance of coverage, outdoor-to-indoor penetration and wide bandwidth up to 30 GHz, and finally some bands above 30 GHz that will handle wide bandwidth use cases, but possibly at a disadvantage to coverage and deployment complexity. Both FDD and dynamic TDD, where the scheduler assigns the transmission direction dynamically, are part of NX. However, it is understood that most practical deployments of NX will likely be in unpaired spectrum, which calls for the importance of TDD.

The phased standardization process in 3GPP entails attention to forward compatibility to allow the flexibility of later introduction of new features without affecting existing devices. Ultra-lean design, where transmissions are self-contained with reference signals transmitted along with the data, minimizes broadcasting of signals. Terminals make no assumptions on the content of a subframe unless they are scheduled to do so. The consequence is significantly improved energy efficiency as signaling not directly related to user data is minimized

Stand-alone deployments as well as tight interworking with LTE are supported. Such interworking is key for consistent user experience with NX when used at higher frequency ranges or at initial NX rollout with limited coverage. The chosen multi-connectivity solution builds on the RRC/PDCP-based dual connectivity solution for LTE Rel-12. The RAN architecture can handle a mix of NX-only, LTE-only, or dual-standard base stations. The eNBs are connected to each other via the X2* interface and to the core network via the S1* interface as the only open RAN related interfaces to be standardized. It is envisioned that these should be an evolution of the existing S1 and X2 interfaces to support features such as network slicing, on demand activation of signals, UP/CP splits in the CN, and support for a new connected dormant state. The current working

assumption is that LTE and NX share at least integrated higher radio interface protocol layers (PDCP and RRC) as well as a common S1* connection to the packet core (EPC).

Enabling full potential of Multi-antenna technology is a cornerstone of the NX design. Hybrid beamforming is supported and advantages with digital beam forming are exploited. User-specific beamforming through self-contained transmission is key for coverage, especially at high frequencies. For the same reason, UE TX beamforming is proposed as an essential component, at least for high frequency bands. The number of antenna elements may vary, from a relatively small number of antenna elements in LTE-like deployments to many hundreds, where a large number of active or individually steerable antenna elements are used for beamforming, single-user MIMO and/or multi-user MIMO to unleash the full potential of massive MIMO. Reference signals and MAC features are designed to allow exploiting reciprocity-based schemes. Multi-point connectivity, where a terminal is simultaneously connected to two or more transmission points, can be used to provide diversity/robustness, e.g. for critical MTC, by transmitting the same data from multiple points.

The high level key technology components that typically have been used to promote NX are: extension to higher frequencies and wider bandwidths, flexible and scalable L1 design, separation of the user and control plane, energy efficient and forward compatible design, advanced antenna techniques, and tight interworking between NX and LTE.

The NX concept is the Ericsson basis for the upcoming 3GPP standardization of the new non-backwards compatible 5G RAT.

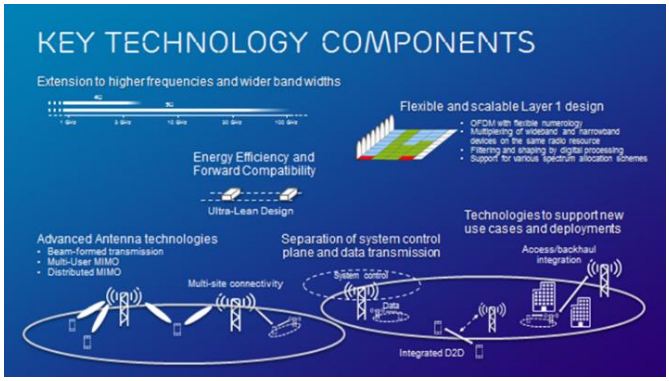


Figure 14: Ericsson High level key technology components

There are different proposals about functional splits and functional interoperability services. Nowadays technology allows splits and placing of NF virtually at any location within NW topology. However, Ericsson believes that such solution will not be attractive to operators due to complexity of such solutions, slower progress in defining new radio and network feature, risk of less future proof, less room for vendor specific innovation around algorithms and last but not least potential risk of OPEX increase due to inter-operability and integration issues.

Based on the fact that a network slice is always complete in terms of adequate business objective to be served, the term network slice should not refer to some smaller aggregate of functions. For smaller aggregate functions maybe it would be enough to use term sub-CN instance or subnetwork instance.

Figure 15: Ericsson 5G view on Network Slicing – One network – many industries, many network slicing

REFERENCES

[1] "Final report on the METIS 5G system concept and technology roadmap," METIS, ICT-317669, April 2015.

[2] A. Osseiran, 5G Mobile and Wireless Communications Technology, Cambridge University Press, 2016.

[3] AT&T and e. al., "Network Function Virtualization: An Introduction, Benefits, Enablers, Challenges & Call for Action," [Online].

[4] O. N. Foundation, "Software-Defined Networking: The New Form for Networks," April 13 2012. [Online].

[5] 3. T. 36.300, "Overall description; Stage 2 (Release 12)," in Technical Specification TS 36.300 V11.7.0, Technical Specification Group Radio Access Network, September 2013.

[6] I.-3. M. project, "Final report on architecture," Deliverable 6.4, Version 1,, January 2015.

[7] 3GPP, "TDOC S2-153651: Study on Architecture for Next Generation System," 3GPP Study Item Description, November 2015.

[8] M. WP6, "Report R6.1 Preliminary asynchronous control functions and overall control plane considerations," Metis 2 report, December 2015.

[9] L. M. Campoy and M. A. Uusitalo, "Description of the spectrum needs and usage principles," METIS deliverable D5.3, August 2014.

[10] E. W. P. U. 2. 23-3244, "Ericsson White Paper: 5G Systems," January 2015.

[11] S. Sun, G. R. MacCartney, M. K. Samimi, S. Nie and T. S. Rappaport, "Millimeter Wave Multi-beam Antenna Combining for 5G Cellular Link Improvement in New York City," IEEE ICC Wireless Communications Symposium, 2014.

[12] M. Inomata, W. Yamada, M. Sasaki, M. Mizoguchi, K. Kitao and T. Imai, "Path loss model for the 2 to 37 GHz band in street microcell environments," *IEICE Communications Express*, vol. 4(5), pp. 149-154, 2015.

[13] D. Colombi, B. Thors and C. Törnevik, "Implications of EMF exposure limits on output power levels for 5G devices above 6 GHz.," IEEE Antennas and Wireless Propagation Letters, 2015.

[14] E. Larsson, O.Edfors, F. Tufvesson and T. Marzetta, "Massive MIMO for the next generation wireless systems," *IEEE Communications Magazine*, vol. vol. 52, pp. 186-195, 2014.

[15] L. LU, G. Li, A. Swindlerhurst, A. Ashikhmin and R.Zhang, "An overview of massive MIMO: Benefits and challenges," *EEE Journal of Selected Topics in Signal Processing*, Vols. vol. 8, no. 5, October 2014.

[16] "36.300, 3GPP, "R12 E-UTRAN Overall description Stage 2"".

[17] D. Hui, Fast Beam Switching with UE-Specific Cluster of Serving Nodes, 2014.

[18] M. Qingyu, "UE centric mobility management in mmW," 2015.

Srđan Knežević has been working for Ericsson since 2005. He has participated in WCDMA and LTE projects as a RAN Solution Architect.

Zagotavljanje storitev za zaščito in reševanje v okoljih 5G

Urban Sedlar, Luka Koršič, Mojca Volk, Janez Sterle, Univerza v Ljubljani, Fakulteta za elektrotehniko

Povzetek — 5G predstavlja naslednjo generacijo mobilnih komunikacij, ki bo omogočala številne nove scenarije uporabe. Ena od pomembnih aplikacij bo tudi v sistemih za zaščito in reševanje naslednje generacije, kjer bodo tehnologije 5G odpravile pomanjkljivosti prejšnjih generacij. V prispevku predstavljamo ogrodje ARCADIA, ki rešuje izzive razvoja, avtomatizirane vzpostavitve in upravljanja skalabilnih, visoko razpoložljivih in porazdeljenih aplikacij, kar bo v okolju 5G z apliciranimi tehnikami SDN, NFV in računalništva v oblaku omogočalo orkestracijo omrežnih in storitvenih gradnikov. Uporabo ogrodja ARCADIA ilustriramo na primeru visoko razpoložljivega sistema 6inACTION za zagotavljanje storitev in aplikacij za zaščito in reševanje. Na primeru prikažemo, kako aplicirati tehnike ARCADIA in s tem omogočiti enostavno vzpostavitev operativnega sistema preko grafičnega vmesnika, bistveno povečanje stopnje razpoložljivosti storitev, tudi v primeru izpadov omrežnih ali storitvenih elementov v primeru naravnih nesreč, ter horizontalno in vertikalno skaliranje v primeru preobremenitev.

Ključne besede — 5G, urgentne komunikacije, zaščita in reševanje, PPDR, SDN, NFV, ARCADIA, 6inACTION

Abstract — 5G represents the next generation in mobile communications, bringing about numerous new service scenarios; one such important application are novel public protection and disaster relief systems, where 5G technologies will help in overcoming the current communications shortcomings. In this article, we present ARCADIA framework, a solution that addresses the challenges of development, automated deployment and management of scalable, highly distributed applications with high availability, which will enable orchestration of network and service elements in 5G environments with SDN, NFV and cloud computing. We illustrate the use of the ARCADIA framework on a service scenario for public protection and disaster relief based on 6inACTION system. In the example, we demonstrate how ARCADIA techniques can be applied to enable efficient deployment of an operational system via a graphical user interface, considerable improvement of service availability, also in case of network and service elements failure due to natural disasters, and horizontal and vertical scaling for overload scenarios.

Keywords — 5G, emergency communications, public protection and disaster relief, PPDR, SDN, NFV, ARCADIA, 6inACTION

I. UVOD

Tehnologija 5G ne predstavlja le gonila razvoja na področju nove generacije vedno bolj zmogljivega mobilnega radijskega vmesnika ter novih povezovalnih konceptov jedrnega mobilnega omrežja (SDN in NFV), ampak tudi inovativen pristop integracije trenutno strogo ločenih rezidenčnih in poslovnih ter industrijskih silosov (npr. namenski komunikacijski sistemi za službe javne varnosti in energetiko) v komunikacijsko in storitveno platformo, ki bo temeljila na enotni omrežni in oblačni infrastrukturi. Sistem bo omogočal vzpostavitev novih vertikal in storitev ter tako zasnovo novih poslovnih modelov in zmožnosti, ki danes na obstoječih rešitvah niso mogoči oziroma smiselni. 5G bo tako moral združevati heterogene tehnološke zmožnosti, ki bodo omogočale zagotavljanje ultra-širokopasovnosti rezidenčnim uporabnikom (npr. UHD video prenos), priklop velikega števila senzorskih naprav (npr. priklop pametnih energetskih senzorjev), M2M aplikacije z zelo majhnimi zakasnitvami (npr. komunikacija med vozili) ter veliko razpoložljivost sistema tudi v ekstremnih in nepredvidljivih razmerah (npr. zahteva za komunikacije profesionalnih služb PPDR), ki so lahko posledica vremena in drugih okoljskih dejavnikov (npr. poplave, žledolom in potres).

Zasnova in načrtovanje sistema, ki bo transparentno izpolnjeval širok nabor specifičnih zahtev ter omrežnih in storitvenih funkcij za podporo različnim scenarijem iz poslovnih in industrijskih vertikal, predstavlja izjemno kompleksen tehnološki izziv. V okoljih 5G se na slednje tehnološke izzive osredotoča predlagan koncept omrežnih rezin (angl. network slicing), ki omogoča preprosto nastavitev in pouporabo omrežnih elementov in funkcij glede na potrebe specifičnega domenskega scenarija, ter njegova nadgradnja v smeri integracije in orkestracije storitvenih gradnikov, kot to predlaga ogrodje ARCADIA (angl. A Novel Reconfigurable By Design Highly Distributed Applications Development Paradigm Over Programmable Infrastructure).

II. OGRODJE ARCADIA

Ogrodje ARCADIA [1], ki se razvija v okviru projekta Obzorje 2020 z imenom ARCADIA (GA št. 645372) rešuje izzive razvoja, avtomatizirane vzpostavitve in upravljanje skalabilnih, visoko razpoložljivih in porazdeljenih aplikacij. Ena od možnih aplikacij takšnega sistema je orkestracija omrežnih in storitvenih gradnikov v sistemih 5G, ki temeljijo na konceptih SDN in NFV. V prispevku bomo predstavili aplikacijo ogrodja na primeru visoko razpoložljivega sistema za zagotavljanje storitev in aplikacij za zaščito in reševanje, ki je bil razvit za heterogena omrežna in storitvena okolja, kot ga predstavlja tudi omrežje 5G.

A. *Visoko porazdeljene aplikacije*

Visoko porazdeljena aplikacija (angl. *Highly Distributed Application* – HDA) je skalabilen sistem programskih gradnikov, ki je prilagojen za izvajanje v več oblakih (angl. *Multi-cloud, multi-IAAS*). Narava aplikacij HDA omogoča veliko fleksibilnost pri pouporabi storitvenih gradnikov, kakršni so podatkovne baze, spletni strežniki, gradniki, ki zagotavljajo storitve omrežnih funkcionalnosti, avtentikacije, ipd. Takšne samostojne gradnike z jasno predpisano

funkcionalnostjo, ki so v sistemu šibko sklopljeni, pogosto označujemo z izrazom mikrostoritve (angl. *microservices*).

B. Komponente in ovijanje

Posamezne gradnike v ekosistemu mikrostoritev lahko realiziramo na več načinov. V preteklosti so bili to namensko postavljeni in vzdrževani strežniki (t.i. bare-metal namestitev); ta možnost je na voljo še danes, saj ne nosi režijskih stroškov (angl. *overhead*) virtualizacije. Trenutno je na voljo več sistemov za upravljanje strojne opreme v podatkovnih centrih, eden od bolj razširjenih pa je MaaS (angl. *Metal as a Service*) podjetja Canonical. V večini sodobnih namestitev pa je mnogo bolj praktična uporaba različnih tehnik virtualizacije:

– Virtualni stroji (virtualizacija tipa 1 in paravirtualizacija); tipična okolja so KVM, ESX, XEN, ipd.;
– Kontejnerji; popularni rešitvi s tega področja sta Docker in LXC;
– Virtualni stroji, ki temeljijo na *unikernelu* – razširjenem jedru operacijskega sistema, ki že vključuje želeno funkcionalnost, npr. podatkovno bazo; ta kategorija združuje nizke zahteve in majhne režijske stroške kontejnerjev z močno izolacijo virtualnih strojev.

Posamezne komponente v porazdeljenem sistemu želimo upravljati in orkestrirati, za kar morajo slednji zagotavljati ustrezne vmesnike. To je v ogrodju ARCADIA mogoče doseči na dva načina: v prvem je gradnik razvit skladno z ogrodjem in že v osnovi podpira oddaljen nadzor (upravljanje, zbiranje statistike, ipd.), v drugem, ko pa želimo za osnovo mikrostoritve uporabiti obstoječo programsko opremo (npr. odprtokodno podatkovno bazo), pa je potrebno prilagoditev zagotoviti naknadno z uporabo "ovijanja". Ovoj (angl. *wrapper*) predstavlja dodatno programsko opremo, ki poskrbi za sprejemanje ukazov oddaljenega nadzornika in za poročanje stanja, potrebne informacije pa naprej izmenjuje z obstoječo programsko opremo (npr. preko vmesnika HTTP, konfiguracijskih datotek, ipd.).

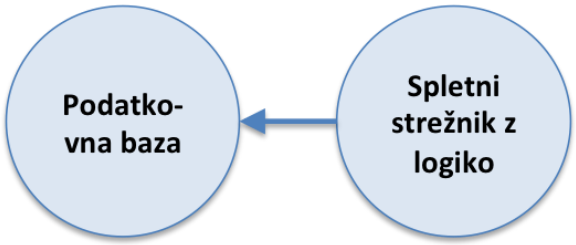
C. Nadzornik ARCADIA

Nadzornik predstavlja možgane sistema za vzpostavitev in orkestracijo porazdeljenih aplikacij. Njegova naloga je ugotovitev in upoštevanje odvisnosti pri vzpostavitvi aplikacije, koordinacija uporabljenih hipervizorjev za zadostitev infrastrukturnih potreb, nastavitev posameznih gradnikov ter spremljanje in prilagajanje njihovega delovanja skozi celoten življenjski cikel aplikacije.

Nadzornik s komponentami komunicira preko programskih vmesnikov (angl. *Application Programming Interface* – API), ki so lahko del komponente same, ali pa jih zagotavlja prilagodilni ovoj. Komunikacija obsega tako nastavitev gradnikov kot tudi zbiranje njihovih metrik, na osnovi katerih lahko administrator aplikacije zagotovi njeno horizontalno ali vertikalno skaliranje.

D. Graf storitve

Graf storitve vsebuje ključne informacije za vzpostavitev HDA; gre za matematičen opis odvisnosti posameznih sistemskih gradnikov, ki poleg potrebnih povezav predpisuje tudi pravilen vrstni red za njihovo postavitev. Primer grafa preproste spletne aplikacije, ki je sestavljena iz 2 gradnikov: podatkovne baze in spletnega strežnika, je prikazan na Slika 1. Graf nakazuje odvisnost programske logike spletnega strežnika od podatkovne baze, kar pomeni, da je pri začetni postavitvi najprej potrebno namestiti in nastaviti instanco podatkovne baze, podatke o njej (IP naslov, uporabniško ime in geslo, ime baze) pa je nato mogoče v naslednjem koraku uporabiti pri konfiguraciji programske logike na spletnem strežniku.



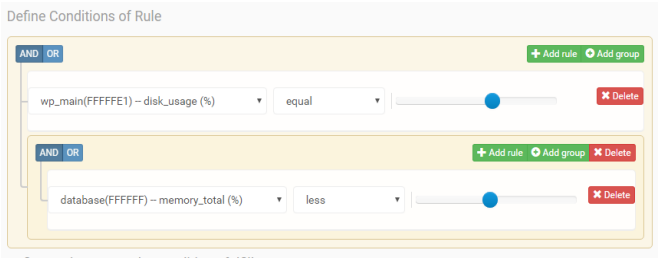
Slika 1: Graf preproste aplikacije spletnega bloga

Pri večjih porazdeljenih aplikacijah, ki temeljijo na več deset mikrostoritvah, lahko postane graf zapleten, ugotavljanje odvisnosti in prenašanje podatkov med vozlišči pa netrivialno. Nadzornik ARCADIA za manipulacijo z grafi in ugotavljanje odvisnosti uporablja funkcionalnosti podatkovne baze neo4j [2].

E. Monitoring in odzivanje na spremembe

Nadzornik v sistemu spremlja vse potrebne statistike posameznih gradnikov porazdeljene aplikacije; sistemske statistike zagotavlja sama virtualizacijska infrastruktura (OpenStack nadzornik); na ta način je mogoče sistematično zbirati podatke o obremenjenosti CPU, razpoložljivem pomnilniku, prostoru na disku, ipd. Drug del statistik se dotika same aplikacije, in jih bodisi zagotavlja sama aplikacija, bodisi njen ovoj. V obeh slednjih primerih so razpoložljive metrike označene na sistematičen način, z uporabo anotacij v programski kodi (angl. *annotations*), kar nadzorniku omogoča, da sam odkrije tako njihova imena kot tudi podatkovne tipe.

Na osnovi monitoringa ključnih metrik infrastrukture in aplikacije je na nadzorniku mogoče definirati pravila, s katerimi vplivamo na delovanje sistema kot celote (vzpostavljanje novih virtualnih instanc VM, povečevanje zmogljivosti obstoječih virov, ipd.). Uporabniški vmesnik za definiranje pravil je prikazan na sliki 3. Preprost primer pravila bi bil: če se obremenitev CPU poveča nad 80 %, poženi novo instanco strežnika.



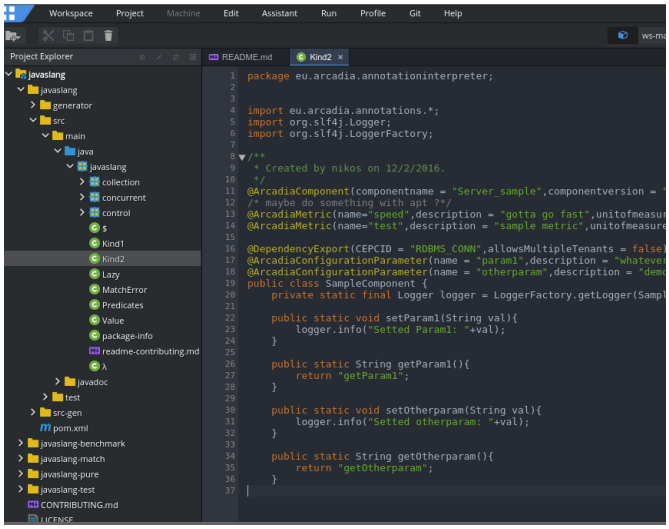
Slika 2: Definiranje pravil (politik) odziva na metrike

F. Razvoj storitev

Ogrodje ARCADIA temelji na programskem jeziku Java, in se poslužuje številnih javanskih konstruktov (npr. anotacije, deklarativna obdelava podatkovnih tokov, ipd.). Posledično zaradi kompatibilnosti tudi razvoj pravih (angl.

native) ARCADIA aplikacij, kot tudi prilagodilnih ovojev, poteka v Javi.

Za razvoj in objavo aplikacij na nadzorniku je predvideno spletno razvojno okolje (angl. *Integrated Development Environment* – IDE), ki temelji na odprtokodnem urejevalniku Eclipse Che.



Slika 3: Spletno razvojno okolje (IDE) za pisanje in objavo porazdeljenih aplikacij

III. PRIMER UPORABE

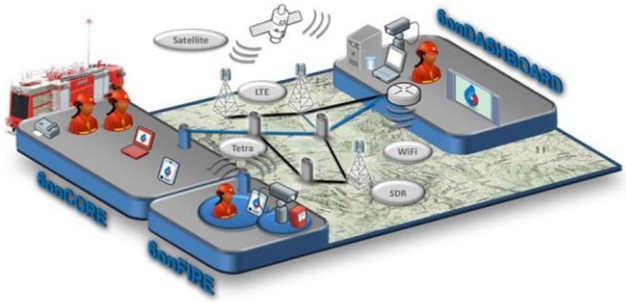
Za prikaz uporabnosti ogrodja ARCADIA v okoljih 5G smo na njegovi osnovi vzpostavili porazdeljeno aplikacijo 6onDASHBOARD, ki predstavlja strežniški del porazdeljenega sistema 6inACTION.

V grobem sistem 6inACTION sestavljajo naslednje komponente:

– 6onCORE – Hrbtenično omrežje, ki terenskim in mobilnim enotam za zaščito in reševanje zagotavlja dostop do taktičnega interneta čez različna namenska, javna ali ad-hoc omrežja (3G, 4G, 5G, satelit, xDSL, optika, WiFi).
– 6onDASHBOARD – Spletna aplikacija, ki nudi programski vmesnik API za povezovanje mobilnih aplikacij ter gosti spletno stran s prikazom splošnega stanja posamezne intervencije (lokacija enot na terenu, stanje senzorjev, prikaz slikovnega in video gradiva s terena ipd.).
– 6onMOBILE – Namenska aplikacija za pametne mobilne terminale, ki nadzornemu centru omogoča spremljanje lokacije uporabnikov (npr. reševalnih enot na terenu), tem pa omogoča sporočanje alarmov, statusnih sporočil in hitrih obvestil o stanju na terenu vključno s slikami in zajetim videom.

Sistem 6inACTION je namenjen predvsem organizacijam in uporabnikom na področju zagotavljanja zaščite in reševanja (angl. *Public Protection and Disaster Relief* – PPDR), razvit je bil v okviru EU projekta GEN6 [3]. Cilj integracije rešitve 6onDASHBOARD v ogrodje ARCADIA je zagotoviti:

– enostavno vzpostavitev operativnega sistema v enem ali več podatkovnih centrih preko grafičnega vmesnika;
– visoko stopnjo razpoložljivosti navkljub izpadom omrežnih in storitvenih elementov v primeru naravnih nesreč,
– horizontalno in vertikalno skaliranje v primeru preobremenitev posameznih aplikacijskih komponent,
– dinamično prilagajanje delovanja porazdeljene aplikacije na osnovi pravil.



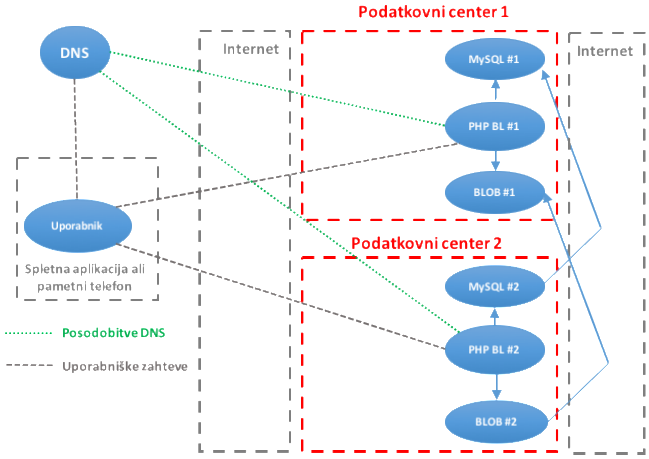
Slika 4: Sistem 6inACTION

A. *Graf storitve*

Integracija aplikacije 6onDASHBOARD v ogrodje ARCADIA zahteva, da aplikacijo razdelimo na več komponent, ki jih nato lahko uporabimo kot osnovo za ovijanje oziroma razvoj programskega agenta za komunikacijo z nadzornikom ARCADIA. Določili smo naslednje storitvene komponente:

– PHP BL (angl. *PHP Business Logic*) – Spletni vmesnik za komunikacijo z uporabniki (API, spletna stran).
– MySQL – Podatkovna baza, ki vsebuje podatke o uporabnikih, alarmih, poročilih, ipd.
– BLOB (angl. *Binary Large Objects*) shramba – Deljena shramba za uporabniške podatke.

Graf storitve z omenjenimi komponentami je prikazan na sliki 5.



Slika 5: Graf storitve 6onDASHBOARD

Vloga in odvisnost storitvenih komponent:

– PHP BL – spletni vmesnik razvit v programskem okolju PHP; za svoje delovanje potrebuje delujočo podatkovno bazo in datotečno shrambo za branje in shranjevanje datotek (npr. slika, video).
– MySQL – strežnik MySQL [4], ki enemu ali več spletnim gradnikom PHP BL nudi storitve podatkovne baze; strežnik dodatno omogoča tudi sinhronizacijo z oddaljeno podatkovno bazo (replikacija).

– BLOB shramba – predstavlja deljeno datotečno shrambo, dostopno preko protokola SAMBA [5]; gradnik dodatno podpira sinhronizacijo datotek z oddaljeno datotečno shrambo.

Uporaba skupne podatkovne baze (MySQL) in deljene datotečne shrambe (BLOB) znotraj istega podatkovnega centra porazdeljeni aplikaciji omogoča, da spletni strežniki (PHP BL) delujejo neodvisno drug od drugega in zato lahko te komponente poljubno dodajamo ali odvzemamo oziroma horizontalno skaliramo.

S tem pa še ne preprečujemo izpada sistema, v kolikor izpade celoten podatkovni center. V ta namen želimo aplikacijo vzpostaviti v dveh podatkovnih centrih, pri čemer lahko ogrodje ARCADIA poskrbi, da sta stanji podatkovnih baz ter deljenih shramb aplikacije 6onDASHBOARD v obeh podatkovnih centrih enaki; to nadzornik doseže z nastavitvijo MySQL replikacije in konfiguracijo datotečne sinhronizacije.

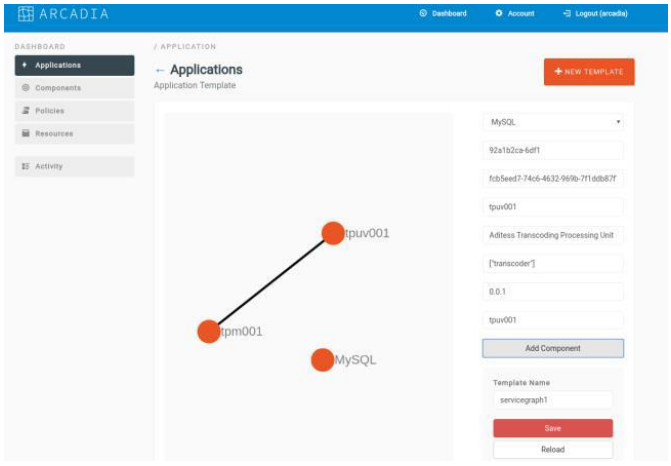
Vsem komponentam moramo tudi določiti njihove konfiguracijske parametre (npr. minimalno število procesorskih enot, količina delovnega pomnilnika ipd.) ter metrike za nadzor in zbiranje statistike (npr. odzivni čas spletne strani, število vnosov v podatkovno bazo na sekundo ipd.).

Omenjene metrike in konfiguracijske parametre uporablja ovoj oziroma agent, ki je razvit ločeno za vsako komponento znotraj porazdeljene aplikacije 6onDASHBOARD, ter omogoča komunikacijo z nadzornikom ARCADIA.

B. *Vzpostavitev in delovanje*

Aplikacijo 6onDASHBOARD vzpostavimo znotraj uporabniškega vmesnika nadzornika ARCADIA. Vzpostavitev zajema naslednje korake:

– izbor vseh potrebnih komponent za vzpostavitev porazdeljene aplikacije,
– določitev virtualizacijskih parametrov posameznih komponent (npr. CPU, RAM ipd.),
– določitev storitvenih parametrov posameznih komponent (npr. uporabniško ime, geslo ipd.),
– določitev omrežnih parametrov posameznih komponent (npr. javni ali zasebni naslov IP),
– umestitev komponent v storitveni graf,
– določitev stopnje porazdeljenosti aplikacije (lokacija komponent je lahko bodisi samodejna, ali pa podatkovni center za vsako komponento določimo ročno).



Sl. 6: Vzpostavitev porazdeljene storitve znotraj grafičnega vmesnika nadzornika ARCADIA [1]

Za dinamično prilagajanje strežniškim obremenitvam (npr. povečano število uporabniških zahtev na spletni strežnik, ki povzroči počasnejše odzivanje, ali pa izpad celotnega podatkovnega centra) nadzornik ARCADIA omogoča pisanje pravil in izvajanje politike v skladu s pravili. Pravila in odzive lahko upravljamo v grafičnem vmesniku nadzornika ARCADIA, pri čemer smo omejeni na sistemske metrike (npr. poraba CPU, RAM) ter na tiste metrike in konfiguracijske parametre, kot jih nudi posamezna komponenta porazdeljene aplikacije.

C. *Testiranje*

V testne namene smo postavili porazdeljeno aplikacijo 6onDASHBOARD v dva ločena podatkovna centra, oba na osnovi platforme OpenStack, ter omogočili sinhronizacijo podatkovnih baz (MySQL) ter deljene shrambe (BLOB shramba) med dvema ločenima podatkovnima centroma. Postavitev omogoča dinamično povečevanje in zmanjševanje števila spletnih strežnikov (PHP BL) ter odzivanje na pravila, določena v nadzorniku ARCADIA.

Na ta način nam dinamično upravljanje sistema omogoča prihranke strežniških virov, saj je ob dobro napisanih pravilih vzpostavljenih optimalno število komponent in njihova zmogljivost. Poleg tega imamo zagotovljeno visoko razpoložljivost celotnega sistema, ki jo je možno povečati, če porazdeljeno aplikacijo namestimo v več podatkovnih centrov.

V kolikor imamo zagotovljen in upravljan tudi sistem za dodeljevanje domenskih imen (angl. *Domain Name System* – DNS), lahko z dinamičnim krmiljenjem vnosov DNS dosežemo, da bo ob vzpostaviti novega spletnega strežnika selitev uporabniške spletne seje na nov strežnik za uporabnika povsem transparentna.

IV. ZAKLJUČEK

V prispevku smo opisali ogrodje ARCADIA, ki naslavlja pomembno nišo v sodobnih okoljih 5G, ki temeljijo na konceptih SDN, NFV ter računalništva v oblaku. Ogrodje omogoča orkestracijo porazdeljenih aplikacij, ki presegajo enega samega ponudnika infrastrukture kot storitve. Ob številnih težavah in izpadih, ki posameznega ponudnika prizadenejo bodisi zaradi človeških ali tehničnih napak, predstavlja takšen sistem elegantno možnost za povečanje razpoložljivosti storitev, ta vidik pa bo igral pomembno vlogo tudi v sistemih pete generacije, če bodo le-ti želeli zadostiti zahtevam najbolj kritičnih aplikacij, kot jih predstavljajo okolja profesionalnih služb in javne varnosti.

ZAHVALA

Projekt ARCADIA je prejel financiranje iz razisko-valnega in inovacijskega programa Obzorje 2020 s strani Evropske unije z oznako GA št. 645372.

LITERATURA

[1] Ogrodje ARCADIA, http://www.arcadia-framework.eu/
[2] Podatkovna baza neo4j, https://neo4j.com
[3] H2020 projekt GEN6, http://www.gen6-project.eu
[4] Podatkovna baza MySQL, https://www.mysql.com
[5] Protokol SAMBA, https://www.samba.org

Urban Sedlar (urban.sedlar@fe.uni-lj.si) je doktoriral leta 2010 na Fakulteti za elektrotehniko, Univerze v Ljubljani. Zaposlen je v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko (LTFE), kjer se ukvarja z raziskavami in razvojem na področju internetnih sistemov in storitev, računalništva v oblaku in sistemi za obdelavo velike količine podatkov.

Luka Koršič (luka.korsic@fe.uni-lj.si) je magistriral leta 2010 na Fakulteti za elektrotehniko, Univerze v Ljubljani. Trenutno je zaposlen v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko (LTFE). Njegova raziskovalna področja obsegajo omrežne sisteme nove generacije ter rešitve za testiranje in verifikacijo omrežnih rešitev.

Mojca Volk (mojca.volk@fe.uni-lj.si) je doktorirala leta 2010 na Fakulteti za elektrotehniko, Univerze v Ljubljani. Zaposlena je v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko (LTFE). Ukvarja se z raziskavami na področju IoT, aplikacijami in storitvami za digitalno zdravje, ter komunikacijskimi sistemi in aplikacijami za potrebe javne varnosti.

Janez Sterle (janez.sterle@fe.uni-lj.si) je magistriral leta 2012 na Fakulteti za elektrotehniko, Univerze v Ljubljani. Zaposlen je v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko (LTFE). Trenutno se ukvarja z raziskavami na področju naslednje generacije mobilnih omrežij ter komunikacijskimi rešitvami in aplikacijami za potrebe javne varnosti.

Povezovanje naprav v heterogenih in zgoščenih komunikacijskih okoljih omrežij 5G

Andrej Hrovat, Carolina Fortuna, Mihael Mohorčič
Odsek za komunikacijske sisteme, Institut Jožef Stefan, Slovenija

Povzetek — Prispevek opisuje izzive povezovanja naprav v omrežja 5G v katerih je potrebno poleg zagotavljanja zmogljivejših komunikacij med in za ljudi zagotavljati tudi komunikacijske storitve med napravami, s čimer je možno uvajati tako imenovane koncepte interneta stvari. Temeljni izzivi povezovanja med napravim in njihovega vključevanja v 5G so v zanesljivosti, zakasnitvi, veliki gostoti naprav in heterogenosti komunikacijskih tehnologij. Za razvoj in testiranje novih algoritmov in protokolov za vzajemno delovanje ter njihovo integracijo v obstoječe in prihajajoče komunikacijske tehnologije je potrebno ustrezno fleksibilno eksperimentalno okolje. V prispevku je predstavljeno tudi eksperimentalno okolje LOG-a-TEC, del evropske iniciative FIRE/FIRE+, ki podpira vrsto kapilarnih tehnologij in standardov ter omogoča testiranje novih algoritmov in protokolov v realnem obratovalnem okolju.

Ključne besede — kapilarna omrežja, celična omrežja 5G, heterogena omrežja, LOG-a-TEC, komunikacija med napravami (MTC)

Abstract — This article describes the challenges of connecting devices to 5G networks that need to provide more efficient utilization of scarce radio spectrum, higher data rates, lower latency and in addition to human centric services and applications support also efficient communications between devices and thus the Internet of Things concept. The main challenges for interconnecting devices and integrating them into 5G represent the required reliability, latency, high density of devices and heterogeneity of communication technologies. Flexible experimental testbeds are inevitable for the development and testing of new algorithms and protocols required for interaction and integration into existing and future communication technologies. This paper presents also the experimental testbed LOG-a-TEC, which is part of the European initiative FIRE/FIRE+ and supports a range of capillary technologies and standards and testing of new algorithms and protocols in real operational environment.

Keywords — capillary networks, cellular 5G networks, heterogeneous networks, LOG-a-TEC testbed, machine type communication (MTC)

I. UVOD

Omrežja 5G bodo morala z vpeljavo vrste novih tehnologij in konceptov poleg zmogljivejših komunikacijskih storitev med in za ljudi zagotavljati tudi podporo komunikacijskim storitvam med napravami (MTC - Machine Type Communication) in s tem omogočiti napovedano množično uvajanje povezanih naprav v okviru koncepta interneta stvari (IoT) ter digitalno preobrazbo gospodarstva in družbe. V segmentu povezovanja med napravami so ključni izzivi omrežij 5G povečanje zanesljivosti zagotavljanja povezav, zmanjšanje zakasnitev, povečanje gostote povezanih naprav in predvsem podpora heterogenim komunikacijskim tehnologijam in standardom ne glede na njihovo skladnost s 3GPP [1]. Za omrežja, ki bodo pokritje celičnega omrežja razširila z uporabo raznoterih tehnologij, primarno razvitih za povezovanje med napravami, se je uveljavilo skupno ime kapilarna omrežja. Ta omrežja, ki se bodo v celična omrežja 5G povezovala preko ustreznih prehodov in bodo v internet povezovala različne naprave, senzorje in aktuatorje, bodo izrazito heterogena tudi glede dinamičnosti in gostote povezanih naprav, predvsem pa bodo občutljiva na porabo energije.

Nova heterogena in močno zgoščena omrežja bodo imela predvsem težave z medsebojno interferenco povezanih naprav. Za prilagoditev na visoko stopnjo pouporabe radijskega spektra skušajo regulatorji vpeljati nova fleksibilna pravila dodeljevanja spektra, zasnovana na konceptih souporabe, priložnostne uporabe in vzajemnega zmanjševanja interference, ter nove standarde [2]. V splošnem pouporabo radijskega spektra zagotovimo s pomočjo časovnega, prostorskega ali frekvenčnega ločevanja. Zlasti v zgoščenih urbanih in poslovnih okoljih ali v visoko avtomatiziranih proizvodnih prostorih mora hkrati komunicirati veliko število naprav, tako da le frekvenčna in prostorska ločitev zagotavljata potrebno pasovno širino vsem uporabnikom. V obeh strategijah je oddajna moč ključni faktor učinkovitosti delitve spektra. Manjša oddajna moč zmanjša tudi območje interference naprave in posledično povečuje možnost prostorske pouporabe frekvence. Poleg tega je nižje ojačenje oddajnika povezano z manjšimi emisijami izven kanala, kar dodatno povečuje možnost uporabe večjega števila kanalov znotraj določenega frekvenčnega pasu. Poleg učinkovitejše izrabe frekvenčnega spektra učinkovit nadzor oddajne moči zmanjšuje porabo energije naprave in posledično povečuje življenjsko dobo baterijsko napajanih naprav.

Za večji izkoristek omejenega radijskega spektra morajo biti končne naprave čim bolj prilagodljive. Prilagodljiv dostop do spektra je pogosto zasnovan na osnovi programirljivega radia (SDR - Software Defined Radio), ki pa se v polni izvedbi v komercialno dostopnih končnih napravah ne uporablja, tudi v prihodnje pa ga zaradi stroškov in porabe energije ni pričakovati v napravah z omejenimi zmogljivostmi kakršne bodo prevladovale pri množičnem uvajanju MTC. S tega vidika imajo običajne komercialno dostopne oddajno-sprejemne enote precejšno prednost, saj v večini primerov podpirajo le omejen oziroma izbran nabor konfiguracij (npr. omejen nabor oddajnih moči in modulacijskih shem).

Za razvoj in testiranje ustreznih postopkov vzajemnega delovanja različnih naprav v heterogenih in zgoščenih komunikacijskih okoljih omrežij 5G je potrebno vzpostaviti čim bolj reprezentativna eksperimentalna okolja s podporo celičnim in kapilarnim omrežjem. Eno takih okolij

predstavlja eksperimentalno omrežje LOG-a-TEC, ki je preko evropske iniciative FIRE/FIRE+ vključeno v federacijo testnih omrežij Fed4FIRE in na voljo za izvajanje eksperimentov širši raziskovalni skupnosti.

V tem prispevku na kratko orišemo glavne izzive obsežnih IoT omrežij za celična in necelična, t.j. kapilarna omrežja 5G, predstavimo pomen eksperimentalnih okolij za razvoj in testiranje različnih postopkov delovanja naprav v heterogenih in zgoščenih komunikacijskih okoljih omrežij 5G, izpostavimo nekaj funkcionalnosti, ki jih morajo takšna eksperimentalna okolja podpirati, nato pa podrobneje predstavimo eksperimentalno okolje LOG-a-TEC in tipe eksperimentov, ki jih lahko v tem okolju izvedemo v smislu preučevanja naprav v heterogenih in zgoščenih komunikacijskih okoljih.

II. IZZIVI OBSEŽNIH OMREŽIJ IOT

Osnovni izzivi povezovanja heterogenih naprav z namenom vzpostavljanja obsežnih omrežij IoT so predvsem cena posamezne naprave, življenjska doba baterij, zagotavljanje pokritja (notranja okolja, regionalno, globalno), razširljivost omrežij in podpora različnim primerom uporabe. Povezljivost med napravami in tip dostopa sta močno odvisna od vrste aplikacije. Veliko naprav izrablja radijske tehnologije, ki delujejo v nelicenčnem frekvenčnem spektru. Nekatere so namenjene komunikacijam kratkega dosega z omejenimi varnostnimi ter QoS zahtevami in so uporabne predvsem za domača notranja okolja, nekatere pa tudi za komunikacije z daljšim dosegom. Za aplikacije IoT, ki potrebujejo pokritje večjega področja (mesto, regija, država,…), obstajata dve alternativi, in sicer rešitve v licenčnih celičnih radijskih pasovih in v nelicenčnih radijskih pasovih.

V prvo skupino sodijo rešitve, ki uporabljajo celična omrežja v licenčnih radijskih pasovih, primarno namenjena visoko kvalitetnim glasovnim in podatkovnim storitvam. V zadnjem času se namreč hitro razvijajo dodatne celične rešitve za prostrano pokrivanje z nizkimi močmi (Low Power Wide Area, LPWA), in v 3GPP Rel.13 (2016) so specificirali več različnih tehnologij LPWA; EC-GSM-IoT (Extended Coverage GSM IoT), eMTC (LTE Cat. M1 oziroma LTE za machine-type communication) in NB-IoT (NarrowBand IoT). Predvsem tehnologija NB-IoT predstavlja obetavno rešitev za obsežna omrežja IoT. Izrablja pasovno širino 180 kHZ, podpira več kot 200.000 naročnikov, je implementirana programsko na omrežnem nivoju v obstoječem omrežju LTE, omogoča razširjeno pokritje (20 dB) in močno podaljša življenjsko dobo baterij (do 10 let). NB-IoT je načrtovana za kompaktno integracijo in vzajemno delovanje z LTE, kar omogoča veliko fleksibilnost namestitve. Frekvenčni nosilec je lahko umeščen v varnostni pas med kanali LTE, v običajni kanal LTE ali kot samostojni nosilec v pasu GSM. Poleg tega v primerjavi z eMTC močno zmanjšuje kompleksnost naprav, ki je primerljiva s kompleksnostjo nelicenčnih tehnologij LPWA.

V drugo skupino spadajo tehnologije LPWA, kot na primer SigFox, LoRa, Ingenu in druge, ki delujejo v nelicenčnih radijskih pasovih. Načrtovane so namensko za aplikacije MTC in so prilagojene za zelo nizko porabo energije in nizke oziroma omejene zahteve za pretok, zanesljivost in QoS.

Celične tehnologije LPWA imajo vsekakor ključno vlogo pri razvoju in razširjanju IoT, predvsem pa so primerne za aplikacije, ki zahtevajo globalno pokritje (npr. sledenje tovoru). Povsod prisotna celična omrežja zagotavljajo omrežjem IoT pouporabo funkcionalnosti dostopovnih omrežij kot so varnost, upravljanje omrežja, QoS in globalno povezljivost ne da bi imele končne naprave te funkcionalnosti dejansko vgrajene. Seveda te tehnologije zahtevajo nadgradnjo obstoječih celičnih omrežij, rešitve pa so stroškovno vezane na poslovne modele operaterjev mobilnih omrežij. Z nadaljnjo digitalno preobrazbo gospodarstva in družbe te tehnologije tudi ne bodo zagotavljale zadostne zmogljivosti z vidika sočasno povezanih naprav, zato se v omrežjih 5G predvideva sobivanje s kapilarnimi omrežji za bolj omejeno povezljivost ogromnega števila naprav. Kapilarna omrežja temeljijo na komunikacijskih tehnologijah kratkega dosega ter na tehnologijah LPWA, in za dostop do celičnega ali kateregakoli drugega dostopovnega omrežja uporabljajo ustrezne omrežne prehode. Ti preko zalednih omrežij zagotavljajo povezljivost v oblak, kjer je implementirano shranjevanje podatkov, obdelava in upravljanje.

III. BREZŽIČNA EKSPERIMENTALNA OKOLJA

V okviru evropske iniciative FIRE/FIRE+ in ameriške iniciative GENI je na voljo vrsta različnih eksperimentalnih okolij [3][4], med katerimi so tudi okolja za eksperimentiranje z rešitvami za omrežja 5G, senzorska omrežja in kapilarna omrežja. Radijske platforme v eksperimentalnih okoljih lahko razdelimo na platforme SDR in tehnološko specifične rešitve. Najpogosteje uporabljene platforme SDR temeljijo na univerzalnem programskem radiju (USRP – Universal Software Radio Peripheral), medtem ko tehnološko specifične rešitve uporabljajo na trgu dostopne vmesnike IEEE 802.11 WLAN, IEEE 802.15.1 (Bluetooth) in IEEE 802.15.4 PAN ter opremo LTE različnih proizvajalcev.

Za brezžična eksperimentalna okolja je zelo pomembno poznavanje radijskega okolja v času izvajanja eksperimentov, kar v različnih omrežjih rešujejo na različne načine. Zaznavanje spektra s tehnološko specifičnimi rešitvami je razmeroma omejeno z že vgrajenimi funkcionalnosti s strani proizvajalca (merjenje RSSI). Implementacija naprednejših pristopov, kot so na primer detekcija na osnovi kovariančnih metod, detekcija na osnovi metode lastnih vrednosti in ciklično-stacionarna detekcija, je na vgrajenih napravah s komercialnimi radijskimi moduli izjemno zahtevna ali celo nemogoča. Eksperimentalno okolje LOG-a-TEC omogoča dostop do algoritmov za zaznavanja spektra tudi na vgrajenih napravah. Rešitev omogoča dostop do algoritma za zaznavanje spektra preko lokalnega vmesnika z uporabo lokalnega radijskega sprejemnika (npr. SNE-ESHTER). Poleg tega je preko oddaljenega vmesnika in obdelave v oblaku omogočen dostop tudi do ostalih oddaljenih vgrajenih naprav.

Poleg poznavanja radijskega okolja je za ponovljivost eksperimentov v testnih omrežjih potrebno zagotoviti primerljive razmere z ustreznimi generatorji signalov. Ker omogočajo platforme SDR oddajo poljubnih signalov velikih pasovnih širin, so v splošnem primerne za simuliranje interference. Vendar pa obstaja le nekaj primerov testnih omrežij, kjer so na voljo vnaprej konfigurirani programski

moduli SDR, ki zagotavljajo profil signala običajnih motilcev. Tehnološko specifične vgrajene naprave pa so omejene na oddajo signalov, ki so značilne za fizične nivoje implementiranih komunikacijskih protokolov in običajno niso uporabne za simuliranje motilnih signalov drugih tehnologij. Eksperimentalno omrežje LOG-a-TEC zagotavlja nadzorovano generiranje interference z uporabo oddajno-sprejemnih radijev CC2500 in CC1101, nameščenih na nizkocenovnih vgrajenih napravah. Za oddajni profil različnih motilcev v frekvenčnih pasovih, ki se običajno uporabljajo v testnem omrežju LOG-a-TEC, že obstajajo vnaprej razviti programski moduli. Na primer, na voljo sta oddajna profila mikrofona v frekvenčnem pasu UHF in mikrovalovne pečice v pasu 2.4 GHz (ISM).

Za mnoge eksperimente v brezžičnem okolju je izrednega pomena tudi poznavanje razmer na posamezni brezžični povezavi. Rezultati različnih postopkov za oceno kvalitete povezave (LQE – Link Quality Estimation) večinoma temeljijo na simulacijah in le redki postopki so bili implementirani na dejanski strojni opremi, kot na primer USRP ali s Contiki skladnimi vozlišči WSN. Testno omrežje LOG-a-TEC omogoča ocenjevanje LQE z zagotavljanjem obstoječih in naprednih postopkov za LQE, kot tudi programskih modulov za oceno in klasifikacijo povezav. Moduli presegajo trenutne obstoječe rešitve predvsem z vidika uporabljenih algoritmov (sprotno strojno učenje) in njihovih vhodnih lastnosti.

IV. EKSPERIMENTALNO OKOLJE LOG-A-TEC

Eksperimentalno okolje LOG-a-TEC vključuje radijske tehnologije kot so: LoRa, SigFox, IEEE 802.15.4a, IEEE 802.15.4, ZigBee, TVWS in tehnologije za implementacijo lastnih protokolnih skladov. Ta izbor tehnologij omogoča eksperimente IoT, MTC in kapilarne 5G. Poleg tega je eksperimentalno omrežje komplementarno z obstoječimi testnimi omrežji v Fed4FIRE/Fed4FIRE+, saj namensko razvito vozlišče podpira štiri različne brezžične tehnologije in osem vrst brezžičnih oddajno-sprejemnih enot. V sklopu eksperimentalnega omrežja je razvita tudi programska oprema za lokalizacijo, generiranje nadzorovanega šuma in signalov, napredno zaznavanje spektra, napredno ocenjevanje kvalitete povezave ter podpora za sestavljanje in dinamično preoblikovanje protokolnega sklada. Tabela 1 povzema vse ključne gradnike in funkcionalnosti treh generacij omrežja LOG-a-TEC. Omenjeni elementi omogočajo izvajanje novih, naprednih eksperimentov, kot so:

– preučevanje algoritmov za radijsko lokalizacijo,
– natančnejše zaznavanje spektra potrebno za dinamičen dostop do spektra,
– nadzor interference in generiranje heterogenih signalov, ki je pomembno za primerjanje natančnosti tehnik zaznavanja spektra in prediktorje kvalitete povezave,
– razvoj in ocena novih ali prirejenih protokolov MAC, ki niso skladni z IEEE 802.15.4 in njihovo vrednotenje z MAC komponentami IEEE 802.15.4,
– samostojna ocena zmogljivosti klasifikatorjev in prediktorjev kvalitete povezave in njihovo vrednotenje z standardiziranimi več-skokovnimi protokoli usmerjanja.

LOG-a-TEC uporablja visokonivojski programski vmesnik, ki uporabniku abstrahira detajle povezane s strojno opremo. Vmesnik je implementiran z uporabo pristopa Representational State Transfer (REST) [5] in omogoča, da uporabniški eksperimenti za zaznavanje spektra, lokalizacijo in dostopa do medija vzajemno delujejo s testnim okoljem preko zahtev HTTP in oblike RESTful [6][7]. Testno okolje LOG-a-TEC 1.0 je vključeno v projekt Fed4FIRE+ in je popolnoma združljivo s preostalimi brezžičnimi testnimi omrežji (npr. w.iLab.t, Iris) [3]. Naslednja generacija omrežja, LOG-a-TEC 2.0, omogoča oddaljeni nadzor testnega omrežja preko vmesnika, ki temelji na protokolu CoAP (Constrained Application Protocol) [8]. Vključuje tudi dodatne programske module, ki omogočajo eksperimente za prilagodljivo omreženje vključno s prilagajanjem usmerjanja na osnovi obremenitve in topologije [9][10]. LOG-a-TEC 2.0 vsebuje dva ločena brezžična vmesnika, prvega za izvajanje eksperimentov in drugega za nadzor in upravljanje omrežja. LOG-a-TEC 3.0 že obstoječim oddajno-sprejemnim enotam dodaja tehnologije MTC v ustreznih frekvenčnih pasovih (UWB 3.5-6.5 GHz, LoRa 868 MHz, SigFox 868 MHz).

V testnem omrežju LOG-a-TEC je za fiksne in prenosne eksperimente na voljo več različnih funkcionalnosti:

1. Različne radijske tehnologije: LoRa, Sigfox, IEEE 802.15.4a, zaznavanje spektra v TVWS in radio za implementacijo lastnih protokolnih skladov. Z razpoložljivimi tehnologijami je možno, poleg tradicionalnih IoT in celičnih 5G eksperimentov, izvajati tudi kapilarne eksperimente 5G/MTC.

   Naštete tehnologije so podprte s sledečimi oddajno-sprejemnimi enotami:

   – SNN-S272 (Semtech SX-1272) omogoča preizkušanje komunikacije dolgega dosega z nizkimi močmi (LoRa).
   – Bazna postaja SigFox s testnimi napravami za eksperimentiranje komunikacij dolgega dosega z nizkimi oddajnimi močmi in za ultra ozke pasovne širine LPWAN UNB.
   – SNPN-UWB (DWM1000 UWB) za komunikacijske eksperimente kratkega dosega in za ultra široke pasove.
   – SNE-ESHTER (NXP TDA18219HN 470-862 MHz) omogoča napredno zaznavanje spektra z uporabo kovariančnih metod v sub-GHz-pasu.
   – SNE-ISMTV-TI868 (TI CC1101) in SNE-ISMTV-TI24 (TI CC2500) omogočata implementacijo enostavnih in učinkovitih protokolov v frekvenčnih pasovih 2.4 GHz in sub-GHz, ki ne temeljijo na IEEE 802.15.4, ter podpirajo funkciji zaznavanje spektra in generiranja signala/interference.

2. Opisane radijske tehnologije omogočajo izvajanje eksperimentov v različnih frekvenčnih pasovih: 470-862 MHz, 860-1000 MHz in 3,5-6,5 GHz
3. Razpoložljive programske funkcionalnosti: klasifikacija LOS/nLOS, generatorji motilnih signalov, interference in šuma, napredno zaznavanje spektra z algoritmi na osnovi kovariančnih metod, vgrajeni LQE in prediktorji kvalitete povezave, programska oprema za klasifikacijo kvalitete povezave, CRime in konceptualna struktura ProtoStack za načrtovanje lastnih protokolnih skladov.

A. Napredni programski moduli

V okviru testnega omrežja je na voljo več različnih naprednih programskih modulov.

Programski modul za generiranja nadzorovane interference in šuma: Generiranje šuma je uporabno predvsem za testiranje odpornosti zgornjih omrežnih nivojev na izgubo paketov. To je možno ponazoriti z izpuščanjem

	LOG-a-TEC 1.0	LOG-a-TEC 2.0	LOG-a-TEC 3.0
brezžične funkcionalnosti	prilagodljivo in napredno zaznavanje spektra in funkcija generiranja signalov v sub-GHz pasu	eksperimenti na nivoju paketov, načrtovanje lastnih protokolov, sestavljivi in modularni protokolni skladi, prilagodljivo in napredno zaznavanje spektra in funkcija generiranja signala v sub-GHz pasu	eksperimenti s tehnologijami ultra ozkega in ultra širokega pasa, eksperimenti na nivoju paketov, načrtovanje »clean slate« protokolov, sestavljivi in modularni protokolni skladi, prilagodljivo in napredno zaznavanje spektra in funkcija generiranja signala v sub-GHz pasu
brezžične tehnologije	TVWS, prilagodljivi ne-IEEE 802.15.4, IEEE 802.15.4	TVWS, prilagodljivi ne-IEEE 802.15.4, IEEE 802.15.4	LoRa, Sigfox, IEEE 802.15.4a, TVWS, prilagodljivi ne-IEEE 802.15.4, IEEE 802.15.4
frekvenčni pasovi	470-862 MHz, 868MHz, 2,4GHz	470-862 MHz, 868MHz, 2,4GHz	860-1000MHz, 3.5 GHz to 6.5 GHz, 470-862 MHz, 868MHz, 2.4GHz
razširitveni radijski moduli za platformo VESNA	SNE-ISMTV-UHF (NXP TDA18219HN), SNE-ISMTV-TI868 (TI CC1101 in Atmel AT86RF212), SNE-ISMTV-TI24 (TI CC2500 in Atmel AT86RF231)	SNE-ISMTV-TI868 (TI CC1101 868MHz in Atmel AT86RF212), SNE-ISMTV-TI24 (TI CC2500 2.4 GHz in Atmel AT86RF231)	SNN-S272 (Semtech SX-1272), SNPN-UWB (DWM1000 UWB), SNE-ESHTER (NXP TDA18219HN 470-862 MHz), SNE-ISMTV-TI868 (TI CC1101, Atmel AT86RF212), SNE-ISMTV-TI24 (TI CC2500, Atmel AT86RF231)
programske komponente in moduli	zaznavanje spektra z detekcijo energije, generiranje signalov vključno z profilom brezžičnega mikrofona, dinamično alociranje oddajne moči s pristopom teorije iger	protokolni skladi po meri, zaznavanje spektra z detekcijo energije in kovariančnimi metodami, generiranje signalov vključno z profilom brezžičnega mikrofona, dinamično alociranje oddajne moči s pristopom teorije iger	Lokalizacija v zaprtih prostorih in zunanjem okolju, LOS/nLOS klasifikacija kanala, klasifikacija in predikcija kvalitete povezave, protokolni skladi po meri, zaznavanje spektra z detekcijo energije in kovariančnimi metodami, generiranje signalov vključno z profilom brezžičnega mikrofona, dinamično alociranje oddajne moči s pristopom teorije iger, …
HW platforma	VESNA 1.0	VESNA 1.0	VESNA 1.0 in VESNA 2.0
operacijski sistem	po meri	Contiki, po meri	Linux, Contiki, po meri
oddaljeni dostop	oddaljen nadzor, rekonfiguracija in eksperimentiranje preko http		

Tabela 1: Razpoložljivo eksperimentalno testno okolje

paketov, ki sledi določeni porazdelitvi (npr.: Poisson). Vendar pa je generiranje nadzorovane interference veliko bolj realen pristop. S programskim modulom za generiranje šuma lahko eksperimentatorji z radijem TI CC1101 kontrolirano generirajo signal brezžičnega mikrofona, medtem ko radijski vmesnik TI CC2500 omogoča generiranje interference tipa mikrovalovne pečice. Na podlagi meritev bo razvit tudi ustrezen modul za simuliranje interference brezžičnega telefona.

Programski modul za napredno zaznavanje spektra: Večina vgrajenih radijskih oddajno-sprejemnih enot lahko zaznava samo energijo. V primeru omrežja LOG-a-TEC, omogoča vozlišče VESNA z razširitvijo SNE-ESHTER napredno zaznavanje spektra s kovariančnimi metodami (CAV, CFN, MAC, itd), ki tečejo na samem vozlišču [10]. V primeru, da je vozlišče žično povezano v internet, omogoča s kombinacijo obdelave na samem vozlišču in v oblaku izvajanje detekcije na osnovi lastnih vrednosti in ciklično-stacionarno detekcijo. S predhodno opisanimi pristopi je napredno zaznavanje spektra mogoče v frekvenčnem pasu med 470 MHz in 900 MHz.

Programski moduli za napredno ocenjevanje kvalitete povezav (LQE), predikcijo in klasifikacijo: V različici LOG-a-TEC 2.0 je trenutno implementirana osnovna strojna in programska oprema LQE in predikcija preko knjižnice CRime [9]. Poleg tega je implementiran tudi estimator WMEWMA, on-line prediktor linearne regresije in algoritmi

za klasifikacijo povezav. Eksperimentatorji lahko ocenijo različne izvedenke in konfiguracije LQE-jev.

Oddaljeno sestavljanje protokolnih skladov z različnimi funkcionalnostmi in konfiguracijami usmerjevalnih tabel: LOG-a-TEC 2.0 omogoča oddaljeno konfiguriranje modulov uporabljenih v eksperimentih z enostavnimi konfiguracijskimi sporočili in ne s pošiljanjem binarne kode samim vozliščem. Na primer, s sporočilom Javascript Object Notation (JSON) se vozlišču pove ime modula LQE/LQP, ki se naj uporabi v eksperimentu. Usmerjevalni protokoli nato uporabijo LQE/LQP, da iz usmerjevalne tabele določijo ceno povezave. Medtem ko so lahko v večini primerov usmerjevalne odločitve na osnovi topologije in obremenitve porazdeljene in vgrajene, obstajajo primeri ko so na osnovi informacij naprednega zaznavanja spektra izračunane centralno v oblaku in šele nato konfigurirane v usmerjevalno tabelo.

V. PODPRTI TIPI EKSPERIMENTOV V HETEROGENIH IN ZGOŠČENIH KOMUNIKACIJSKIH OKOLJIH

Testno omrežje LOG-a-TEC omogoča izvajanje vrste specifičnih eksperimentov za preučevanje delovanja zgoščenih omrežij IoT in MTC v okviru kapilarnih omrežij 5G:

1. Izvajanje eksperimentov s heterogenimi MTC brezžičnimi tehnologijami (LoRa, Sigfox, IEEE 802.15.4a, TVWS, ne-IEEE 802.15.4, IEEE 802.15.4) - oddajanje, sprejemanje in zaznavanje ob istem času na isti lokaciji.
2. Istočasno izvajanje eksperimentov na isti lokaciji z naprednimi funkcionalnostmi kot so ozkopasovni in širokopasovni eksperimenti na nivoju paketov, načrtovanje lastnih sestavljivih in modularnih protokolnih skladov, funkcije prilagodljivega in naprednega zaznavanja spektra in generiranja signalov v sub-GHz spektru.
3. Uporaba naprednih programskih komponent, ki omogočajo lokalizacijo, klasifikacijo LOS/nLOS, oceno kvalitete povezave, klasifikacijo povezave in predikcijo kvalitete povezave, razvoj novih protokolnih skladov, zaznavanje spektra z detekcijo energije in kovariančnimi metodami, generiranje signalov, alociranje moči s pristopom teorije iger.
4. Eksperimenti z natančnejšimi informacijami o spektru. Gradnja natančnejše podatkovne baze zasedenosti spektra, ki poleg modeliranja razširjanja radijskih signalov upošteva tudi podatke porazdeljenega zaznavanja. Trenutna dostopovna politika TVWS, ki temelji na geolokalnih podatkovnih bazah (Ofcom, UK), ne upošteva motenj med sekundarnimi uporabniki. Torej je uporaba informacij zaznavanja spektra za zmanjšanje interference in povečanje kvalitete storitev zanimiva tako za storitve v pasu TVWS kot tudi za storitve v nelicenčnem ISM pasu.
5. Generiranje nadzorovane interference je pomembno predvsem za ocenjevanje in primerjanje algoritmov za zaznavanje spektra. Uporaba nadzorovane interference omogoča ponovno reproduciranje eksperimentov in ocenitev interferenčno specifičnih zmogljivosti različnih višje nivojskih protokolov in LQE-jev. Funkcionalnost je praktično uporabna za katerikoli tip eksperimenta.
6. Razvoj novih ali prilagoditev obstoječih protokolov MAC. Preko razpoložljivih rekonfigurabilnih oddajno-sprejemnih enot, ki niso omejene na standard IEEE 802.15.4, in programskega modula CRime je možno razviti in preizkusiti novo tehnologijo MAC. To je izjemnega pomena predvsem pri pojavu novih tehnologij IoT, ki ne sledijo standardu IEEE 802.15.4, kot na primer LoRa in SigFox.
7. Ovrednotenje ne-IEEE 802.15.4 MAC komponent s komponentami IEEE 802.15.4 MAC.

VI. ZAKLJUČEK

Z intenzivnejšim uvajanjem koncepta interneta stvari, razvojem avtonomnih vozil in v splošnem digitalno preobrazbo gospodarstva in družbe, dobiva komunikacija med napravami v okviru omrežij 5G precej večjo pozornost, kot v mobilnih omrežjih prejšnjih generacij, pri čemer za povezovanje naprav izkorišča tako celične kot kapilarne tehnologije. Za posamezna področja uporabe je seveda treba ustrezno rešiti vrsto izzivov povezovanja naprav, od ustrezne zanesljivosti in zakasnitev do problematike delovanja naprav v komunikacijsko zelo zgoščenih okoljih, delovanja pri nizkih oddajnih močeh na velike razdalje ter vzajemnega delovanja heterogenih tehnologij. Reševanje teh izzivov poleg teoretičnega in simulacijskega pristopa zahteva tudi testiranje v kar se da realnih obratovalnih razmerah. V ta namen so posamezni proizvajalci komunikacijske opreme, predvsem pa raziskovalne inštitucije, postavili vrsto različnih eksperimentalnih okolij in nekatera tudi začeli povezovati v t.i. federacije eksperimentalnih omrežij. Ena teh federacij, Fed4FIRE, ki je podprta tudi s strani Evropske komisije, omogoča eksperimente na področjih interneta naslednje generacije in omrežij 5G, vanjo pa je vključeno tudi eksperimentalno omrežje LOG-a-TEC. Slednje je predvsem osredotočeno na eksperimentiranje s kapilarnimi tehnologijami in komunikacijo med napravami v nelicenčnih frekvenčnih pasovih.

ZAHVALE

Raziskovanje na področju omrežij 5G delno sofinancira Javna agencija za raziskovalno dejavnost Republike Slovenije preko raziskovalnega programa »P2-0016 Komunikacijska omrežja in storitve«.

LITERATURA

[1] Condoluci, M., Dohler, M., Araniti, G., Molinaro, A., & Zheng, K. (2015). Toward 5G densenets: architectural advances for effective machine-type communications over femtocells. *IEEE Communications Magazine*, *53*(1), 134-141.

[2] Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T., & Ladid, L. (2016). Internet of things in the 5G era: Enablers, architecture, and business models. *IEEE Journal on Selected Areas in Communications*, *34*(3), 510-527.

[3] Fed4Fire+ - Federation for Future Internet Research and Experiments, https://www.fed4fire.eu/,

[4] GENI – Global Environment for Network Innovations http://www.geni.net/,

[5] Šolc, T., Fortuna, C., Mohorcic, M. "Low-cost testbed development and its applications in cognitive radio prototyping." Cognitive Radio and Networking for Heterogeneous Wireless Networks. Springer Int. Publishing, 2015. 361-405.

[6] Anton, C., Toma, A., Cremene, L., Mohorcic, M., Fortuna, C. "Power allocation game for interference mitigation in a real-world experimental testbed." In Communications (ICC), 2014 IEEE International Conference on (pp. 1495-1501)

[7] Dionísio, R., et al. "Combination of a geolocation database access with infrastructure sensing in TV bands." EURASIP Journal on Wireless Communications and Networking 2014.1 (2014): 1-14.
[8] Bekan, A., Mohorcic, M., Činkelj, J., Fortuna, C. "An architecture for fully reconfigurable plug-and-play wireless sensor network testbed." IEEE GLOBECOM 2015: connecting all through communications, 6-10 Dec 2015, San Diego, USA, 7.
[9] Fortuna, C., Mohorčič, M. "A framework for dynamic composition of communication services." ACM transactions on sensor networks, 2015, vol. 11, no. 2, doi: 10.1145/2678216.
[10] Šolc, Tomaž, "Spectrogram of the received signal strength (RSSI) in a 1 MHz wide channel for frequencies between 470 MHz and 900 MHz detection of narrowband transmissions using maximum autocorrelation detector.", http://log-a-tec.eu/bokeh/vss-05-jsi-c-building/

Andrej Hrovat je na Odseku za komunikacijske sisteme Inštituta Jožef Stefan zaposlen od leta 2004, v zadnjem obdobju na mestu znanstvenega sodelavca. Poleg tega je tudi asistent na Mednarodni podiplomski šoli Jožefa Stefana. Diplomiral in magistriral je leta 2004 oziroma 2008 na Fakulteti za elektrotehniko v Ljubljani. Leta 2011 je doktoriral na Mednarodni podiplomski šoli Jožefa Stefana. Sodeluje pri različnih mednarodnih in domačih raziskovalnih in aplikativnih projektih povezanih s profesionalnimi mobilnimi komunikacijskimi sistemi, 2/3/4/5G, tehnologijami WiFi in WiMAX, satelitskimi in senzorskimi omrežji.

Carolina Fortuna je diplomirala (2006) na Technical University of Cluj-Napoca in doktorirala na Mednarodni podiplomski šoli Jožefa Stefana (2013). Zaposlena je na Odseku za komunikacijske sisteme Instituta Jožef Stefan kot znanstvena sodelavka, od leta 2014 pa je tudi asistentka na Mednarodni podiplomski šoli Jožefa Stefana. Raziskovalno se ukvarja z reševanjem komunikacijskih problemov na omrežnem nivoju kot je izbira dostopovnega omrežja in upravljanja omrežja z uporabo aktualnih tehnik strojnega učenja in semantike. Raziskuje uporabnost fleksibilnih omrežnih arhitektur v napravah z omejenimi zmogljivostmi na različnih področjih uporabe Interneta stvari.

Mihael Mohorčič je diplomiral (1994), magistriral (1998) in doktoriral (2002) na Fakulteti za elektrotehniko Univerze v Ljubljani. Zaposlen je na Institutu Jožef Stefan kot znanstveni svetnik in vodja Odseka za komunikacijske sisteme, na Mednarodni podiplomski šoli Jožefa Stefana pa je izvoljen v naziv izrednega profesorja. V zadnjem času se raziskovalno ukvarja predvsem z obsežnimi brezžičnimi senzorskimi omrežji, s heterogenimi, kognitivnimi in elastičnimi radijskimi omrežji ter s pametnimi energetskimi omrežji, pri čemer sodeluje na vrsti mednarodnih in domačih projektov.

The strategic research and innovation agenda for pervasive mobile virtual services

Felipe Gil-Castiñeira; Francisco J. González-Castaño, University of Vigo, Spain

Abstract — The European Union has promoted the creation of Technology Platforms (ETP) as industry-led fora to develop research and innovation agendas and roadmaps that should be supported by private and public funding. One of the main roles of ETPs is the development of industry-focused Strategic Research and Innovation Agendas (SRIAs). This paper presents a summary about the most relevant challenges and proposals collected in a recent SRIA published by the Networld 2020 ETP for Pervasive Mobile Virtual Services in 5G, such as Virtualized Networks and Services or new schemes for Radio Networks.

Keywords — 5G, SRIA, Mobile Services, Virtualisation.

I. INTRODUCTION

As indicated in the SRIA [1], in 5G and beyond networks, the first fundamental change is the availability of processing and storage as core services provided by the network itself. Therefore, the proposal is akin to the classic paradigm of distributed computing. The definition of a reference architecture for next generation networks is challenging due to the required Key Performance Indicators (KPIs), which go from the transport of massive volume of data, to the capacity to connect trillions of devices, namely:

- 1000 times higher mobile data volume per geographical area,
- 10 to 100 times more connected devices,
- 10 to 100 times higher typical user data rate,
- 10 times lower energy consumption,
- End-to-End latency < 5ms,
- Location precision < 3m,
- Mobile speed up to 500 km/h,
- Ubiquitous 5G access including low population density areas.

Beyond 5G, the SRIA pursues a next generation network comprising new virtualisation techniques, especially focused on network functions; and spectrum unleashing new radio and optical bands. The new paradigm bringing new opportunities to verticals like automotive, industry 4.0, entertainment, energy and e-health, is termed Pervasive Mobile Virtual Services.

The paradigm entails a much more complex service model than just transporting packets end to end, and will have a strong influence on telcos. Technologies such as cloud computing and mobile edge computing (MEC) will have a deep impact, interleaved with network function virtualization (NFV) and software defined networks (SDN) and assisted by them. A second fundamental change is the explosion of internet of things (IoT) involving machine to machine (M2M) communications. IoT will comprise a much larger number of terminals with a broader range of requirements than human data communications. The IoT needs new network control solutions that can effectively handle the authentication, naming, addressing, routing and related functions for such an unprecedented number of terminals. Radio systems will have to provide solutions to accommodate very low traffic and low energy terminals as well as high capacity ones.

A huge increase of corporate customers is also expected. They will subscribe combined transport and computing services under complex SLAs.

Summarizing, the SRIA document in Pervasive Mobile Virtual Services identifies challenges and opportunities in four research areas:

- Virtualised Networks and Services.
- Radio Networks and Signal Processing.
- Optical Networks.
- Experimentation with Verticals.

II. NETWORK SERVICES VIRTUALISATION

Network services virtualisation tackles several aspects. First of all, it is important to review the traditional concept of domain, largely identified as an administrative concept in communication networks. Software networks will allow a higher degree of flexibility where multiple domains may exist at the same time across different dimensions. On the other hand, such software networks will allow the deployment of hierarchical multitenancy, where network providers may offer their (virtual) resources to other network providers, which can follow the same approach towards other network providers. To this end, it is necessary to extend the ETSI NFV MANO architecture to enable recursive deployments of functional components for multitenancy.

Virtualisation on low-cost resource-constrained networks devices is a challenging task, so it is also important to adopt light virtualisation environments like containers and unikernels, for example.

With such heterogeneous infrastructure, it is important to provide mechanisms to simplify network configuration, towards some sort of self-configuration. For example, in ultra-dense deployments, mobility management is challenging due to the frequent handovers when equipment moves across successive small cells. Interference coordination for overlapping small cells has to be thus considered. In such ultra-dense scenarios, subscribing access to network providers on demand is still far from feasible. Last but not least, in a virtualised network environment, Security should be considered an integral component of the architecture. For instance, in order to prevent any tenants from accessing the information of other tenants.

III. RADIO NETWORKS AND SIGNAL PROCESSING

The number of connected devices is increasing from the current ca. 10 billion to an estimated 20-fold within the next five years. In addition, networks should satisfy customers' diverse needs in terms of traffic types and required bandwidth, which will be usually provided by multi-service networks that will share physical resources.

Advanced terminals (such as end-user terminals or vehicles) can provide connectivity to other devices or take advantage of multi-hop device-to-device (D2D) communications. If the network controls their communication interfaces the overall performance would be improved.

To satisfy the spectrum requirements to fulfil the increasing demand for capacity, networks will rely on the use of millimetre-wave and higher frequencies. Nevertheless, at such frequencies communication is limited to small ranges (specially due to limitations in power consumption and space to install a large number of antennas in mobile terminals), so it will be necessary to deploy a huge number of small cells which have to be configured, controlled, and connected to the network using high-throughput and low latency backhaul links.

To satisfy the need of un-interrupted services, resilience, flexibility, or dynamic deployment it will be necessary to create new heterogeneous integrated network architecture, which includes the more traditional macro and small cells, new elements such as high altitude communications platforms, satellites, and also *moving networks* that will follow the traffic demand.

IV. OPTICAL NETWORKS

The complexity of 5G networks will require optical networks able to handle high volumes of high-speed data flows. The flexible architectures proposed in 5G for the optimization of the balance between distributed and centralized processing require also flexible and easily adaptable optical network infrastructures.

Novel architectures to homogenise, automate the control and coordinate the different optical elements will also be necessary. Such architectures will converge towards an integrated platform exploiting commodity hardware.

V. EXPERIMENTATION AND VERTICALS

Research in 5G is also a challenge. Interdisciplinary groups of researchers including engineers (communications, electrical and software engineers), economists, sociologists, lawyers, bio-engineers, user's associations and professional associations will have to work together to address the challenge to create a novel communication network.

Early tests of research results, products, or services, should be performed to guarantee their correct operation in a real scenario. Therefore, it is necessary to create new experimentation facilities, or extend the existing ones, in order to provide enhanced experimentation infrastructures on top of which research teams and third party experimenters will be able to test their vertical applications and solutions in a fully featured infrastructure that is adapted to the vertical sector. This way, a wide range of stakeholders, from SMEs to big industrial partners, will be able to test their developments and offer high quality products and services.

VI. RESEARCH DIRECTIONS

In order to address the challenges, the SRIA identifies other research directions contributed by researchers from industry and academia.

Regarding Virtual Networks and Services, the proposed research directions are, among others:

- Generalisation of controller intelligence in SDN networks, beyond the current-state of the art in which the controllers are standard entities, but their intelligence relies on proprietary engines.
- Including terminals themselves into the SDN architecture by embedding virtual nodes into them. For example, this will allow network controllers to i) assign access connections to terminals in a globally optimal fashion and ii) directly monitor terminal network state within a unified architecture.
- Ultra-dense deployments, which will provide low latencies, ultra-high data rates, and a huge number of simultaneous connections. However, this feature hides many challenges in multiple domains. For example, among others:
  - Trade-offs between utilisation of resources, network performance, and energy efficiency.
  - Software Networks.
  - Multi-tenancy.
- As previously said, enforcing security across a highly complex hierarchical virtualised network
- Lightweight network virtualisation allowing on-demand automatic deployment of vertical mobile operators. This has deep implications in edge computing, as it will be necessary to take network processing as close as possible to end terminals deployed in such small environments as a factory.
- Multimedia uplink transmission. This is essential, for example, for drones.

In the area of Radio Networks and Signal Processing the SRIA document also identifies several possibilities:

- Technologies that facilitate a dynamic resource allocation and network optimization. For example:
  - Device to device communications.
  - New satellite networks.
  - Terahertz communications.
  - Cognitive Radio for Machine to Machine.
- Low latency services, which will need paradigms such as Mobile Edge Computing and Mobile Cloud.
- Moving Networks, which allow a flexible deployment. Such networks would include in-vehicle relays, and D2D relaying to offload the traffic from macrocells.
- Enhanced Broadcast/Multicast services that will be able to preserve a suitable QoS to the different users or groups of users.
- Cross layer design for networks with support for multiclass services, in order to support massive connections with diverse QoS profiles while optimizing power consumption and other parameters, the coexistence with Machine-Type Communications, etc.
- Error correction and redundancy.

Some examples in the field of Optical Networks are:

- The integration of networks in the access, combining radio and fixed (optical) network technologies.

– Increase the capacity of existing networks and create a converged infrastructure.
– The convergence of a multitude of access technologies requires a network that is able to encapsulate dissimilar protocols and applications with different latency and packet-loss requirements.
– Dynamic, flexible and adaptive networks.
– New monitoring techniques.

Another relevant aspect, also as previously mentioned, is the definition of *verticals*. The following verticals are explicitly cited:

– Research testbeds.
– Public protection and disaster relief.
– Mission critical applications, for which network slicing will be a key enabler.
– Industry 4.0.
– Integrated moving networks.
– Drone networks.
– Social networks.

VII. Roadmap and Recommendations

The SRIA concludes with a research roadmap that makes a prediction about the state of some technologies in the period 2017-2022, and after the year 2022. In this case, the identified key technologies and topics are SDN and NFV, security, UAVs, moving networks, radio networks, SatCom systems, and optical networks.

A set of recommendations are also provided to focus the work in each one of the four research areas that were identified to make Pervasive Virtual Mobile Services a reality and that will mark the strategy research and innovation agenda for the upcoming years.

Security is a key topic for Virtual Networks and Services, and should be included in the core of the designed architecture. The new paradigm of Software Networks will allow the creation of new flexible networks, but it should be validated through large-scale tests. In this regard, SDN and NFV should be pushed to their limits, and study how to unify interfaces, create multi-tenancy networks, reduce energy consumption, use resource-constrained devices, include terminals as part of the network, and handle ultra-dense deployments.

There are several research directions that should be addressed regarding Radio Networks and Signal Processing, such as new radio protocols for efficient backhauling and fronthauling (including terahertz and visible light communications), cross-layer optimization to support multi-services, social-aware network management, the integration of satellite networks, and the creation of new tools for the optimization of the radio network and the usage of the spectrum.

Optical Networks will be essential to link and integrate the different elements and create a ubiquitous Digital Environment. Such networks should scale dynamically to match "supply" with the "demand", and to support services with diverse performance requirements. It will be necessary to create new novel architectures that foster the convergence of heterogeneous systems, creating networks that are able to orchestrate a pool of resources (for example to share/slice them or to integrate the access and core networks).

Finally, it is necessary to create large-scale testbeds, and to foster inter-disciplinary research.

VIII. Conclusions

In this paper we have summarized the most relevant challenges and proposals collected in the SRIA for Pervasive Mobile Virtual Services in 5G. It classifies the research topics in four areas, identifies some of the research directions and provides a roadmap and recommendations to promote the necessary research in the industry and the academia.

Acknowledgments

We would like to acknowledge and thank the Expert Advisory Group of the European Technology platform Networld 2020, and more particularly to the authors of the Strategic Research and Innovation Agenda for Pervasive Mobile Virtual Services.

References

[1] Strategic Research and Innovation Agenda (SRIA) document on "Pervasive Mobile Virtual Services", Expert Advisory Group of the European Technology Platform Networld 2020, September 2016

Felipe Gil-Castiñeira received the M.Sc. degree in telecommunication engineering (major in telematics) and the Ph.D. degree in telecommunication engineering from the University of Vigo, in 2002 and 2007, respectively. He is currently an Associate Professor with the Department of Telematics Engineering, University of Vigo. Between 2014 and September 2016, he was the head of the Intelligent Networked Systems area in Gradiant. His research interests include wireless communication technologies and core network technologies, multimedia communications, embedded systems, ubiquitous computing, and the Internet of things. He has published more than sixty papers in those fields in international journals and conference proceedings. He has led several national and international R&D projects.

Francisco J. González Castaño is a Full Professor with the Department of Telematics Engineering, UVIGO, where he leads the Information Technologies Group. Previously, he was a research engineer with Televes SA, Spain and an assistant professor with the Computer Science Department, University of Wisconsin-Madison, USA. Since its foundation in 2008 until 2013, he was CTO in Networks & Applications with Gradiant, Spain. His research interests include intelligent multimedia systems, data analytics and wireless networks. He has published over 100 papers in those fields in international journals and many additional papers in international conference proceedings. He holds two Spanish patents and two US patents. He has led many international and national projects.

Pogledi SOEK na predlog Evropske komisije za reformo regulatornega okvirja v zvezi z upravljanjem s spektrom

SOEK, Sekcija operaterjev elektronskih komunikacij pri Gospodarski zbornici Slovenije

Povzetek — Za spodbujanje izgradnje 5G omrežij je Evropska komisija predlagala novo politiko upravljanja spektra, ter krepitev pristojnosti organov na evropskem nivoju. V skladu s tem se porajajo vprašanja suverenosti nacionalnih politik. Pogled SOEK se osredotoča na predlagano evropsko reformo v povezavi s strateškimi in zakonodajnimi težnjami v Republiki Sloveniji.

Ključne besede — 5G, politika upravljanja spektra, Evropska komisija

Abstract — In order to enhance the investments in the 5G networks, European Commission proposed new spectrum management policy including the harmonisation of competences and practices across internal market. Regarding this, the state sovereignty and national politics are in question. SOEK view is concentrating on the proposed European reform and its connection to strategic and legislative tendencies in Republic of Slovenia.

Keywords — 5G, Spectrum management policy, European commission

I. UVOD

Izmed pomembnejših nalog, ki jih je SOEK identificiral v letošnjem in prihodnjih letih, je nedvomno tudi implementacija sprememb v politiki upravljanja spektra. Z upravljanjem spektra se ukvarjata predvsem pristojno ministrstvo, ki prenaša Evropske direktive v nacionalne zakone in pripravlja strateške usmeritve, ki so podlaga za izvajanje politike s strani nacionalnega regulatorja (Agencije za komunikacijska omrežja in storitve RS).

Agencija za komunikacijska omrežja in storitve (AKOS) s postopki podeljevanja pravic uporabe frekvenc za opravljanje javnih elektronskih komunikacijskih storitev z javnimi razpisi in javnimi dražbami ter preverjanjem obveznosti iz odločb o dodelitvi frekvenc skrbi za ustrezno rabo omejene naravne dobrine, seveda na podlagi prej omenjenih politik. Z razvojem tehnologij in rastočih potreb končnih uporabnikov po storitvah mobilnega širokopasovnega dostopa ter drugih storitev, se povečujejo tudi potrebe po frekvenčnem prostoru, ki je dobrina, katera v omejenih količinah pripada posameznim državam. V celotnem spektru frekvenčnega prostora se nahaja množica različnih frekvenc v različnih frekvenčnih pasovih, preko katerih se omogočajo storitve, kot so ladijske, letalske, radioamaterske, frekvence za oddajanje medijskih vsebin ter frekvence, namenjene mobilnim komunikacijam in še marsikatere druge. Vse upravlja prej omenjena agencija, ki je torej pri tem odvisna tako od strateških usmeritev države, kot tudi od harmoniziranih mednarodnih dokumentov.

Pogled industrije pa je nekoliko bolj pragmatičen in bi moral biti upoštevan predvsem pri strateškem odločanju države, ter ocenjevanju vrednosti in določanju trajanja posameznih frekvenčnih pasov.

Kot opisano v nadaljevanju, je Evropska komisija z akcijskih načrtom 5G in predlagano spremembo regulatornega okvira prepoznala nujnost prilagoditve regulatornega okolja potrebam gospodarstva, z namenom spodbujanja konkurenčnosti celotne Evrope, ki bi z odpravo prevelike regulacije prinesla hitrejši napredek in rast gospodarstva.

II. AKCIJSKI NAČRT 5G IN PREDLAGANA SPREMEMBA REGULATORNEGA OKVIRJA

14. septembra 2016 je Evropska komisija kot nadgradnjo Digitalne agende objavila paket dokumentov, kot spremljajočih predlogu direktive Recast, torej novega regulatornega okvirja.

Evropska komisija vidi 5G kot novo generacijo omrežnih tehnologij, ki bo omogočila industrijsko transformacijo skozi brezžične storitve širokopasovnega dostopa, katere bodo omogočale hitrosti tudi preko 10 gigabitov na sekundo in izkoriščanje različnih dosegljivih brezžičnih virov, od Wi-Fi do 4G ter simultano koordinirala milijone povezanih naprav, tudi novih aplikacij, kot na primer Internet stvari. Glede na vsestranskost inovativnih poslovnih modelov, bodo učinki tehnologij 5G, s prodornimi virtualnimi mobilnimi storitvami, od virtualne resničnosti do oddaljenega nadzora in sodelovanja, virtualnega zdravstvenega nadzora, povezanih in samovozečih vozil, segli na mnoga različna področja, med drugim transport, zdravstvene storitve, proizvodnjo, logistiko, energetiko, medije in zabavo. To bo dosegljivo predvsem s prodornimi virtualnimi mobilnimi storitvami, od virtualne resničnosti do oddaljenega nadzora in sodelovanja, virtualnega zdravstvenega nadzora, povezanih in samo-vozečih vozil in drugih možnosti razvoja.

Glede na trenutno dogajanje v svetu telekomunikacij, bi lahko prva živa omrežja 5G videli v prvi ali drugi polovici leta 2019, večji razmah implementacije pa se pričakuje v letu 2020.

Trenutno poteka standardizacija omrežja naslednje generacije, prav tako pa se pripravljajo prvi laboratorijski testi omrežja prihodnosti. Kot že samo ime pove, gre za naslednjo generacijo mobilnih omrežij, ki bo še hitrejša in odzivnejša, zmožna pa bo zagotavljati storitev tisočim uporabnikov oz. napravam na eni točki.

5G pomeni naslednji tehnološki preskok. Deloma zaradi uporabe novega frekvenčnega spektra, deloma pa tudi zaradi tega, ker bo vključeval povsem nov radijski vmesnik. Novi radijski vmesnik je znan pod imenom NR (new radio) -

tehnologija je še vedno v razvojni fazi. Nekaj operaterjev po svetu je že preizkušalo tehnike F-OFDM (Filtered Orthogonal Frequency Division Multiplexing), ki zagotavljajo do 100 % višjo vršno hitrost in pa SCMA (Sparse Code Multiple Access), ki bo zagotavljala simultano ogromno število povezav in višje vršne hitrosti. Testi kažejo, da lahko tehnika SCMA zagotavlja do 300 % več povezav v smeri proti omrežju, v smeri proti uporabniku pa le-to poviša za do 80 %.

Frekvenčni pasovi, o katerih se govori v povezavi s 5G tehnologijo, so v delu spektra pod 6 GHz in 28 GHz. Tehnike, ki se bodo uporabljale v teh pasovih, vključujejo napredne antenske sisteme (usmerjanje frekvenčnih snopov in sledenje uporabnika), ki bodo izboljšale delovanje na razdalji in okoljih brez direktne vidljivosti.

Realizacijo bodo morali izpeljati operaterji sami. Dejstvo pa je, da bodo investicije v omrežje 5G izjemno visoke in vsaka dodatna pomoč države v smislu infrastrukture bi bila dobrodošla.

Prav tako se je že letos pojavil tudi velik interes industrije, ki želi vlagati v razvoj omrežij 5G, predvsem pri razvoju terminalne opreme in pa primerov uporabe. Sama tehnologija bo namreč omogočala povezljivost milijonov naprav M2M.

Glede na dejstvo, da tehnologije 5G še niso v celoti standardizirane in da je predviden predvsem razvoj novih storitev, je Evropska komisija že v predlogu novega regulatornega okvirja, v direktivi Recast predlagala rok trajanja odločb o dodelitvi pravic uporabe radiofrekvenčnega spektra, ki naj bi bil najmanj 25 let. Predlagani rok in harmonizacija postopkov ter časovnic podelitev je v Evropskem političnem prostoru sprožila mnoge polemike, ki so večinoma izvirale predvsem iz pomislekov držav članic o zmanjšanju suverenosti pri odločanju o rabi omejenih dobrin. Celotni sveženj novega regulatornega okvirja je v posvetovanju v Evropskem parlamentu in Evropskem svetu, pripombe na predlog direktive pa je podal tudi BEREC. Funkcija BEREC se s tem sicer povečuje, vendar ugovarja roku trajanja odločb. Svet, ki predstavlja mnenje držav članic, predlogu sicer do določene mere nasprotuje, medtem ko je parlamentarni odbor ITRE predlagal celo 30 letni rok. Čeprav se morda zdi, da je tolikšna debata o trajanju in pristojnostih glede frekvenčnega spektra morda celo pretirana, pa operaterji pozorno spremljamo razvoj dogodkov, ki je bistven za nadaljnji razvoj novih tehnologij.

Polemike strokovne javnosti se vrtijo okoli vprašanja, zakaj investirati v 5G? Glede na to, da je bilo do sedaj pri vsaki novi tehnologiji povsem jasno, kaj operater lahko pričakuje, trenutno temu ni tako. Pri tehnologijah 2G se je omogočilo brezžične govorne komunikacije, pri 3G vsaj osnoven prenos podatkov, torej elektronsko pošto, tehnologija 4G je omogočila širokopasovni dostop, vendar pa je njegovo zagotavljanje še vedno zelo drago. Kaj pa lahko sploh pričakujemo od 5G? Verjetno ponovno visoke stroške za operaterje, tveganje pri nabavi opreme zaradi pomanjkljive standardizacije, investicijsko neprijazno okolje zaradi regulatorne nepredvidljivosti, itd., medtem ko so se končni uporabniki »razvadili« z nizkimi cenami mobilnega širokopasovnega dostopa.

Navedenega se Evropska komisija in Evropski parlament dobro zavedata, zato sta predlagala ustrezen čas veljavnosti odločb o dodelitvi pravice do uporabe radiofrekvenčnega spektra.

III. ZAKONSKA IMPLEMENTACIJA V REPUBLIKI SLOVENIJI

Kaj pa se dogaja v Republiki Sloveniji?

Trenutno je v 'ciljni ravnini' novela ZEKom-1c, ki implementira Direktivo o zniževanju stroškov iz leta 2014. Zakonodajalec ne razume teženj industrije in argumentacije Evropske komisije, čemu je potrebno podaljšati čas veljavnosti pravic uporabe frekvenčnega spektra, zato ga je pustil na največ 15 letih. V tem namreč vidi nezanemarljiv vir proračunskega prihodka, ki bi ga namesto na 15 dobil šele na 25 let. Morda ne vidi, da bi za daljše obdobje lahko zaračunal več? Kakorkoli že, Slovenija ne sledi trendom razvoja in spodbujanja investicij. Skrb vzbuja tudi dejstvo, da v Republiki Sloveniji le stežka sledimo rokom za implementacijo direktiv in se pravočasno ne odzivamo na spremembe na trgu, kar investicijskega okolja nedvomno ne spodbuja. Glede na pretekle izkušnje ne moremo pričakovati, da bi nov regulatorni okvir implementirali do predpisanega leta 2019. Regulator pa bo v tem času moral izvesti razpis za frekvenčni pas 700 MHz (5G) pod pogoji veljavne zakonodaje.

Zavedajoč se nujnosti spremembe veljavnega zakonskega določila, ki v nobenem primeru ne dopušča podelitve frekvenc za dlje kot 15 let, je SOEK že v odgovoru na poziv strokovni, zainteresirani in drugi javnosti v letu 2013, ponovno pa v posredovanem prispevku v okviru priprave novele ZEKom-1 in nato še v okviru javne obravnave osnutka ZEKom-1c, predlagal spremembe določil v poglavju o radiofrekvenčnem spektru, zlasti spremembo določila 1. odstavka 53. člena ZEKom-1, ki določa čas veljavnosti odločbe o dodelitvi radijskih frekvenc.

V fazi obravnave predlogov sprememb ZEKom-1 na delovnih telesih Vlade RS in Vlade RS naši predlogi za podaljšanje veljavnosti odločb o dodelitvi radijskih frekvenc niso bili upoštevani, čeprav smo se v teh predlogih izrecno sklicevali na predlagano evropsko reformo in na predlog Evropske komisije, da naj se pravice do uporabe spektra za namene investiranja v visoko zmogljiva omrežja podeljujejo najmanj za 25 let.

Evropski parlament je ob razpravi o reformi Evropskega zakonodajnega okvira zavzel stališče, da je spekter "kri v žilah" mobilne ekonomije in pogoj za nove storitve za potrošnike. Evropski parlament predlaga, da naj zakonodajalci v štirih korakih podprejo in izboljšajo pristop Evropske komisije glede politike upravljanja spektra. Prvi predlagani korak je podaljšanje veljavnosti licenc (nedoločen čas ali minimalno 30 let) in okrepitev ukrepov za izboljšanje dolgoročne predvidljivosti in vzdržnosti poslovnih modelov operaterjev.

Uvajanje omrežij 5G, ki so naslednja generacija mobilnih širokopasovnih storitev, z enormnim pozitivnim socio-ekonomskim potencialom v zasebnem in javnem sektorju (ob predvideni zagonski investiciji 56 milijard evrov se na evropski ravni predvideva več kot 2,3 milijona novih delovnih mest, na letni ravni pa se pričakuje koristi na ocenjenih 113 do 165 milijard evrov), bo od operaterjev terjalo dolgotrajen postopek načrtovanja in gradnje novega omrežja, ki bo glede na izkušnje trajal najmanj tri leta. To pomeni, da od časa dodelitve radijskih frekvenc do njihove komercializacije preteče več let. V primeru omejitve najdaljšega obdobja veljavnosti odločbe o dodelitvi radijskih frekvenc na 15 let je dejansko čas povratka investicije zgolj 12 let, kar pa je za tako veliko investicijo, kot je gradnja

mobilnega omrežja pete generacije, veliko prekratka in za investitorje nespodbudna doba, z daljšo dobo pa se mnogo bolj spodbujajo tudi inovacije. To so prepoznali tudi v mnogih EU državah, kjer so bili že izvedeni razpisi za dodelitev frekvenc za zagotavljanje storitev končnim uporabnikom oziroma so v postopku izvedbe in so dodelili frekvence za obdobje, ki je bistveno daljše od 15 let.

Upoštevaje dejstvo, da je Agencija za komunikacijska omrežja in storitve v objavljenem *Programu dela in finančnem načrtu za leto 2017* navedla, da namerava v letu 2017 pripraviti javne razpise za nove frekvenčne pasove za javne komunikacijske storitve, je sprememba določila 1. odstavka 53. člena ZEKom-1 (podaljšanje veljavnosti ODRF) v obravnavani noveli ZEKom-1c po prepričanju SOEK nujna, ker je veljavnost dovoljenj potrebno uskladiti pred izvedbo razpisov.

LITERATURA

[1] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:COM_2016_0590_FIN
[2] 5GforEuropeAnActionPlan-StaffWorkingDocument.pdf
[3] COMMISSION STAFF WORKING DOCUMENT 5G Global Developments Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 5G for Europe: An Action Plan {COM(2016) 588 final}
[4] http://www.fiercewireless.com/5g/madden-why-5g
[5] http://www.cullen-international.com/

SOEK je Sekcija operaterjev pri Gospodarski zbornici Slovenije, ustanovljena leta 2013. SOEK nadaljuje delo ustanovnih članov, ki so do ustanovitve SOEK delovali znotraj Združenja za informatiko in telekomunikacije. Poslanstvo SOEK je podpiranje razvoja elektronskih komunikacij v Sloveniji ter si z namenom doseganja največjih koristi za končne uporabnike članov SOEK in za lastne člane, prizadeva za izboljšanje nacionalnih in evropskih regulatornih aktov na področju elektronskih komunikacij in poslovnega okolja za delovanje članov sekcije na področjih glavnih gospodarskih dejavnosti članov sekcije. V letu 2016 je SOEK v okviru GZS organiziral dva posveta, o indeksu DESI in ZEKom-1c, člani SOEK so proaktivno sodelovali na mednarodni delavnici »European Views on Net Neutrality«, prizadevali so si k tolmačenju različnih problematik v okviru Digitalne Slovenije, med drugim pojma soinvestitorstva. DID je sprejel več pripomb, ki so bile s strani SOEK podane na predlog ZEKom-1C, poleg tega je SOEK sodeloval pri preprečitvi uvedbe prispevka na deficitarne vsebine, kot je bilo prvotno predvideno s strani Ministrstva za kulturo v medijski strategiji. Aktivno, s konstruktivnimi pripombami, pa je SOEK sodeloval tudi pri drugi aktualni zakonodaji in drugih pomembnih dokumentih, ki močno vplivajo na oblikovanje slovenskega trga elektronskih komunikacij.

Slovenska iniciativa 5G

Meta Pavšek Taškov, Agencija za komunikacijska omrežja in storitve RS, Slovenija

Povzetek — Članek opisuje Akcijski načrt za 5G v Evropi, COM (2016) 588, odzive na iniciativo 5G v Sloveniji in priprave na svetovno konferenco WRC-19. Predstavljena je slovenska iniciativa 5G, ki jo je Agencija za komunikacijska omrežja in storitve objavila na svoji spletni strani in s katero v sodelovanju z Ministrstvom za javno upravo poziva investitorje k prijavi projektov za testiranje in prihodnjo rabo tehnologije 5G. S tem želi podpreti pobudo Evropske komisije, da omogoči razvojne projekte za tehnologijo 5G ter v okviru tega čimprejšnje uvajanje omrežij 5G v Sloveniji. Z Akcijskim načrtom za 5G v Evropi, zapisanim v dokumentu *5G for Europe - An Action Plan COM(2016) 588 final*, želi Evropska komisija, poleg ostalih smernic, promovirati in finančno podpreti vse 5G-PPP za preizkuse, ki bi jih evropske države izvajale od 2017 dalje, kot tudi za pred-komercialna testna delovanja opreme 5G. Agencija je ponudila uporabo frekvenčnega pasu 3400 - 3800 MHz za testiranje projektov 5G po mestih Slovenije. Ena od prioritetnih vertikal bi lahko bila prihodnja uporaba infrastrukture 5G za izboljšanje storitev sistema javne varnosti ter zaščite in reševanja (PPDR). Poleg tega bi v okviru iniciative 5G lahko v omejenem obsegu testirale tudi frekvence v UHF kanalih, ki jih ima Slovenija koordinirane v skladu s sporazumom GE06 - predvsem za doseganje visokih prenosnih hitrosti do 100 Mbit/s, zlasti z namenom priprave nove platforme za prenos avdiovizualnih vsebin, tako za oddajanje enemu prejemniku (unicast), kot tudi več prejemnikom (multicast) in radiodifuzije - s kratico eMBMS. Agencija lahko pomaga pri vzpostavitvi mednarodnih stikov z evropskimi administracijami, saj bodo imeli prednost projekti, v katerih slovenski deležniki sodelujejo s partnerji iz sosednjih ali drugih evropskih držav.

Ključne besede — 5G, Akcijski načrt za 5G v Evropi, PPDR, 3400 – 3800 MHz, 26 GHz, UHF pas, 100 Mbit/s , avdiovizualne vsebine preko LTE/5G, unicast, multicast , eMBMS, WRC-19

Abstract — This article describes European 5G action plan COM (2016) 588, news regarding the proposed projects for 5G testing in Slovenia and WRC-19 preparations. AKOS and the Ministry of Public Administration has published Slovene 5G initiative on AKOS web page to encourage investors to submit project proposals for testing and future use of 5G technologies in order to support the 5G Manifesto for timely deployment of 5G in EU and in its framework as well an early introduction of 5G networks in Slovenia. With 5G Action Plan for Europe COM(2016) 588 European Commission wants to promote and financially support all 5G –PPP tests started from 2017 as well a pre-commercial 5G test-beds. Agency has offered the frequency band 3400 - 3800 MHz for test beds for 5G projects primarily in Slovene cities. One of priority verticals could be use of future 5G infrastructure to improve the performance of public safety and disaster relief (PPDR). Additionally in framework of 5G Initiative, frequencies in UHF channels allocated to Slovenia in accordance to Geneva06 could be tested in limited range for high-speed wide band services up to 100 Mbps, primarily to establish new platform for transmission of audio-visual content in unicast, multicast or broadcast (eMBMS). As preference is given to projects which involve partners from neighbouring and other European countries, the Agency could support such initiatives using international connections to find appropriate partners.

Keywords — 5G, 5G Action Plan for Europe, PPDR, 3400-3800 MHz, 26 GHz, UHF band, 100 Mbps , audio-visual content over LTE/5G, unicast, multicast , eMBMS, WRC-19

I. UVOD

Agencija za komunikacijska omrežja in storitve (v nadaljevanju Agencija) je dne 22. 12. 2016 v sodelovanju z Ministrstvom za javno upravo pozdravila 5G pobudo Evropske komisije in 13. 1 2017 javno pozvala morebitne investitorje k prijavi projektov za testiranje in prihodnjo rabo tehnologije 5G.

Cilji pobude 5G so:

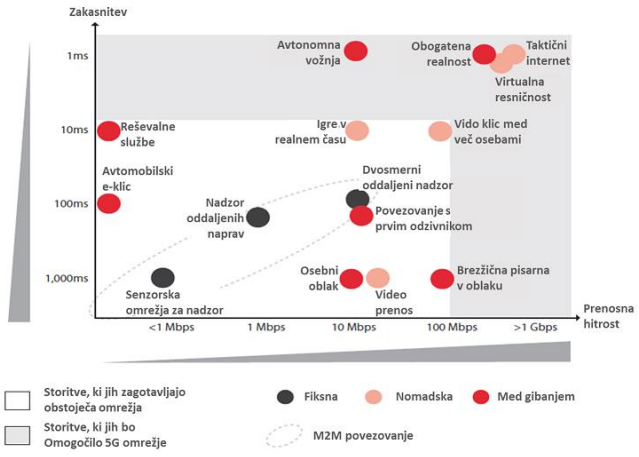
1. uporabiti radiofrekvenčni spekter za dosego največjega možnega družbeno ekonomskega napredka, saj bo 5G povezljivost ključna na vseh področjih družbenega življenja, kot so promet, transport, zdravstvo in energija;
2. spodbuditi razvoj v vseh segmentih gospodarstva in posledično naložbe ter ustvarjanje novih delovnih mest;
3. zagotoviti dostop do sodobnih mobilnih komunikacij in modernih storitev tudi na drugih področjih življenja čim širšemu krogu prebivalstva;
4. ohraniti razvoj učinkovite konkurence na trgih storitev mobilnih elektronskih komunikacij;
5. ohraniti tehnološko in storitveno nevtralnost pri rabi spektra v skladu z evropskimi okviri.

S pobudo je želela Agencija podpreti čimprejšnje uvajanje omrežij 5G v Sloveniji, v skladu z Akcijskim načrtom za 5G v Evropi, COM (2016) 588 [1]. Z njim Evropska komisija promovira in finančno podpira projekte 5G za preizkuse in za pred-komercialna testna delovanja opreme 5G, predvsem meddržavne projekte EU za vzpostavitev digitalnega ekosistema na osnovi povezljivosti 5G in vzpostavitvi testnih okolij za razvoj omrežij 5G v Evropi. Prednostno bodo sredstva namenjena predvsem za meddržavne projekte, zato je Agencija na pobudo deležnikov septembra 2016 poslala predlog za sodelovanje v čezmejnih projektih 5G naslednjim državam: Avstriji, Hrvaški, Italiji, Madžarski, Danski, Švedski, Norveški, Finski, Litvi, Latviji in Estoniji.

5G je peta generacija mobilne telefonije in predstavlja tehnološki preboj[1]. Ker je omrežna arhitektura razdeljena na več različnih vertikal, ki so lahko različno konfigurirane glede na vrsto uporabe (npr. različna pasovna širina, različne prenosne hitrosti, različna kakovost storitev, različne zakasnitve, ipd.), omogoča tehnologija 5G hkratno delovanje različnih storitev, kot so denimo storitve v realnem času, množični prenos podatkov, ultra hiter širokopasovni internet in prenos avdiovizualnih vsebin, podporne storitve in kritične storitve, primerne za varnost in zaščito. 5G gre pretežno v smeri izboljšane podpore komunikaciji stroj-stroj (M2M, ang. Machine to Machine communication), poznani tudi pod imenom internet stvari (IoT, ang. Internet of Things). Razvoj gre v smeri čim cenejših naprav z vgrajenimi SIM karticami,

[1] http://www.akos-rs.si/5g

majhno porabo baterije, bistveno manjšimi zakasnitvami kot pri tehnologiji 4G. Te naprave bodo gonilo avtomatizacije industrije t.i. Industrija 4.0, avtomatiziranega prometa, pametnih mest, pametnih zgradb in podobno.



Vir: GSMA Intelligence

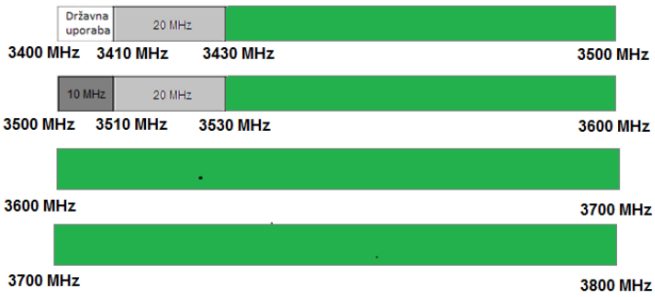
Slika 1: Prednosti 5G – nadgradnja prejšnjih generacij – tehnološki in družbeni preboj

Ker 5G prinaša spremembe na tako širokem področje družbenega življenja, so bili k sodelovanju poleg mobilnih operaterjev, proizvajalcev opreme in terminalov, vabljeni tudi Ministrstvo za obrambo, Ministrstvo za notranje zadeve, v okviru vertikale za izboljšanje storitev sistema javne varnosti ter zaščite in reševanja. Vabljeni so bili tudi deležniki, ki ponujajo podporne storitve: elektroenergetska podjetja, vodovodna podjetja ter podjetja, katerih glavna dejavnost je promet (projekt samo-vozečih vozil in pametnega prometa), pa tudi lokalne skupnosti, kjer bi se lahko testno izvajali projekti pametnih zgradb ali pametnih naselij, ter industrija, kjer bi preko 5G lahko zaživela pametna industrija 4.0, v kateri je proizvodnji proces robotiziran ali pa gre za obdelavo ogromne količine podatkov in so uporabljeni informacijski koncepti, kot so ERP (Enterprise Resource Planning), SCM (Supply Chain Management), CRM (Customer Relationship Management) in PLC (Product Lifecycle Management)).

Agencija je pozvala zainteresirano javnost, da jo obvesti o pripravi projektov, ki bi vključili najnovejšo tehnologijo 5G ter navede, za kateri segment gospodarstva bi bil ta projekt primarno namenjen. Za projekte, v katerih zainteresirana javnost sodeluje s partnerji iz sosednjih ali drugih evropskih držav, ki so s stališča EU prednostni, je Agencija pripravljena pomagati pri vzpostavitvi mednarodnih stikov z evropskimi administracijami.

Agencija je predlagala uporabo frekvenčnega pasu 3400 – 3800 MHz za testiranje projektov 5G po mestih Slovenije za obdobje skladno z drugim odstavkom 53. člena ZEKom-1.

S tem je želela podpreti čimprejšnje uvajanje omrežij 5G v Sloveniji v skladu z Akcijskim načrtom za 5G v Evropi, COM (2016) 588. S tem dokumentom želi namreč Evropska komisija, poleg ostalih smernic, promovirati in finančno podpreti vse preizkuse 5G-PPP, ki bi jih evropske države izvajale od 2017 dalje, kot tudi za pred-komercialna testna delovanja opreme 5G, kjer podpira predvsem meddržavne EU projekte zlasti v zvezi z akcijsko točko 7, ki govori o čezmejnem sodelovanju v evropskih projektih za vzpostavitev digitalnega ekosistema na osnovi 5G-povezljivosti in vzpostavitvi testnih okolij za razvoj 5G v Evropi. Ena od prioritetnih vertikal bi lahko bila prihodnja uporaba infrastrukture 5G za izboljšanje storitev sistema javne varnosti ter zaščite in reševanja (PPDR).



Slika 2: Deli spektra v pasu 3400 – 3800 MHz za testiranje 5G (zeleno)

Če bo potrebno, lahko Agencija da na voljo za testiranje tudi del spektra v pasu 26 GHz, ki je v NURF[2] namenjen za širokopasovne brezžične dostopovne sisteme BWA (angl. Broadband Wireless Access systems).

V okviru iniciative 5G pa je možno v omejenem obsegu testirali tudi frekvence v UHF-kanalih, ki jih ima Slovenija koordinirane v skladu z sporazumom GE06, predvsem za doseganje visokih prenosnih hitrosti do 100 Mbit/s, zlasti z namenom priprave nove platforme za prenos avdiovizualnih vsebin, tako za oddajanje enemu prejemniku (unicast), kot tudi več prejemnikom (multicast) in radiodifuzije - s kratico eMBMS.

II. AKCIJSKI NAČRT ZA 5G V EVROPI COM(2016)588[1]

Osnova za nastanek Akcijskega načrta za 5G v Evropi COM (2016) 588 je bila želja, da bi Evropa po 24 letih od uspešne uvedbe GSM, s hitro uvedbo prihajajoče tehnologije 5G, spet postala vodilna celina v okviru mobilnih tehnologij. To je nova revolucionarna tehnologija, ki bo spremenila človeško družbo, saj bo s širokopasovnimi povezavami, giga-bitnimi hitrostmi in mili-sekundnimi zakasnitvami omogočila preobrazbo industrije, podporo množičnemu povezovanju, ne samo ljudi, ampak tudi stvari. Z novo arhitekturo, ki bo omogočila množico virtualnih omrežij različnih karakteristik preko enega fizičnega omrežja za tako imenovane vertikale, bo omogočila komunikacijsko platformo za različne sektorje gospodarstva.

Strategija Evropske komisije o enotnem digitalnem trgu[3] poudarja pomen omrežij velike kapacitete (kot je 5G) za evropski trg, da bo Evropa lahko ostala konkurenčna na globalnem trgu. Tehnologija 5G predstavlja priložnost za gospodarski razcvet, saj naj bi prihodki z naslova 5G v svetu leta 2025 dosegli 225 milijard EUR[4], letni prihodki štirih glavnih sektorjev 5G oziroma vertikal pa kar 114 milijard letno.[5]

Evropska komisija je v letu 2013 v okviru Evropskega akcijskega načrta 5G COM(2016)588 namenila 700

[2] Splošni akt o načrtu uporabe radijskih frekvenc
[3] https://ec.europa.eu/digital-single-market/en/digitising-european-industry
[4] https://www.abiresearch.com/press/abi-research-projects-5g-worldwide-service-revenue/
[5] Studying automotive, health, transport and energy sectors: https://ec.europa.eu/digital-single-market/en/news/study-identification-and-quantification-key-socio-economic-data-strategic-planning-5g

milijonov EUR javnih sredstev za financiranje javno zasebnih partnerstev 5G-PPP, s ciljem, da bo 5G tehnologija v Evropi zaživela do leta 2020.

Tudi predlog nove okvirne direktive[6], tako imenovani »European Electronic Communications Code« je bil zasnovan s ciljem čim hitrejše uveljavitve 5G s čim manjšimi stroški in regulatornimi ovirami. Pred kratkim sprejeta pravila za odprti internet[7] pa omogočajo pravno varnost storitvam 5G.

S ciljem, da Evropa ne bi zaostajala za ZDA in daljnim vzhodom, je Evropska Komisija v akcijskem načrtu 5G COM (2016) 588 zapisala naslednje akcijske točke:

1. Izdelava skupne časovnice in promocija uvedbe 5G v Evropi:
   a. 2017 preliminarna 5G-testiranja znotraj 5G-PPP in 2018 prva nekomercialna testiranja preko državnih mej;
   b. Do konca 2017 članice izdelajo 5G-časovnice, kot del nacionalne širokopasovne strategije;
   c. Do konca 2020 vsaka članica s tehnologijo 5G opremi vsaj eno večje mesto in do 2025 morajo vsa večja mesta in transportne poti imeti nemoteno 5G pokrivanje.
2. Prioritetni pasovi za uvedbo 5G:
   a. Do konca 2016 določiti prioritetne pasove za uvedbo 5G: pod 1 GHz, med 1 in 6 GHz ter nad 6 GHz.
   b. Točka je delno že realizirana. Komisija za radijski spekter RSC (angl. Radio Spectrum Comitte) je sprejela mandat CEPT za harmonizirane tehnične pogoje za uvedbo 5G-sistemov v prioritetnem spektru:
      i. Pod 1 GHz: 700 MHz
      ii. Med 1 in 6 GHz: 3400 – 3800 MHz
      iii. Nad 6 GHz: 24,25 – 27,5 GHz
3. Dati na voljo dovolj spektra za 5G:
   a. Do konca 2017 na osnovi mnenja Skupine za politiko radijskega spektra RSPG (angl. Radio Spectrum Policy Group) določiti nabor 5G-asov;
   b. Do konca 2017 na osnovi študij CEPT določiti priporočila za licenciranje posameznih 5G-pasov v spektru nad 6 GHz;
4. FWBA (angl. Fixed Wireless Broadband Access) oziroma konvergenca fiksnega in brezžičnega širokopasovnega dostopa:
   a. Obveznosti pokrivanja z optičnimi in celičnimi omrežji s predpisanimi prenosnimi hitrostmi in kvaliteto storitev QoS vseh urbanih področji in transportnih poti za nemoteno pokrivanje s 5G do 2025 ter nadzor izpolnjevanje obveznosti;
   b. Nemudoma določiti najboljše evropske prakse in uskladiti določbe nove okvirne direktive (RSPG in BEREC že pripravljata poročili o dobrih praksah glede obveznosti pokrivanja in o pokrivanju v zahtevnih pogojih).
5. Globalna interoperabilnost 5G:
   a. Leta 2019 na voljo prvi globalni standardi 5G;
   b. Standardizacija dostopovnih omrežij in central z omogočenimi specialnimi primeri uporabe 5G. Standardizacija naj bo odprta za inovacije;
   c. Do konca 2017 – partnerstva med industrijami za definiranje standardov, ki bodo podprti s preizkusi v industriji skozi mednarodna sodelovanja in digitalizacijo industrije.
6. Digitalni ekosistem za 5G-povezljivost:
   a. 2017 začetek ključnih tehnoloških eksperimentov, vključno s terminali in aplikacijami razvitimi preko 5G-PPP, ki bodo namenjene napredku v industriji;
   b. Do marca 2017 predstaviti natančno časovnico za napredne pred-komercialne preizkuse vodilnih vertikal 5G leta 2018, z namenom, da bo Evropa vodilna v razvoju 5G.
7. Infrastruktura 5G za storitve PPDR:
   a. EC spodbuja članice, da razmišljajo o uporabi infrastrukture 5G za izboljšanje delovanja elektronskih komunikacijskih storitev za zaščito, reševanje in javno varnost, vključno s hibridnim pristopom oziroma souporabo komercialnih omrežij 5G, ter da vključijo BBPPDR v nacionalne plane za 5G.
8. 5G infrastruktura za storitve PPDR:
   a. EC bo v sodelovanju z industrijo in EIB Group 43 določila cilje, možne konfiguracije, in modele za objekt tveganega financiranja, po možnosti povezanimi z drugimi digitalnimi ukrepi za začetek delovanja. Izvedljivost je ocenila do konca marca 2017, ob upoštevanju možnosti za povečanje zasebnega financiranja z dodajanjem več virov javnega financiranja predvsem s strani European Fund for Strategic Investments (EFSI) in ostalih EU finančnih inštrumentov.

Za Slovenijo je zanimiva zlasti akcijska točka 7, ki govori o uporabi infrastrukture 5G za izboljšanje storitev sistema javne varnosti ter zaščite in reševanja (PPDR).

III. ODZIVI NA INICIATIVO 5G

Na iniciativo5G so se odzvali naslednji deležniki: operater Telekom Slovenije, proizvajalca opreme Ericsson in Iskratel, predstavniki uporabnikov MNZ Policija, MORS URSZ in Slovenska vojska in deležnik iz raziskovalne sfere Fakulteta za Elektrotehniko v Ljubljani (LTFE). Dne 16. 3. 2017 je bil na pobudo ministra za javno upravo sklican ustanovni sestanek iniciative 5G, kjer je minister Koprivnikar predstavil politično odločitev Slovenije, da se množica profesionalnih infrastruktur poenoti in podprl pobudo za vertikalo 5G za širokopasovna omrežja za sistem javne varnosti ter zaščite in reševanja (v nadaljevanju BB PPDR), saj bo to omogočilo zagotavljanje javne varnosti, zaščite in reševanja pa tudi podpornih storitev preko skupne vertikale 5G PPDR, obenem pa omogočilo povezljivost z obstoječimi sistemi.

Cilj Slovenije je postati zelena referenčna država za digitalno tehnologijo. Zelena – okolju prijazna, referenčna – obstoječa omrežja uporabiti, nadgraditi in souporabiti za širokopasovne in podporne storitve PPDR.

Direktorat za informacijsko družbo je predstavil aktivnosti glede navezave stikov z organi Evropske Unije.

Agencija je podala predlog spremembe 53. člena ZEKom-1 za odločbo o dodelitvi radijskih frekvenc za daljše časovno obdobje do 3 let za testiranje novih tehnologij v okviru Evropskih razvojnih projektov in dala na voljo spekter.

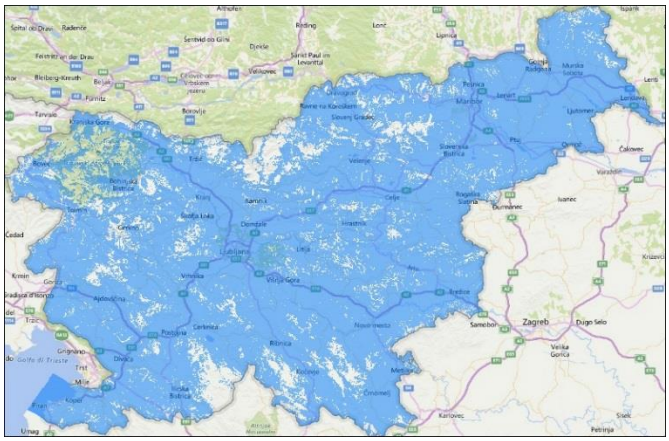
Vsi deležniki so predstavili, kje se vidijo v projektu 5G PPDR. Predstavili so prvo verzijo »White paper«, ki bo

[6] https://ec.europa.eu/digital-single-market/en/connectivity-european-gigabit-society

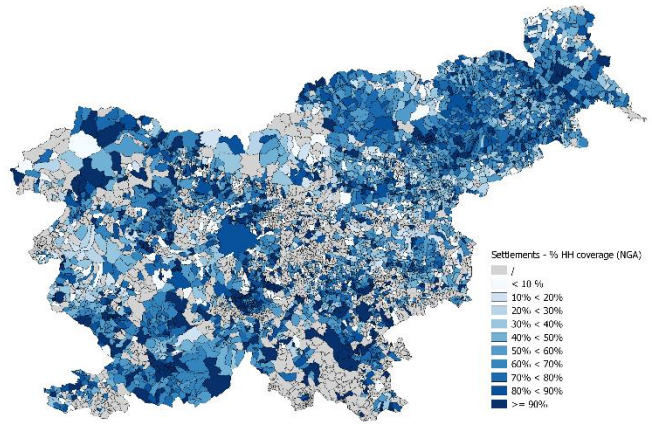
[7] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2120&from=en

osnova za prijavo evropskega projekta 5G. Poudarili so, da mora slovenski projekt BB PPDR ponuditi nekaj novega, tako na tehničnem, kot tudi regulatornem področju in predstavljati dolgoročno, tehnološko napredno rešitev za določeni segment/vertikalo uporabe. To bi bila lahko vertikala BB PPDR. Projekt 5G PPDR je v zasnovan kot vtičnik[8] 5G (plug in) na obstoječem omrežju LTE, ki pa bo seveda za vertikalo 5G uporabljal, skladno z mnenjem RSPG, v prvi fazi spekter 5G v pasu 3500 MHz.

Končni cilj omrežja 5G BB PPDR je, da bi deležniki imeli MVNO na vseh mobilnih operaterjih, ki imajo skupaj danes odlično pokrivanje z omrežji LTE, v prihodnje pa bodo imeli pokrivanje z omrežjem 5G, najmanj enake kvalitete. Na dan 31. 12. 2016 sta dva operaterja imela 97 % pokritost prebivalstva, tretji pa čez 90 % (slika 3). Pokritost prebivalstva s fiksnim omrežjem NGA je 82% (Slika 4).



Slika 3: Pokritost z omrežjem 4G (10 Mb/s) (*Vir: AKOS)*



Slika 4: Pokritost s fiksnim omrežjem NGA (*Vir: AKOS)*

Da bi končni cilj projekta lahko bil zagotovljen, morata biti rešena tehnični in pravni vidik nacionalnega gostovanja PPDR MVNOja. Ta MVNO bi moral imeti v primeru požara ali drugih intervencij, kot t.i. »first responder«, zagotovljeno prioritizacijo prometa – podobno kot »modra luč« v cestnem prometu.

Ericsson je pripravil osnutek dokumenta (White paper) in ga poslal deležnikom v komentar in dopolnitev. V času do drugega sestanka so izrazili interes tudi Inštitut Jožef Stefan in Joint Research Center (JRC) Evropske komisije. JRC se je povezal z Ministrstvom za javno upravo, Direktoratom za informacijsko družbo in jim predstavil, kako vidijo možnosti sodelovanja. Agencijo so obvestili o podrobnostih možnega sodelovanja. Okvirno so seznanili morebitne slovenska partnerje, da že sodelujejo z Italijo, kar bi projektu dodalo mednarodni pomen, sodelovanje pri tehnološko najnaprednejših evropskih projektih pa bi poleg meritev in dodatnega testiranja ter izmenjave znanja prineslo promocijo Slovenije, saj bi vertikalo 5G za PPDR želeli promovirati v okviru Evropske Unije. Prav tako sodeluje JRC z organizacijama ITU in ETSI ter bi rešitev vertikale 5G za PPDR želel standardizirati na osnovi slovenskega razvojnega projekta. Pozdravljajo tudi usmerjenost te pobude v konkretne rešitve, nadgradljivost iz obstoječih omrežij 4G in politično odločitev Slovenije, ki jo je predstavil minister Koprivnikar, da se množica profesionalnih infrastruktur poenoti in izvaja preko skupne vertikale 5G PPDR.

Po pogovorih z MJU/DID in pregledu osnutka dokumenta je JRC potrdil pripravljenost sodelovanja v iniciativi 5G. To bo za slovenski projekt 5G PPDR pomenilo:

- mednarodni značaj,
- promocijo slovenske industrije znotraj Evropske Unije in morda tudi širše (sodelovanje z ITU),
- standardizirano vertikalo 5G za PPDR,
- pomoč pri implementaciji te vertikale v izbranem testnem slovenskem mestu.

Glede morebitnega sodelovanja z Inštitutom Jožef Stefan in z njim sodelujočega HIPOT-R&D d.o.o. so pogovori še v teku. Gre za morebitno vključitev senzorjev kot pametne IoT-podpore uporabniškim scenarijem projekta 5G PPDR. Ti senzorji bodo morali podpirati protokole 3GPP, ki zahtevajo ultra nizke hitrosti in razširjeno pokrivanje, predvsem NB-IOT ali EC-GSM.

Na sestanku 20. 4. 2017 so deležniki predstavili svoje videnje in prispevek v projektu in definirali časovnico in uporabniške primere. Do naslednjega sestanka bodo deležniki dokončali osnutek osnovnega dokumenta in dokončno potrdili vloge.

DID in Agencija sta projekt predstavila Evropski komisiji dne 4. 5. 2017 v Bruslju.

IV. SCENARIJI PROJEKTA 5G PPDR

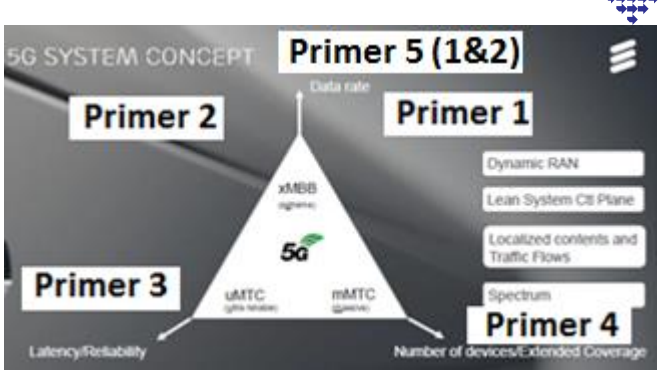
Projekt 5G PPDR ponuja novosti na tehničnem in regulatornem področju. Za začetek projekta je potrebno zagotoviti finančna sredstva zlasti za:

- laboratorijsko testiranje,
- vzpostavitev testnih okolij na terenu, za kar je potrebno pripraviti ustrezno promocijo in dati testnim uporabnikom na voljo opremo,
- za skupni nadzor in vodenje projekta.

Agencija projekt podpira z naslednjimi ukrepi:

- na razpolago za testiranje so frekvence v radiofrekvenčnem pasu 3400 – 3800 MHz (3430 – 3500 MHz/3530 – 3800 MHz);
- pripravil bo tehnične in regulatorne ukrepe za uvedbo kvalitete storitve (QoS), pomagal bo pri pripravi medresorskega regulatornega okvirja, ki bo t.i. »first responderjem« omogočilo prioritizacijo prometa v primerih nujnega posredovanja.

[8] 5G vtičnik v tem dokumentu pomeni dvoje: na strani core omrežja pomeni predvsem virtualizacijo, ki omogoča bolj fleksibilen dizajn omrežja glede na uporabniške primere / namenske omrežje rezine. Na strani radija pa so to 5G vtičniki "5G plugins" – posamične dopolnitve nad LTE-jem za 5G



Slika 5: Novosti 5G tehnologije zahtevane za 5G PPDR projekt – katere prednosti tehnologije bodo uporabljene v 5 uporabniških primerih (vir: Ericsson Public safety Slovenia USE CASE overall requirements and architecture study, April 2017)

Ostali deležniki so v osnutku dokumenta definirali tehnične zahteve za projekt 5G PPDR in scenarije uporabe za katere so zahtevane naslednje novosti tehnologije 5G (Slika 5):

– xMBB (extreme MBB/capacity) – ekstremne hitrosti prenosa za ekstremne količine podatkov – izziv je kapaciteta,
– mMTC(massive MTC/extended coverage) podpora množični komunikaciji – izziv je dodatna pokritost,
– uMTC(ultra reliable MTC/latency) – podpora ultra zanesljivi komunikaciji – izziv so zakasnitve in ekstremna zanesljivost.

Določili so pet scenarijev, ki pa bi jih lahko testirali na naslednjih treh primerih uporabe:

– velika športna prireditev,
– nadzor državne meje,
– nadzor cestnega prometa.

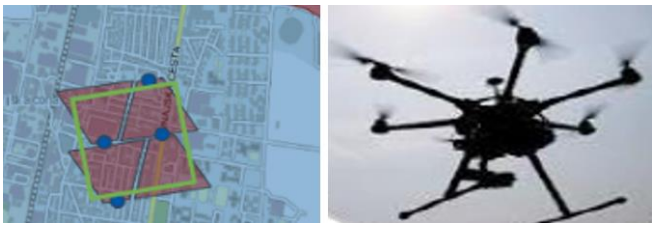
Teh pet scenarijev/primerov uporabe je:

1. Zagotavljanje varnosti ob množici udeležencev:

Slika 6: Primer 1 – varnost ob množici udeležencev (vir: Ericsson)

Lahko gre za množično prireditev na stadionu, nadzor meje ob navalu beguncev ali nadzor prometa ob zastoju/prometni nesreči. Pomembna je ekstremno velika prenosna hitrost množice podatkov. Uporabniški primer: prenos videa visoke razločljivosti v živo iz kamer, ki jih imajo policisti/reševalci na uniformi v kombinaciji z videonadzorom iz helikopterja do lokalnega robnega oblaka, kjer se vnaprej obdela. Pri tem so uporabljene funkcije, kot npr. prepoznavanje obrazov, prepoznavanje avtomobilskih registrskih tablic, prepoznavanje anomalij (v vedenju, prometu, …). Prenos tako obdelanega signala se prenese do glavne podatkovne baze centralnega oblaka skupaj s podatki o lokaciji. V primeru zaznane anomalije, se sproži alarm.

2. Stalni daljinski nadzor situacije:



Slika 7: Primer 2 – stalni daljinski nadzor situacije (vir: Ericsson)

Lahko gre za množično prireditev na stadionu, nadzor meje ob navalu beguncev ali nadzor prometa ob zastoju/prometni nesreči. Primer uporabe: prenos videa visoke razločljivosti iz velikega števila samo-krmiljenih dronov, ki jih spustimo nad neko območje. Operater nastavi območje na zemljevidu, ki ga želi daljinsko video nadzorovati. Nad območje prileti veliko število dronov s kamerami, ki sami skrbijo za navigacijo, se znajo izogibati oviram in upoštevajo vremenske okoliščine (veter), sami skrbijo za stanje baterije (ko je baterija blizu izrabe, ta dron pristane in namesto njega vzleti nov dron), pri pokrivanju danega področja z video nadzorom med seboj sodelujejo. Sami se odločijo, kdaj je potrebno snemati, varčujejo z baterijo. V primeru izpada mobilnega omrežja imajo možnost vzpostaviti začasno bazno postajo (na dronu). Potrebujemo lahek reduciran EPC z omejenimi funkcionalnostmi.

3. Daljinska kontrola in nadzor dronov/vozil in 112 nove generacije:

Slika 8: Primer 3 – daljinska kontrola in nadzor (vir: Ericsson)

Primer uporabe: krmiljenje dronov v realnem času/ daljinsko krmiljenje vozil (remote driving) /112 storitev nove generacije. Lastnosti take aplikacije so: združitev na nivoju centra za kontrolo in upravljanje (Event Command & Control Center), ki je lociran skupaj z aplikacijskim strežnikom v robnem oblaku, ultra zanesljivo omrežje z ultra nizkimi zakasnitvami, prenos podatkov v realnem času za: podatke o lokaciji povezanih/krmiljenih naprav in krmiljenje izven optične vidljivosti. Za storitev 112 nove generacije pa tudi souporaba podatkov o lokaciji in stanju državljanov centra 112 s »first responderjem« na terenu.

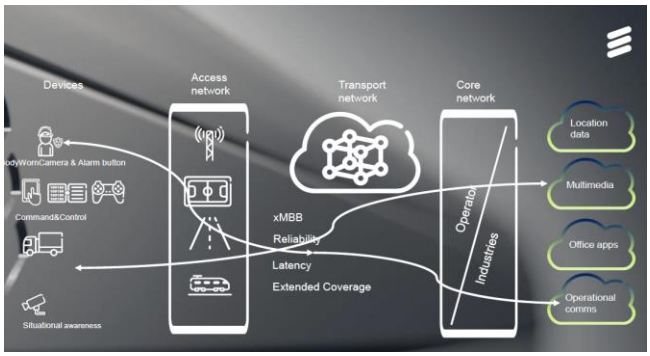
4. Zanesljiv prenos nujnih informacij:

Slika 9: Primer 4 – Zanesljiv prenos nujnih informacij (vir: Ericsson)

Primer uporabe: Alarmni gumb za pooblaščene osebe. Podpora za »first responderje«. Lastnosti storitve: ko se alarm sproži, mora biti sporočilo s čim bližje 100 %-zanesljivostjo brez napake dostavljeno centru za kontrolo in upravljanje (Command Control Center). Pomembna je zanesljivost prenosa signala, malo manj pomembna, a še vedno zaželena je majhna zakasnitev pri prenosu signala, zanesljivo mora biti delovanje omrežja in dobra pokritost ozemlja, mobilnost in nadzor predaje zveze mora biti brez motenj/prekinitev, pomembne so tudi tehnike za izboljšanje pokritosti.

5. Požar v kleti na veliki prireditvi (kombinacija primerov 1 in 2):

Uporabniški primer: gasilci gasijo v kleti, kjer je odpovedal protipožarni sistem, zaradi dima ni viden izvor požara. Droni, ki so bili poslani, da spremljajo požar, so izgubili povezavo z omrežjem 5G. Gasilci vzpostavijo IoT omrežje. Uniforme imajo opremljene s senzorji temperature, senzorji, ki zaznajo, če se zgrudijo na tla in gumbom SOS. Postavijo v prostoru senzorje temperature. Ko pogasijo požar, dve termični kameri še vedno nadzorujeta klet in video signal v živo prenašata preko omrežja 5G. Vzpostavijo se začasne bazne postaje (na dronu), senzorsko IoT omrežje, prenos videa v živo iz kamer, zanesljiv prenos signala z gumba SOS.



Vir:

Slika 10: Deli omrežja in posebni parametri za kvaliteto storitev, uporabljeni v štirih scenarijih 5G PPDR projekta (vir: Ericsson)

Slika 10 prikazuje, kateri deli omrežja in kateri posebni parametri za kvaliteto storitev so uporabljeni v štirih scenarijih projekta 5G PPDR. Slika 11 pa prikazuje vrednosti za posebne parametre kvalitete storitve 5G PPDR projekta.

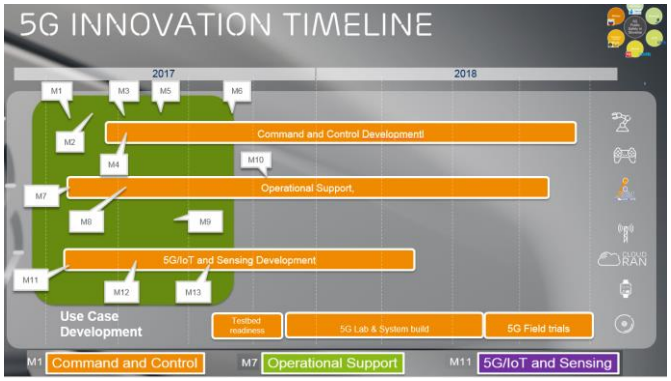
Performance Measure	Requirement
Peak data rate	DL: [20 Gbps] UL: [10 Gbps]
Peak spectral efficiency	DL: [30 bps/Hz] UL: [15 bps/Hz]
Spectrum Scalability	Yes
Bandwidth	Reference to IMT-2020
Control plane latency	[10 ms]
UP latency URLLC, one-way	[0,5 ms]
UP latency eMBB, one way	[4ms]
Latency for infrequent small packets	10s / 20byte packet
Mobility	Up to 500 km/h
Inter-system mobility	Yes
Reliability	[1-10^{-5}] in [1ms]
Ue Battery life	10-15 years
User experienced data rate	100/50 Mbps DL/UL [ITU]

Slika 11: Vrednosti parametrov iz trenutno sprejete verzije tehničnega poročila za 5G, ki bodo predvidoma uporabljeni v projektu (vir: Ericsson)

Projekt 5G PPDR bo sledil časovnici, zapisani v akcijski točki 1 dokumenta COM (2016) 588:

– 2017: preliminarna testiranja 5G znotraj 5G-PPP,
– 2018: prva nekomercialna testiranja preko državnih mej,
– do konca 2020 bo s tehnologijo 5G opremljeno vsaj eno večje mesto v Sloveniji in začel se bo komercialni start vertikale 5G za PPDR.

Slika 12 prikazuje planirano časovnico razvoja 5G-funkcionalnosti projekta 5G PPDR.



Slika 12: Časovnica razvoja 5G-funkcionalnosti projekta 5G PPDR.

V. NOVI SPEKTER ZA 5G PO WRC-19

Točka dnevnega reda AI 1.13 govori o frekvenčnih pasovih za tehnologijo 5G, ki jo na nivoju ITU imenujejo IMT-2020 in na WRC-19 želijo:

– pasove s primarno mobilno alokacijo določiti za IMT:
  – 24,25 – 27,5 GHz, 37 – 40,5 GHz, 42,5 – 43,5 GHz, 45,5 – 47 GHz, 47,2 – 50,2 GHz, 50,4 – 52,6 GHz, 66 – 76 GHz in 81 – 86 GHz;
– določiti za IMT in za primarno mobilno alokacijo:
  – 31,8 – 33,4 GHz, 40,5 – 42,5 GHz in 47 – 47,2 GHz.

Agencija podpira vse predlagane pasove. Zadržana je le glede podpasu 37 – 39,5 GHz, kjer bi bila uvedba IMT problematična zaradi velike uporabe fiksnih zvez v tem radiofrekvenčnem pasu. Ta pas je ključni pas za mobilne operaterje za tako imenovane »last mile« povezave do baznih postaj. Delovna skupina znotraj CEPT ECC-PT1 študira možno souporabo fiksnih in mobilnih zvez v okviru te točke dnevnega reda za WRC-19. Če bi se izkazalo, da je sobivanje možno v primeru, da ima določeni del spektra isti mobilni operater za fiksne in mobilne zveze, bi lahko uvedli IMT tudi v tem pasu.

Primarna pasova za 5G v Sloveniji sta skladno s mandatom za 5G Evropske komisije in časovnico CEPT pasova 3400 – 3800 MHz in 26 GHz (24,25-27,5 GHz). V podpasu 24,549 – 25,053 GHz / 25,557 – 26,061 GHz bi lahko izvajali testiranja 5G, saj ima Slovenija popisan mednarodni sporazum s sosednjimi državami za BWA. CEPT študira tudi radiofrekvenčni pas 40,5 – 42,5 GHz, za nas pa bi bil zanimiv frekvenčni pas 33,8 – 33,4 GHz. Oba pasova sta trenutno nezasedena in bi bila zelo primerna za uporabo v notranjosti zgradb in za dodatno kapaciteto za najbolj podatkovno obremenjene bazne postaje za razdalje do 50 m. Višji frekvenčni pasovi so zanimivi zaradi velikih kapacitet, a bi bili uporabni pretežno v notranjosti zgradb.

Evropska komisija je v mandatu za 5G od CEPT zahtevala tudi študije na pasu 28 GHz. Če bi te študije

pokazale, da ni motenj obstoječim storitvam (npr. FSS) in ne bi bilo prevelikega nasprotovanja ostalih članic EU, bi glede na to, da v tem pasu še nimamo izdanih odločb o dodelitvi radijskih frekvenc, lahko ta pas podprli.

Točka dnevnega reda AI1.16 govori o dodatnem spektru za brezžične dostopovne sisteme (WAS/RLAN) v frekvenčnem pasu med 5.150 MHz in 5.925 MHz – možne dodatne alokacije za mobilne storitve. Agencija bo podprla tiste dele pasu, za katere bodo študije pokazale, da je koeksistenca z ostalimi storitvami možna. Ker trenutno študije ne kažejo najbolj obetavnih rezultatov, je Agencija podprla predlog Švice in še nekaterih držav CEPT za dodatne študije v pasu 6 GHz za možno uporabo WAS/RLAN.

Glede dnevnega reda za WRC-23 AI 2.5 je DID skupaj z Agencijo podprl prizadevanja Finske za proučitev regulatornega okvirja za uvedbo IMT v pasu 470 – 694 MHz v Regiji 1, kar bi omogočilo fleksibilno uvedbo novih platform za avdiovizualne vsebine preko omrežij 4G/5G, vključno z novimi multimedijskimi storitvami IPTV in OTT v načinih unicast, multicast ali broadcast.

LITERATURA

[1] Commission, European. (14. 9 2016). COM(2016) 588 final: 5G for Europe: An Action Plan {SWD(2016) 306 final}. Brussels.
[2] „5G-PPP, 5G Vision,“ https://5g-ppp.eu/roadmaps/, 2016.

Meta Pavšek Taškov je diplomirala leta 1990 in magistrirala leta 1993 na Fakulteti za elektrotehniko. Od leta 1989 je bila zaposlena v Iskri Hipot – Šentjernej, v mešanem razvojno raziskovalnem oddelku Inštituta Jožef Stefan in Iskre Hipot na Inštitutu Jožef Stefan v Ljubljani. Od leta 1995 je zaposlena na AKOS (Agenciji za komunikacijska omrežja in storitve RS), ki se je takrat imenovala Uprava RS za telekomunikacije, in sicer na področju za radiokomunikacije oz. upravljanje radiofrekvenčnega spektra. Leta 2012 in 2013 je bila vodja projekta LTE, 2014 pa namestnica predsednice razpisne komisije za javni razpis z javno dražbo za mobilne tehnologije v pasovih 800/900/1800/2100/2600 MHz. Novembra 2015 se je udeležila svetovne radijske konference WRC-15 kot namestnica vodje delegacije. Od leta 2016 je vodja oddelka za mobilne zveze na AKOS.

IoT za pametna mesta

Marjan Turk, Direktorat za informacijsko družbo, Ministrstvo za javno upravo Republike Slovenije

Povzetek – Prispevek opisuje predlog projekta *IoT za pametna mesta*, ki predvideva uporabo tehnologije IoT, masovnih podatkov in računalništva v oblaku za digitalizacijo mest in skupnosti. Predlagana je vzpostavitev standardne integracijske platforme *IoT za digitalno Slovenijo* in sistematično uvajanje IoT senzorskih omrežij v mestih. Na osnovi generiranih masovnih odprtih javnih podatkov bodo razvite inovativne storitve za različna področja družbenega udejstvovanja na lokalni ravni.

Ključne besede – digitalizacija, pametna mesta in skupnosti, IoT, masovni podatki, računalništvo v oblaku, odprti javni podatki, digitalna družba, digitalno preoblikovanje

I. UVOD

V zadnjih letih je z razvojem digitalnih tehnologij in interneta digitalizacija postala globalni mega-trend številka ena. Kdor je med digitalno aktivnimi, napreduje, kdor ne, še hitreje nazaduje. Če se želimo uvrstiti med napredne digitalne družbe in si zagotoviti ustrezno mesto v Evropskem enotnem digitalnem prostoru ter ohraniti oz. povečati raven blaginje, izbire ni. Strategija razvoja informacijske družbe do leta 2020 tako določa, da bo Slovenija investirala v digitalizacijo družbe in podjetništva, v digitalno rast in kompetence ter zasledovala strateško usmeritev inovativne in intenzivne uporabe IKT in interneta na vseh razvojnih področjih. Vizija Slovenije je, da s pospešenim razvojem digitalne družbe izkoristi razvojne priložnosti IKT in interneta, postane napredna digitalna družba in referenčno okolje za inovativno uporabo digitalnih tehnologij.

Nezadržna širitev urbanizacije je svetovni trend, ki pred mesta in skupnosti postavlja naloge obvladovanja perečih problemov naraščajočega prebivalstva v mestnih območjih. Mesta se soočajo s številnimi problemi, ki ogrožajo njihov trajnostni razvoj; od velike gostote poseljenosti, gospodarskih izzivov, neustrezne mestne infrastrukture za transport, oskrbo z vodo, energijo in upravljanje z odpadki, do potreb po sodobni komunikacijski in informacijski digitalni infrastrukturi. Trajnostni razvoj mest je pogojen z učinkovitim spopadanjem z naštetimi problemi, ki so kompleksni, dinamični in medsebojno prepleteni, zato jih je treba podrobno spoznati. Mesta morajo priti do ustreznih instrumentov in nove ravni inteligence – postati morajo pametna. Uporaba naprednih digitalnih tehnologij za reševanje razvojnih, gospodarskih in političnih izzivov, s katerimi se soočajo, je v tem kontekstu izbira, ki nima alternative.

Mesta so gospodarsko, tehnološko in politično močnejša, kot so bila kadarkoli prej in so v razvitih digitalnih družbah v Evropi gonilo rasti in ustvarjanja. V teh okoljih, v katerih živi tri četrtine Evropejcev in polovica Slovencev, ustvarjajo tudi do 85 % BDP, kar lahko pripišemo učinkoviti izrabi razvojnega potenciala digitalnih tehnologij za oblikovanje digitalno spodbujenih priložnosti za poslovanje, izobraževanje, kreativnost in storitve, ki povečujejo produktivnost, učinkovitost in raven blaginje. Spremembe, ki jih prinaša digitalna doba, še posebej v mestih učinkovito odpravljajo dosedanje ovire za poslovanje, komunikacije in družbeno udejstvovanje. Prednosti intenzivne in inovativne uporabe digitalnih tehnologij postavljajo mesta in lokalne skupnosti v jedro digitalnega preoblikovanja družbe. V prizadevanjih za digitalno preoblikovanje so ravno lokalna okolja najbolj primerna za vzpostavitev partnerstev, razvoj kompetenc, generiranje in uporabo novih podatkovnih virov, investiranje v digitalno infrastrukturo in digitalno reševanje problemov lokalnih skupnosti. S široko uporabo digitalnih tehnologij lahko mesta postanejo pametna, si zagotovijo trajnostni razvoj ter spodbudno vplivajo na rast in blaginjo v državi.

Čeprav je Slovenija ena izmed najbolj razpršeno in redko poseljenih držav v Evropski uniji (v mestih živi le okoli polovica prebivalstva), se mora, če se želi pripraviti na prihodnje izzive, tudi naša država čimprej podati na pot intenzivne digitalizacije mest. Pri tem moramo upoštevati, da je hierarhično neodvisno in nepovezano razvojno okolje lokalne samouprave za projekte digitalizacije zelo zahtevno. Iskanje odgovorov na vprašanja; kam, po kateri poti in kako naprej, je zato vse prej kot enostavno. Strateške vidike usmerjanja razvoja morajo nasloviti lokalne skupnosti same, njihova združenja, delno tudi državna uprava, hkrati pa ne gre prezreti tudi tržnega interesa IKT-podjetij, ki ponujajo digitalne storitve in rešitve za pametna mesta. Kakšna je v teh okvirih lahko vloga države in kam usmeriti omejena razvojna sredstva?

II. DIGITALIZACIJA MEST IN SKUPNOSTI

Pametno mesto določajo trije elementi, ki mu omogočajo trajnostni razvoj:

- podatkovna analitika za boljše odločitve,
- sposobnost predvidevanja problemov, njihovo proaktivno reševanje in minimiziranje posledic,
- koordiniranje virov in procesov za hitro odzivanje in učinkovito delovanje.

Slika 1: Komponente pametnega mesta (IBM)

Pametno mesto mora biti sposobno učinkovito upravljati vire za zadovoljevanje družbenih, gospodarskih in okoljskih potreb v dobrobit občanov, kar pa je vse prej kot lahka naloga, saj so mesta pogosto organizirana po ločenih področjih in so le redko upravljana kot celovita entiteta, po navadi pa odločevalci tudi nimajo vpogleda v dogajanje v mestu v realnem času, niti ne kvalitetnih agregiranih podatkov, na osnovi katerih bi lahko sprejemali odločitve. Navedeni izzivi kličejo po digitalizaciji, ki lahko bistveno pripomore k usposobljenosti mest za njihovo reševanje.

Digitalizacija mesta in skupnosti pelje po poti zahtevnega preoblikovanja, ki vključuje družbene, gospodarske, urbane, mobilnostne, izobraževalne, tehnološke in kulturne spremembe. Mesta s tem postajajo izhodiščna digitalna platforma za digitalno preoblikovanje celotne družbe, kar navaja tudi strategija Digitalna Slovenija 2020, v kateri je razvoj pametnih mest in skupnosti ena izmed dveh vsebinskih prioritet.

Slika 2: Ključni elementi pospeševanja digitalnega preoblikovanja mest in skupnosti.

Tehnološko zahtevne projekte je možno obvladovati le z načrtnim vlaganjem v razvoj digitalnih kompetenc, s posebnim poudarkom na izobraževanju odločevalcev na lokalni in državni ravni. Uvajanje rešitev temelječih na internetu stvari zahteva dobro razvito digitalno informacijsko in komunikacijsko infrastrukturo, kar zahteva osredotočene investicije, kjer primerne infrastrukture še ni na voljo. Eden izmed rezultatov digitalizacije je generiranje obsežnih podatkov, ki so lahko ob ustrezni analitiki in vizualizaciji dragocen vir podatkov za odločevalce, ki mesta upravljajo in strateško usmerjajo njihov razvoj, med drugim tudi njihovo digitalizacijo, s ciljem oblikovanja pametnih mest.

Ob tako pomembni vlogi, kot jo imajo mesta in skupnosti v digitalnem preoblikovanju družbe, je treba upoštevati dejstvo, da je lokalna samouprava deklarativno neodvisna in da to lahko vodi v neusklajeno digitalizacijo. Nesistematična implementacija digitalnih tehnologij pa lahko že v izhodišču bistveno zmanjša potencial izrabe prednosti, ki temelji na:

– povezovanju,
– odprtosti in dostopnosti,
– uporabi standardnih rešitev,
– pravilih interoperabilnosti,
– analitiki masovnih podatkov in
– souporabi digitalne infrastrukture.

Čeprav je lokalna samouprava del celovitega državnega sistema so lokalne skupnosti pri informatizaciji in razvoju lokalne e-uprave vse od reorganizacije lokalne samouprave leta 1996 bolj ali manj prepuščene same sebi, zato je tokrat treba digitalizacijo mest zastaviti bolj sistematično, usklajeno in na osnovi širokega povezovanja.

Strateško vodenje digitalnega preoblikovanja mest in skupnosti mora temeljiti na dolgoročnih strategijah in razvojnih partnerstvih, ki morajo omogočati neovirano sodelovanje med lokalnimi skupnostmi, sektorji in vrednostnimi verigami na lokalni in regijski ravni ter zagotoviti sistemsko povezanost s prizadevanji na državni ravni. Za povezovanje in skupne projekte je treba izkoristiti obstoječa združenja občin (Skupnost občin Slovenije, Združenje občin Slovenije in Združenje mestnih občin Slovenije), Strateško razvojno inovacijsko partnerstvo[1] Pametna mesta in skupnosti[2] in na strateški ravni Slovensko digitalno koalicijo[3].

III. PROJEKT IOT ZA PAMETNA MESTA

Sistemski pristop in povezovanje lahko država spodbudi s sofinanciranjem projektov digitalizacije mest in skupnosti, pri katerih zahteva čim širše povezovanje v lokalnem in regionalnem okolju ter sistemsko umestitev projektov na državni ravni. Pri tem se moramo vprašati, kateri so tisti izzivi, ki jih morajo mesta nasloviti najprej, s kakšnimi tehnologijami in po kakšnem modelu?

V okoliščinah hitre urbanizacije in širitve mest izzivi njihovega upravljanja izhajajo iz šestih kompleksnih sistemov različnih omrežij, infrastrukture in podpornih storitev, namenjenih:

– občanom (javna varnost, zdravstvo in izobraževanje),
– gospodarstvu (podporno okolje, regulacija),
– transportu,
– komunikacijam (optična in mobilna omrežja),
– vodooskrbi in
– energiji.

Z naglo širitvijo mest je sistem sistemov vse težje obvladljiv, zato ga morajo mesta z uporabo novih tehnologij prilagoditi novi stvarnosti urbanizacije in si z optimizacijo uporabe omejenih virov zagotoviti trajnostni razvoj.

Izmed digitalnih tehnologij imajo glede na naravo problemov, ki se jih rešuje, največji potencial:

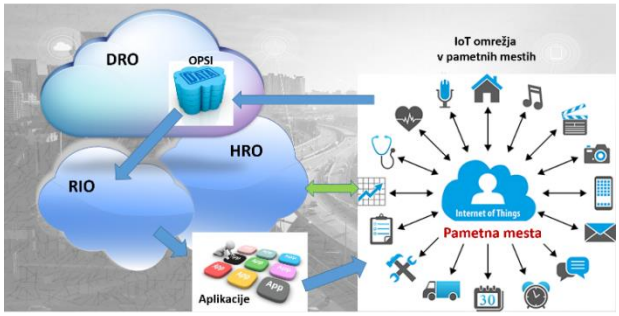
– tehnologija interneta stvari (IoT)[4], oz. prihodnjega interneta
– storitve računalništva v oblaku in
– tehnologija masovnih podatkov, predvsem v navezi z odprtimi javnimi podatki.

Cilj uporabe tehnologije interneta stvari v mestih in skupnostih je razviti povezan inteligentni sistem, ki bo prispeval h gospodarskim dejavnostim, izboljšal zadovoljstvo občanov z javnimi storitvami, prispeval k javni varnosti, trajnostnemu upravljanju z okoljem, učinkovitejšemu upravljanju mest in k spopadanju z drugimi izzivi, s katerimi se soočajo mesta in skupnosti.

Lokalnim skupnostim se sofinancira uvajanje senzorskih omrežij IoT, s katerimi bodo mesta in skupnosti reševala svoje najbolj pereče probleme. Podpre se projekte, ki rešujejo realne potrebe iz lokalnega okolja, sicer projekti ne bodo prispevali k pametnejšemu soočanju z mestnimi problemi.

[1] SRIP – Strateško razvojno inovacijsko partnerstvo
[2] PMiS – Pametna mesta in skupnosti
[3] Slovenska digitalna koalicija – digitalna.si
[4] IoT – Internet of Things, internet stvari

Uporabi se tehnologije merjenja stanja in spremljanja okolja, kar bo skozi višje ravni zlivanja podatkov omogočilo zajem celotne slike stanja, analitiko zbranih masovnih podatkov in ustrezne odzive na dano stanje, preko aktuatorjev pa se je možno tudi odzivati. Spodbuja se povezovanje lokalnih skupnosti oz. projekte, ki bodo vključevali čim večje število lokalnih skupnosti, po možnosti organiziranih na ravni združenj občin.



Slika 3: Shema uporabe tehnologije IoT, oblačnih storitev in tehnologije masovnih podatkov za pametna mesta.

Vzpostavi se standardna integracijska platforma *IoT za digitalno Slovenijo*, ki bo na osnovi njene odprtosti in celovitosti omogočila:

– zbiranje podatkov v standardiziranih formatih,
– enostaven dostop do virov podatkov,
– napredno analitiko in vizualizacijo zbranih masovnih podatkov in
– lažji razvoj inovativnih storitev.

Uporabljene tehnologije so zelo kompleksne, zato jih posamezno podjetje ali projektni partnerji težko obvladujejo. Standardna integracijska platforma se mora zato osredotočiti na:

– vzpostavitev dolgoročnih povezav med sodelujočimi,
– odprtost integracijske platforme,
– zagotovitev rasti platforme in
– stalno inoviranje.

IoT projekti mest in skupnosti morajo biti skladni s standardno integracijsko platformo in uvajati odprte, standardne rešitve, ki bodo temeljile na semantičnih in sintaktičnih interoperabilnostnih pravilih z integracijo odprtih standardov. Podatke, ki jih generirajo senzorska omrežja in ki so zanimivi za razvijalce in uporabnike, se objavi oz. omogoči dostop do njih na nacionalnem portalu odprtih podatkov OPSI[5] in hkrati operativno tudi preko Razvojno inovacijskega oblaka[6]. Na osnovi odprtih podatkov senzorskih IoT omrežij, ki bodo v standardiziranih formatih objavljeni v strojno berljivi obliki in dostopni preko odprtih API-jev[7], in ob dostopnosti do drugih javno-pravnih evidenc, bodo razvijalci v okolju RIO lahko izvajali napredno analitiko in vizualizacijo masovnih podatkov ter razvijali inovativne storitve in aplikacije. S tem bodo med drugim reševali potrebe mest po kvalitetno agregiranih in vizualiziranih podatkih, ki jih potrebujejo pri odločanju in izvajanju javnih funkcij.

Lokalne skupnosti bodo lahko uporabljale storitve računalništva v oblaku, ki jih država ponuja v okviru:

– državnega računalniškega oblaka[8], v katerem je nameščen OPSI,
– hibridnega računalniškega oblaka[9], v katerem bodo na voljo različne informacijske storitve za lokalne skupnosti in
– razvojno inovacijskega oblaka, v katerem bo na voljo razvojno okolje za razvoj storitev na osnovi podatkov iz javno-pravnih evidenc in orodja za analizo in vizualizacijo masovnih podatkov iz senzorskih IoT omrežij pametnih mest.

Standardna integracijska platforma *IoT za digitalno Slovenijo* bo s povezanim in usklajenim uvajanjem tehnologije IoT, računalništva v oblaku in masovnih podatkov domačim IKT podjetjem omogočila razvoj tehnologij in rešitev, s katerimi bodo konkurenčni tudi na tujih trgih. Tehnološko in organizacijsko konsistentna in z deležniki usklajena specifikacija standardne integracijske platforme je ključni faktor uspeha projekta uvajanja IoT v mestih in skupnostih.

V celotnem ekosistemu integracijske platforme bo največji izziv zagotavljanje povezljivosti in interoperabilnosti rešitev, zato je treba dosledno zahtevati odprtost vmesnikov, ki morajo omogočati enostavno povezovanje in objavljanje informacij, kontekstualno povezovanje med storitvami ter zbiranje in obdelovanje informacij v realnem času. Drugi izzivi so še organizacijska kompleksnost in povezovanje, upravljanje z masovnimi podatki, povezljivost, varnost, interoperabilnost, integracija z državnimi IT sistemi in upravljanje celotnega sistema.

IV. TEHNOLOGIJE ZA PAMETNA MESTA

A. *IoT – Internet stvari*

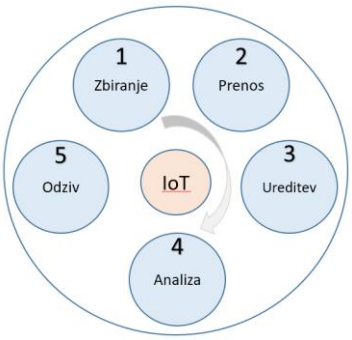
Tehnologija interneta stvari spreminja način interakcije uporabnikov, storitev in aplikacij z okoljem realnega sveta na varen način. Kot termin se je internet stvari pojavil pred 18 leti za oznako potencialov RFID, danes pa se z njim označuje omrežja senzorjev, ki podatke posredujejo v računalniški oblak, ali pa aktuatorje, ki jih je možno upravljati na daljavo.

Z ustreznim razumevanjem podatkov iz senzorskih omrežij interneta stvari lahko država omogoči boljše javne storitve za državljane, prilagojene osebnim potrebam posameznikov in posameznim situacijam, zagotovi lahko večjo transparentnost svojega delovanja ter z uporabo preventivne in prediktivne analitike tudi izboljša življenjsko okolje občanom.

Tok podatkov, zbranih z uporabo senzorskih omrežij IoT, gre skozi pet stopenj:

1. pasivno zbiranje podatkov o realnem okolju,
2. komunikacija IoT naprav z drugimi napravami ter s centralno in/ali porazdeljeno IoT platformo,
3. ureditev zbranih podatkov iz različnih virov in zapis v standardni – dogovorjeni format,
4. analitika masovnih (zbranih) podatkov, iskanje vzorcev za odziv in nadaljnje analize,
5. izbira odziva glede na ugotovitve analitike.

[5] OPSI – Odprti podatki Slovenije
[6] RIO – Razvojno inovacijski oblak
[7] API – Application Programming Interface
[8] DRO – Državni računalniški oblak
[9] HRO – Hibridni računalniški oblak

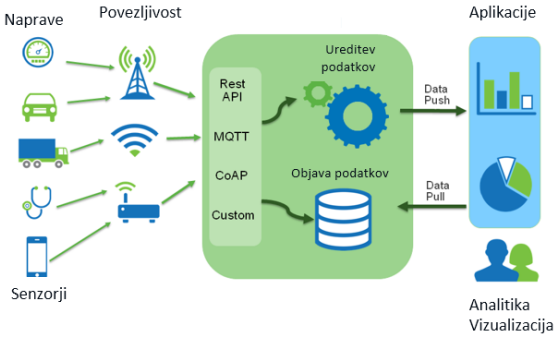


Slika 4: IoT tok podatkov

Uvajanje tehnologije IoT mora zagotoviti sklenitev celotnega tokokroga podatkov, ki jih generirajo senzorska omrežja. V nasprotnem podatki ne bodo kvalitetni, ustrezno analizirani, ali pa ne bodo prispevali k boljšim storitvam za občane in k trajnostnemu razvoju mest. V ta namen je pomembno predvideti vmesni sloj, ki bo zadolžen za orkestracijo obravnave podatkov v IoT omrežju in obvladovanje signalizacije pri množici raznovrstnih naprav in senzorjev. Zato je treba vsem fazam toka podatkov posvetiti ustrezno pozornost pri pripravi standardne integracijske platforme *IoT za digitalno Slovenijo*, ki mora vključevati:

- arhitekturo celotnega sistema, vključno z razdelitvijo funkcionalnosti med lokalno ravnijo in centralnimi funkcijami v Razvojno inovacijskem oblaku,
- standardne odprte vmesnike med različnimi nivoji sistemske arhitekture, ki mora omogočati povezovanje in fleksibilnost za morebitno preureditev vlog oz. porazdeljeno izvajanje funkcij,
- standardne formate zbranih podatkov in interoperabilnostna pravila,
- senzorsko platformo za spremljanje parametrov mesta, ki vključuje senzorje za merjenje kvalitete zraka, svetlobnega sevanja, zvočne onesnaženosti, za spremljanje dogajanja v okolju (požari, video nadzor z analitiko prepoznave vzorcev, indukcijske zanke v transportu, prometna signalizacija,…) in druge, s katerimi je možno spremljati dogajanje in kvaliteto okolja v mestih in skupnostih, kjer bivajo občani,
- referenčno komunikacijsko infrastrukturo za povezovanje senzorjev, ki bo temeljila na sodobnih brezžičnih tehnologijah, kot so 5G, LTE-M[10], LTE-NB[11], LPWAN[12], LoRaWAN[13] ipd.,
- standardne odprte API-je za dostop do podatkov,
- standardne odprte vhodne API-je, ki bodo omogočali zbiranje ostalih podatkov iz mest in skupnosti ter drugih javnih služb in podjetij v javni lasti,
- določiti vlogo OPSI in RIO,
- programska orodja za analitiko in vizualizacijo masovnih IoT podatkov,
- mobilne aplikacije za zbiranje, analizo in vizualizacijo masovnih IoT podatkov,
- pravila za uporabo zbranih masovnih IoT podatkov.

Tehnologije interneta stvari v veliki meri niso standardizirane, kar še posebej velja za najnižji nivo brezžičnih komunikacij. Izbira brezžičnega omrežja za naprave interneta stvari vključuje tehtanje med nasprotujočimi si zahtevami, kot so doseg, trajanje baterije, pasovna širina, gostota, investicijski stroški in stroški delovanja. Pri izbiri rešitev naj bi skladno z navedenimi kriteriji po eni strani prednost imele rešitve, prilagojene specifičnim potrebam različnih vrst senzorskih omrežij, po drugi strani pa brezžične komunikacijske rešitve, ki temeljijo na infrastrukturi ponudnikov javnih komunikacijskih storitev, in ki ne bi zahtevale dodatnih vlaganj v komunikacijsko infrastrukturo.



Slika 5: Arhitektura IoT

Zajemanje podatkov se ne sme omejiti le na javno dostopna ali zasebna namensko postavljena senzorska omrežja, ali le na podatke različnih služb in podjetij, temveč je treba predvideti tudi participativno posredovanje podatkov, ki jih občani lahko aktivno prispevajo preko aplikacij za pametne telefone, spletnih strani in sporočil. Podatke je treba zajeti na čim več področjih in s tem dodatno odpreti priložnosti za povečevanje učinkovitosti procesov ter kakovosti življenja. Standardna integracijska platforma *IoT za digitalno Slovenijo* mora predvideti vse kanale zajemanja podatkov, možnih načinov komunikacije in uporabe tehnologije masovnih podatkov za analitiko, vizualizacijo in razvoj inovativnih storitev. Posebej se predvidi razvoj mobilnih aplikacij za zajem podatkov in za uporabo zbranih masovnih podatkov.

V projekt sistematičnega uvajanja tehnologije IoT je treba komplementarno vključiti tudi različne javne službe in podjetja v javni lasti, ki načrtujejo posodobitev ali gradnjo novih senzorskih omrežij IoT za lastne potrebe. Spodbuja se vsestranska uporaba dogovorjene standardne integracijske platforme v mestih in skupnostih, v širšem javnem sektorju in tudi v zasebnem sektorju. Z vidika zbiranja raznovrstnih podatkov bi lahko posebno velik potencial imelo dogovorjeno ali prostovoljno odpiranje podatkov inovativnih podjetij sodelovalnega gospodarstva, ki želijo poslovati v Sloveniji. Bolj ko bodo zbrani masovni podatki celoviti, boljše bodo možnosti razvoja inovativnih, polno funkcionalnih in uporabniško prijaznih storitev na njihovi osnovi.

B. Podporna tehnologija masovnih podatkov v Razvojno inovacijskem oblaku

Digitalna družba temelji na sposobnosti izrabe velikih količin podatkov (masovnih podatkov) za nove rešitve in storitve za spreminjanje obstoječih in oblikovanje novih poslovnih modelov in načinov delovanja. Vloga tehnologije masovnih podatkov je z razvojem prihodnjega interneta oz. interneta stvari, hitrejšimi komunikacijami in novimi informacijskimi tehnologijami vse večja. Izjemna rast obsega, spremenljivost in različnost masovnih podatkov

[10] LTE-M – LTE Machine to Machine
[11] LTE-NB – LTE Narrow Band
[12] LPWAN – Low Power Wireless Area Networks
[13] LoRaWAN– Long Range brezžična WAN tehnologija

predstavljajo izzive in hkrati ponujajo razvojne priložnosti, ki lahko vodijo do velikih gospodarskih in družbenih koristi. Analiza in obdelava obsežnih količin podatkov omogočata poslovne priložnosti, javna uprava pa lahko z odpiranjem javnih podatkov vsem zainteresiranim omogoči razvoj novih raznovrstnih inovativnih storitev.

Poleg javno pravnih evidenc, ki so pod natančno določenimi pogoji večinoma že dostopne razvijalcem, je v javnem sektorju še veliko neizkoriščenih priložnosti sistematičnega odpiranja javnih podatkov. Na celovito enotno ureditev dostopa čakajo predvsem podatki, ki jih generirajo senzorska omrežja različnih javnih služb in podjetij v javni lasti. Vsekakor je treba to nalogo vključiti v okvir širšega uvajanja interneta stvari v posodobljenih obstoječih in v novo digitaliziranih okoljih javnega sektorja.

Z *razvojno inovacijskim oblakom* bo vzpostavljeno razvojno okolje za podjetja, start-up-e, raziskovalce, študente, javne inštitucije, nevladne organizacije in posameznike, ki bodo z uporabo skupne IT infrastrukture, ki bo v največji možni meri virtualizirala IT okolja državne uprave, lažje in hitreje razvijali napredne e-storitve, e-vsebine in IKT rešitve. S tem bodo podprti razvojno inovacijski projekti e-storitev, mobilnih aplikacij in IKT-rešitev, zasnovanih na sodobnih razvojnih konceptih, temelječih na razvojnih priložnostih odprtih javnih podatkov in interneta. Na vzpostavljeni infrastrukturi se spodbuja povezovanje z uporabniki, razvoj po potrebah iz realnega okolja in participacijo zainteresiranih razvijalcev, ki bodo pri razvoju izkoristili in povezali IoT, računalništvo v oblaku, odprte javne in raziskovalne podatke, tehnologijo masovnih podatkov in mobilne tehnologije.

Za resnično sprostitev digitalnega potenciala masovnih podatkov je treba slovensko družbo in gospodarstvo pripraviti na nove izzive in usposobiti za izrabo priložnosti. Zaostajanje Evrope pri razvoju tehnologije masovnih podatkov, zaradi česar bi lahko odpiranje javnih podatkov prineslo koristi le konkurenčnejšim globalnim tekmecem, tudi Sloveniji narekuje okrepitev vlaganj v raziskave in razvoj lastnih omogočitvenih tehnologij, digitalne infrastrukture in znanja. Sistematično je treba razvijati tehnologijo za obdelavo, analitiko ter vizualizacijo masovnih podatkov, razvijati svoje vire javnih podatkov in infrastrukturo za njihovo izmenjevanje. S prilagajanjem pravnega okvira in razvojnih politik se oblikuje spodbudno razvojno okolje za podatkovno vodeno gospodarstvo (interoperabilnost, varstvo podatkov, varstvo potrošnikov, varnost omrežij, intelektualna lastnina, regulativna stabilnost, vzpostavitev zaupanja potrošnikov v podatkovne tehnologije).

Za dostop do podatkov, njihovo zbiranje in analitiko se v okviru projekta *IoT za pametna mesta* v RIO vzpostavi oblačno platformo *"Odprti podatki Slovenije"*. Platformo za masovne odprte javne podatke se specificira v okviru standardne integracijske platforme *IoT za digitalno Slovenijo*.

Predvidi se aplikativna orodja za zbiranje, orkestracijo, analitiko in vizualizacijo masovnih podatkov iz senzorskih omrežij pametnih mest in drugih institucij javnega sektorja. Vzpostavi se interaktivno spletno mesto, preko katerega bodo dostopni masovni IoT in drugi javni odprti podatki. Ti morajo biti dostopni tudi preko odprtih programskih vmesnikov, kar bo omogočilo razvoj inovativnih storitev in odprto inoviranje. Interaktivni spletni vmesnik mora omogočati enostavne, intuitivne in prijazne vizualizacije podatkov, ki bodo prinašali uvide in odkrivali neznano, nepričakovane vzorce, izjeme in povezave v množicah podatkov in med njimi ter tako izboljšali odločanje in sodelovanje. Na platformi se specificira tudi odprte vhodne programske vmesnike, ki bodo omogočali zbiranje ostalih podatkov iz mest in skupnosti ter drugih javnih služb in podjetij v javni lasti.

V. ZAKLJUČEK

S projektom *IoT za pametna mesta* se s povezovanjem razvojnih aktivnosti in usklajenim razvojem zasleduje medsektorske multiplikativne razvojne učinke in razvoj naprednih storitev ob manjših investicijskih stroških za javni in zasebni sektor. Projekt je zasnovan na uporabi tehnologije IoT v mestih in skupnostih ter komplementarni uporabi tehnologije masovnih podatkov in računalništva v oblaku. Izvedba zahteva sodelovanje večjega števila deležnikov iz državne uprave, lokalne samouprave, zasebnega sektorja in tudi končnih uporabnikov digitalnih storitev. Predlog projekta je zastavljen tako, da spodbuja povezovanje lokalnih skupnosti, razvijalcev, ponudnikov storitev in uporabnikov ter razvoj rešitev po potrebah iz realnega okolja.

Cilj je spodbujanje sistematične implementacije tehnologij IoT senzorskih omrežij v realnih okoljih, s ciljem vzpostavitve čim širšega nacionalnega IoT omrežja na osnovi izbrane integracijske platforme. Prednostno se podpre projekte mest in skupnosti, ki bodo poleg IoT inovativno izkoristili in učinkovito povezali tehnologije prihodnjega interneta, računalništva v oblaku, masovnih podatkov, visoko zmogljivega računalništva, mobilnih tehnologij ter odprtih javnih in raziskovalnih podatkov. Predvideno je spodbujanje drugih javnih služb in podjetij v javni lasti k posodobitvi obstoječih in razvoju novih senzorskih omrežij po dogovorjenih standardih in pravilih. Vzpostavi se standardno integracijsko platformo *IoT za digitalno Slovenijo*, ki bo s svojo celovitostjo in odprtostjo omogočila sistematičen usklajen razvoj in interoperabilne rezultate v obliki masovnih odprtih javnih podatkov. Za zbiranje, objavo, obdelavo in analitiko masovnih IoT podatkov bo na infrastrukturi Razvojno inovacijskega oblaka oblikovana platforma *"Odprti podatki Slovenije"*, na kateri se bodo lahko objavili tudi odprti podatki inovativnih podjetij sodelovalnega gospodarstva, ki bi želela poslovati v Sloveniji.

Bolj ko bodo zbrani masovni podatki celoviti, urejeni in dostopni, lažje jih bo analizirati in vizualizirati ter na njihovi osnovi razvijati inovativne storitve.

Z izvedbo projekta *IoT za pametna mesta* bodo mesta lahko sprejemala boljše odločitve, ponujala boljše javne storitve za občane in gospodarstvo ter si zagotovila trajnostni razvoj.

LITERATURA

[1] IoT: New Paradigm for Connected Government, Dr. Gopala Krishna Behara, maj 2017.
[2] A vision of smarter cities, IBM Institute for Business Value.
[3] Predlog SRIP Pametna mesta in skupnosti, april 2017.
[4] Predlog SRIP PMiS, Horizontalna IKT mreža, april 2017.
[5] DIGITALNA SLOVENIJA 2020 – Strategija razvoja informacijske družbe do leta 2020, Ljubljana, marec 2016.

Marjan Turk je zaposlen na Direktoratu za informacijsko družbo pri Ministrstvu za javno upravo.

Koraki do uresničitve vizije 5G

Janez Öri, Ana Robnik, Simon Čimžar, Iskratel, Slovenija

Povzetek — Pričakovane zahteve za omrežja 5G, ki jih prinašajo različni primeri uporabe v industrijskih in drugih sektorjih ter pri potrošnikih, niso več uresničljive z manjšimi nadgradnjami obstoječih omrežij. Zato je potrebna vizija omrežja 5G in njena uresničitev, ki že vključuje načrtovalske principe, ki bodo podprli vedno nove inovativne storite in aplikacije v teh omrežjih. Članek opisuje kaj obsega vizija omrežja 5G, širši poslovni kontekst pri uvajanju 5G omrežij ter rešitve, ki jih operaterji lahko začnejo uvajati danes, tudi rešitve podjetja Iskratel.

Ključne besede — 5G, NFV/SDN, Oblak, vIMS, internet stvari

Abstract — Expected requirements for 5G networks that have been posted within use cases of industrial and other sectors and also consumers will not stand the challenge of minor upgrades of today's networks. A new 5G vision is required and its realization, which already includes design principles that will support newly defined services and applications using 5G networks. This article explains vision of 5G networks, broader business context when implementing steps towards 5G networks and solutions which are available today, including those from Iskratel.

Keywords — 5G, NFV/SDN, Cloud, vIMS, IoT

I. UVOD

5G prinaša revolucijo v telekomunikacijsko industrijo. Obljuba po ultra-nizkih zakasnitvah in povečani zanesljivosti, bistveno povečanih prenosnih zmogljivostih ter cenovno optimalni programabilni in virtualizirani omrežni arhitekturi, motivira mobilne in konvergenčne ponudnike komunikacijskih storitev (operaterje), da so pričeli s tehnološko in poslovno pripravo, ne glede na status 5G standardov. Omrežje 5G ne bo namenjeno le zagotavljanju čedalje višjih hitrosti za povezovanje uporabnikov do spleta, ampak bo omogočalo bistveno več: povezovanje stvari (internet stvari) in zagotavljanje bistveno bolj prilagodljivih omrežnih karakteristik glede na zahteve posameznih aplikacij. To bo omogočilo uporabo 5G v rešitvah, kot so pametna mesta, inteligentni transport in logistika, energetika, industrijska proizvodnja, javna varnost, zdravje in drugje. Nove povezljivosti in razširjen nabor storitev na teh področjih pa pomenijo za operaterja pomembne nove priložnosti prihodkov. S tehnološkega vidika bo nadgradnja na 5G zahtevala velike spremembe v celotnem omrežju, ne zgolj na radijskem delu. Celotno omrežje se bo temeljito prenovilo, da bo na poslovno učinkovit način odgovorilo na zahteve po višjih pasovnih širinah, velikemu porastu različnih priključenih naprav, zahtevnejši in raznoliki signalizaciji, večji zanesljivosti ter manjšim zakasnitvam. Predvsem pa, da bo omogočilo nove poslovne modele in storitve, kjer so bo virtualizirano omrežje lahko uporabljalo za različne industrije in aplikacije ter omogočilo razvoj rešitev, ki bodo lahko naslovile različne potrebe uporabnikov. Omrežje 5G bo omogočalo gradnjo virtualnih omrežnih poti in rezin omrežij (Network Slices), ki jih lahko pojmujemo kot omrežja na zahtevo z zagotovljeno kakovostjo storitev, in še več, omogočeno bo ponujanje omrežja kot storitev (NaaS, Network as a Service).

Kot pri vsaki novi generaciji omrežij bo za celovito prenovo omrežja potrebna vizija celovite arhitekture, obenem pa tudi kar nekaj evolucijskih korakov. Namen članka je opisati nekaj konkretnih korakov, s katerimi lahko operaterji začnejo uresničevati vizijo 5G.

II. KAJ JE 5G?

Če je bil odgovor na to vprašanje za prejšnje generacije omrežij bolj enostaven, pa je na vprašanje kaj je 5G težje odgovoriti, predvsem zaradi marketinga proizvajalcev ter zelo široko zastavljenih tehničnih in poslovnih pričakovanj povezanih s 5G. Veliko je različnih interpretacij: od tega, da gre zgolj za novo radijsko tehnologijo do mnenja, da gre za celovito prenovo omrežij od konca do konca, vključujoč razlago, da gre za osrednji koncept pri zagotavljanju storitev interneta stvari za različne industrije in tudi, da je 5G osnova in ključni element za digitalno transformacijo tako operaterjev in ponudnikov storitev kot tudi industrijskih sektorjev. Dejstvo je, da potekajo standardizacijske aktivnosti 5G v organizacijah kot so ETSI, 3GPP, IEEE, ONF in ITU, pri čemer moramo poudariti, da 5G še ni standardiziran niti kot termin in znotraj ITU se 5G standardizacija odvija v okviru programa "International Mobile Telecommunications-2020 (IMT-2020) and beyond".

Zato je pomembno, da si operaterji najprej odgovorijo, kaj za njih predstavlja 5G v smislu poslovne in tehnične strategije in to umestijo v širšo poslovno strategijo. Za namen tega članka bomo 5G razumeli celovito v poslovnem, storitvenem in tehničnem smislu.

V tehničnem smislu 5G vključuje vse vrste dostopa s poudarkom na novi generaciji radijskega dostopa, transportno in jedrno omrežje ter sisteme za upravljanje. V smislu storitev zagotavlja 5G izboljšanje govornih, video in podatkovnih storitev, poleg tega pa omogoča tudi platformo za poslovni najem virtualiziranih omrežnih resursov in zagotavljanje odprtih vmesnikov razvijalcem aplikacij in ponudnikom vsebin. Zato je v okviru strategije 5G ključna gradnja poslovnih ekosistemov in umestitev operaterjev v verigi dodane vrednosti pri zagotavljanju celovitih rešitev za različne industrije. Ponudniki omrežij se vse bolj približujejo ponudnikom raznorodnih tehnologij, med njimi tudi omrežnih tehnologij. To je velik preskok v dojemanju njihove vloge. Ponudniki storitev pa dodajajo v svoj nabor storitev digitalne storitve in vsebine.

Vseeno lahko ugotovimo, da je v okviru procesa standardizacije prišlo do konsenza industrije, da je 5G celovita vizija omrežja za:

– izboljšanje mobilne širokopasovnosti,

– masovno komuniciranje naprav (Massive Machine Type Communications),
– visoko-zanesljive komunikacije z majhnimi zakasnitvami,
– virtualizirano omrežje kot platforma za razvoj novih poslovnih modelov.

Izjemno pomembno pri vsem tem je dejstvo, da že v same izhodiščne načrtovalske paradigme 5G vgrajuje principe, ki podpirajo in omogočajo uresničevati zgoraj omenjeno vizijo.

III. POSLOVNI TRENDI IN IZZIVI

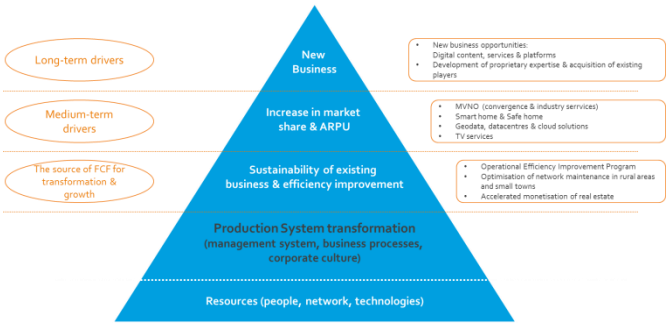
Glede na to, da je strategijo uvajanja 5G potrebno umestiti v širšo poslovno strategijo operaterjev, na kratko poglejmo ključne poslovne izzive v telekomunikacijski industriji.

Prihodki operaterjev od storitev trojčka in četverčka, mobilnih podatkovnih paketov in drugih storitev, ki so jih uvajali v zadnjih letih stagnirajo, tržne bitke za deleže znižujejo cene, zahteve uporabnikov po večjih hitrostih in večjem prenosu podatkov zahtevajo stalne visoke investicije v omrežje. Kot odgovor na te izzive lahko ključne strateške usmeritve operaterjev strnemo v štiri točke:

– Povečanje operativne učinkovitosti in zadovoljstva uporabnikov.
– Cenovno učinkovito investiranje v nadgradnjo zmogljivosti infrastrukture.
– Kratkoročno in srednjeročno povečanje prihodkov na osnovi video storitev, oblačnih storitev in povezovanja stvari.
– Celovita digitalna transformacija, ki vsebuje:
  – spremembo kulture za povečanje organizacijske agilnosti,
  – personalizirano in digitalizirano interakcijo s kupci,
  – uvajanje novih storitev in poslovnih modelov za digitalizacijo družbe in različnih industrij za nove prihodke.

Primer moderne vizije telekomunikacijskega operaterja je Rostelekom [1]. Njej povzetek je prikazan na sliki 1. Ključni kratkoročni poudarek je na transformaciji sistemov in procesov za zmanjšanje operativnih stroškov delovanja (OPEX). To v praksi pomeni konsolidacijo jedrnih omrežnih elementov v regionalne podatkovne centre in postopni prehod na arhitekturo enotnega operaterskega oblaka za vse funkcije delovanja. Pri tem je cilj optimizacija upravljanja omrežja (predvsem za manjše lokacije) z večjo avtomatizacijo in centralizacijo. S tem želijo sprostiti denarni tok za vlaganja v razvoj novih pametnih in konvergenčnih storitev, kjer si srednjeročno obetajo rast prihodkov. Tu je poudarek na oblačnih storitvah, združevanju fiksnih, mobilnih in IT storitvah, geolokacijskih storitvah in na pametnemu in varnemu domu. Že danes pa skupaj s partnerji sodelujejo na ključnih projektih modernizacije državne IKT infrastrukture, kot je na primer vsedržavno uvajanje enotnega sistema in številke 112.

Dolgoročno želijo naslavljati nove poslovne priložnosti z digitalnimi vsebinami, storitvami in platformami. Razvijali bodo lastne kompetence in ekspertna znanja, ki jih bodo dopolnjevali z nakupi ključnih igralcev, s katerimi bodo uspešno postali ponudnik digitalnih storitev in vsebin ter ponudnik naprednih tehnologij.

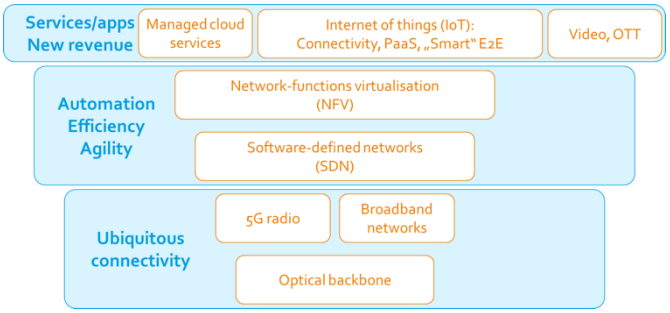


Slika 1: Vizija Rostelekom 2020

IV. REŠITVE DANES IN PREDLAGANI KORAKI

Danes aktualne tehnologije in storitve, ki podpirajo zgoraj naštete poslovne strategije in tudi prehod v 5G, lahko strnemo v:

– Centraliziran ali porazdeljen operaterski (telco) oblak na osnovi tehnologij NFV in SDN, ki se standardizirajo znotraj ETSI NFV in ONF ter so na voljo v odprtokodnih skupnostih, kot odgovor za povečanje operativne učinkovitosti in agilnosti, ki omogoča konsolidacije omrežnih in IT infrastruktur za pospešeno uvajanje novih storitev.
– Širokopasovna dostopovna omrežja naslednje generacije (NGA – Next Generation Access) z uvajanjem optičnega omrežja čim bližje končnim uporabnikom (Fiber to the x – FTTx, pri čemer je x tudi brezžična bazna postaja 4G/5G) ali do samega uporabnika (FTTH).
– Zagotavljanje in upravljane oblačne infrastrukture in IKT storitve za podjetja, video vsebin ter v partnerstvih z različnimi industrijami vseh digitalnih storitev, tudi na osnovi interneta stvari.



Slika 2: Ključne tehnologije in storitve kot odgovor na izzive operaterjev.

Čeprav standardizacija 5G ni zaključena in je predvsem na radijskem delu še veliko odprtih vprašanj, pa v telekomunikacijski industriji obstaja večinski konsenz:

– da bo arhitektura omrežja 5G temeljila na tehnologijah NFV/SDN,
– da je osnovni standard, ki pokriva multimedijske komunikacije v realnem času tudi v omrežju 5G IP Multimedia System (IMS), ki se v okviru ETSI 3GPP med drugim nadgrajuje za podporo kritičnim komunikacijam,
– da bo jedrno podatkovno omrežje 5G temeljilo na arhitekturi EPC, ki jo znana že iz LTE in se prav tako nadgrajuje v okviru standardov 3GPP v Next Generation Core (NG Core),

– da bo za realizacijo zahtevanih omrežnih karakteristik potrebna distribuirana procesna moč, ki se standardizira v okviru pobude ETSI MEC (Multi-access Edge Computing, predhodnik je označeval Mobile Edge Computing),
– da bo večina novih storitev znotraj 5G temeljila na konceptu interneta stvari (Internet of Things – IoT).

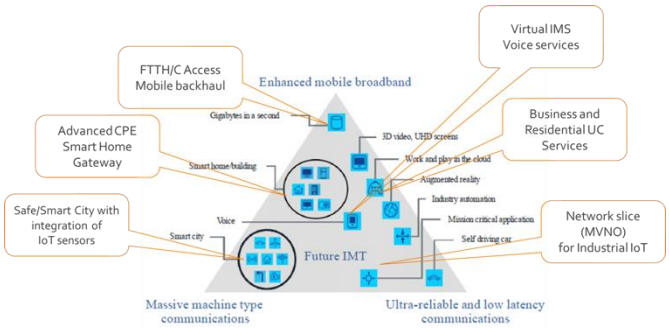
Zaradi tega operaterji lahko nadgrajujejo svoja omrežja in storitve z rešitvami, ki so pripravljena na 5G. Operaterji se sicer nahajajo v različnih poslovnih in tehnoloških okoliščinah, vendar tipično obstajajo poslovno upravičeni razlogi za enega ali več od naslednjih projektov:

– uvajanje konvergenčnega govornega omrežja na osnovi IMS, kar pomeni tudi popolno podporo omrežjem »All-IP« (VoLTE za 4G omrežje),
– konsolidacija in virtualizacija omrežnih elementov in selitev omrežnih funkcij na oblačno infrastrukturo in komercialne strežnike (COTS). V zgornjem primeru to pomeni virtualizirano IMS rešitev, vendar to lahko velja tudi za virtualizirani EPC oz. NG Core ter druge domene omrežja (C-RAN),
– konsolidacija IT infrastrukture v oblak in/ali poenotenje oblačne infrastrukture znotraj podatkovnih centrov,
– uvajanje avtomatiziranih in upravljanih poslovnih VPN storitev (s pomočjo SDN tehnologije).konsolidacija agregacijskega in zalednega (backhaul) omrežja na standardizirana Ethernet stikala, upravljana preko centraliziranega krmiljenja (SDN Controller).

In še bi lahko naštevali. Za vse zgoraj naštete izzive danes obstajajo rešitve, ki so prvi korak ali del v mozaiku do uresničitve vizije 5G.

V. REŠITVE IN IZKUŠNJE ISKRATEL

Tudi Iskratel je razvil in razvija svoje rešitve v skladu z vizijo 5G.



Slika 3: Iskratel rešitve v okviru vizije 5G.

Iskratelove rešitve za operaterje s poudarkom na storitvah IMS in aplikacijah so se preselile na operaterski oblak. Bistvene omrežne funkcije smo virtualizirali. Na osnovi odprtokodnih rešitev (OpenStack) smo produktivizirali in za operaterske zahteve prilagodili tudi lastno oblačno platformo (Cloud Services Platform).

Rešitev virtualni IMS (vIMS) je v svetovnem merilu ena od prvih omrežnih rešitev, ki se uvaja v novi arhitekturi NFV.

Tudi glede na potrebe naših kupcev je Iskratelova rešitev vIMS prva NFV rešitev, ki jo uvajamo na trg. Rešitev je zasnovana kot odgovor na zahteve kupcev in vsebuje:

– virtualizirane jedrne in robne IMS elemente (CSCF, TAS, HSS, EMS, DNS/ENUM, xGCF,…),
– IMS centralizirane storitve (M-AGCF, TGCF, VoWiFi, VoLTE,…),
– strojno platformo COTS (x86),
– produktiviziran oblak na osnovi Openstack (KVM Hypervisor) z dorazvitimi funkcijami za visoko razpoložljivost in georedundanco,
– podporo za NGN storitve in povezovanje z omrežji NGN in TDM,
– regulatorne funkcije (aktivno in pasivno legalno prestrezanje LI/SORM) s podporo hrambi velike količine podatkov,
– centralizirano upravljanje in avtomatizacijo upravljanja storitev na osnovi koncepta MANO (ETSI).

Operaterji si od rešitve vIMS obetajo velike prihranke s selitvijo omrežnih funkcij na oblačno infrastrukturo, predvsem zaradi zmanjšanja števila lokacij, kjer se je nahajala namenska strojna oprema (v primeru rešitve vIMS se zamenjujejo tako klicni strežniki kot telefonske centrale s klasično tehnologijo TDM) in zmanjšanja števila različne opreme, potrebne vzdrževanja, prilagodljive uporabe infrastrukture podatkovnih centrov za več omrežnih funkcij hkrati ter centraliziranega in avtomatiziranega upravljanja omrežne infrastrukture in storitev.

Pri tem gre za obsežne projekte, ki zahtevajo veliko sodelovanja ter uvajanja organizacijskih in tehnoloških sprememb pri operaterju. Zato je, poleg končnega cilja omrežne nadgradnje z arhitekturnimi in tehnoloških izboljšavami, ključnega pomena vnaprejšnje definiranje migracijskega scenarija, ki upošteva:

– obstoječe storitve pri operaterju in njihove želje po novih storitvah za obstoječe ali nove stranke,
– zagotavljanje medsebojne povezljivosti,
– zaledne sisteme BSS/OSS, povezane z omrežno infrastrukturo (aplikativni programski vmesniki) in
– zakonodajne in regulatorne okvire.

Tehnologija 5G sama po sebi ne bo prinesla poslovnih koristi, če ni ustrezno implementirana in pri tem ne upošteva poslovnih modelov. Na primer, če se izvede virtualizacija množice različnih sistemov brez ustrezne konsolidacije, bo tako rešitev morda še težje upravljati.

Kot naslednji korak pri uvajanju arhitekture NFV/SDN in tako imenovanega razslojevanja omrežja (network slicing) se pogosto pojavlja rešitev vEPC, ki jo Iskratel razvija v sodelovanju s partnerji in kot del celovitega paketa za MVNO operaterje [4].

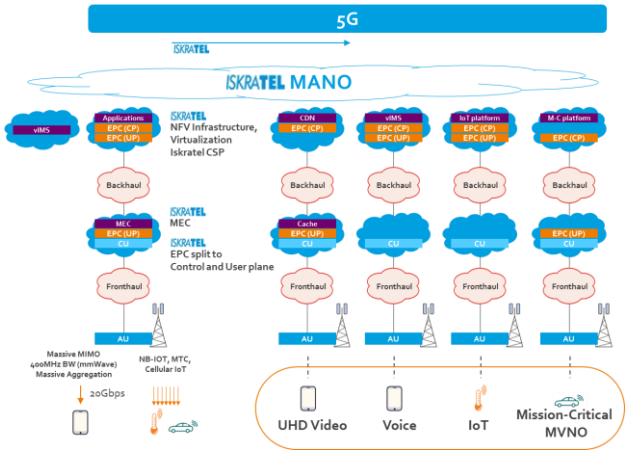
Razslojevanje omrežja je ena od ključnih lastnosti arhitekture 5G, ki bo omogočila več logičnih omrežij na istem fizičnem omrežju. To bo omogočilo nastanek različnih operaterjev MVNO, ki bodo lahko osredotočeni na specifične uporabnike s specifičnimi zahtevami po omrežnih storitvah in poslovnih modelih. Veliko teh bo vezanih na različne storitve IoT.

Operaterji so tako pred strateško dilemo, kako se umestiti znotraj poslovnega ekosistema IoT. Lahko so:

– ponudniki storitev povezovanja in ostalih tehnologij,
– ponudniki platforme IoT in omogočevalniki storitev,
– ponudniki celovitih rešitev od konca do konca z raznorodnim naborom storitev.

Operaterji digitalnih storitev se pri ponujanju storitev za različne industrije tudi ustrezno umeščajo v verigi dodane vrednosti, lahko tudi na različna mesta v tej verigi.

Glede na to, da Iskratelova strategija, poleg rešitev za operaterje, daje poseben poudarek razvoju celovitih infokomunikacijskih rešitev za digitalizacijo energetike, inteligentnega transporta in javne varnosti, je Iskratel lahko dober partner operaterjem pri uvajanju storitev za digitalizacijo industrij in javnega sektorja na osnovi trenda IoT.



Slika 4: Razslojevanje omrežja 5G za različne storitve in scenarije MVNO.

VI. KAKO NAPREJ?

Rešitve, ki temeljijo na konceptih NFV/SDN (vIMS, vEPC), konvergenčne komunikacijske aplikacije, rešitve za optična dostopovna omrežja in specialne rešitve za različne industrijske vertikale, so temelj, s katerimi Iskratel s svojimi partnerji že danes gradi vizijo omrežij 5G. Korake uresničevanja vizije sproti preverja pri svojih kupcih in jih skupaj z njimi dopolnjuje.

Zato bo ključno torišče dogajanja v naslednjih letih povezano s hitrostjo uvajanja 5G. Pri tem bodo ključni migracijski scenariji in sožitje obstoječega (ne nujno starega) z povsem novim. Le tisti dobavitelji opreme in rešitev, ki bodo znali operaterjem in ponudnikom storitev ter vertikalnim sektorjem ponuditi varen prehod in odgovoriti na bistvena vprašanja o ekonomičnosti, koristih in poslovnih modelih, bodo verjetni zmagovalci.

Skrbno spremljamo tudi ukrepe za hitrejše uvajanje 5G v evropskem in svetovnem prostoru. Strategija Komisije za enotni digitalni trg, ki vključuje tudi Akcijski načrt za 5G v Evropi (COM(2016)588) [5], poudarja pomen uvedbe zelo visoko zmogljivih omrežij 5G v vsaki državi, saj so ključna za evropsko konkurenčnost na globalnem trgu. Utemeljeno menimo, da so predlagani ukrepi pomembna spodbuda za uresničitev vizije 5G.

LITERATURA

[1] http://www.rostelecom.ru/en/ir/results_and_presentations/strategy/
[2] Kosei Takiishi, Gartner: Emerging Technology Analysis: 5G, November 2016
[3] Gyanee Dewnarain, Gartner: Hype Cycle for the Telecommunications Industry, Julij 2016
[4] Damjan Slapar, Gašper Jezeršek, Ana Robnik, From Broadband to 5G, Zbornik referatov 33. delavnice o telekomunikacijah VITEL 2017
[5] Comission, European. (14. 9 2016). COM(2016) 588 final: 5G for Europe: An Action Plan {SWD(2016) 306 final}. Brussels

Janez Öri je direktor marketinga in vodja strateškega odbora v Iskratelu. Pred tem je bil odgovoren za produktno strategijo in upravljanje portfelja izdelkov. Diplomiral je s področja telekomunikacij/elektrotehnike na Fakulteti za elektrotehniko Univerze v Ljubljani leta 1997. Od leta 2003 je bil vodja ekipe Iskratelovih tehničnih rešitev in razvoja posla za širokopasovni dostop in IP omrežje.

Ana Robnik je svetovalka za telekomunikacije, koordinira delo v standardizacijskih organizacijah in vodi raziskovalno skupino podjetja Iskratel. Svojo poklicno pot je po univerzitetnem študiju uporabne matematike na Fakulteti za matematiko, fiziko in mehaniko Univerze v Ljubljani in opravljenem magisteriju iz računalništva na Fakulteti za računalništvo Univerze v Ljubljani nadaljevala v razvojno raziskovalni enoti Iskra Kibernetika in kasneje v IT-oddelku Iskratela. Nato se je vključila v razvoj telekomunikacijskih produktov SI2000 in SI3000 ter do leta 2009 vodila sektor za upravljanje in nadzor omrežnih elementov.

Simon Čimžar je arhitekt celovitih rešitev in kompleksnih IP omrežij/rešitev v podjetju Iskratel. Pred tem je bil odgovoren za produktno vertikalo fiksnega dostopa in rešitvami povezanimi s širokopasovnim dostopom. Diplomiral je s področja telekomunikacij/elektrotehnike na Fakulteti za elektrotehniko Univerze v Ljubljani.

Optoelektronske tehnologije v 5G (FiWiN5G)

Boštjan Batagelj, Tomi Mlinar, Mehmet Alp Ilgaz, Laboratorij za sevanje in optiko, Katedra za informacijsko komunikacijske tehnologije, Fakulteta za elektrotehniko Univerze v Ljubljani

Povzetek — Ta članek opisuje projekt FiWiN5G (angl. Fiber-Wireless Integrated Networks for 5th Generation delivery). Glavna tematika projekta FiWiN5G je premik nosilne frekvence na višje frekvenčno območje in povečanje pasovne širine optično podprtih brezžičnih omrežij z uporabo optoelektronskih tehnologij. Predlagani pristop omogoča rešitve, ki so zlasti primerne za visoko zmogljive radijske sisteme, zasnovane v frekvenčnih pasovih milimetrskih valov, kjer je fazni šum eden glavnih omejujočih dejavnikov. Poleg stroškovne učinkovitosti lahko tovrstne rešitve zmanjšajo velikost in kompleksnost baznih postaj, katerih število se bo v 5. generaciji mobilnih omrežij povečalo zaradi zmanjšanja velikosti celice.

Ključne besede — brezžična omrežja, celična arhitektura, milimetrski valovi, prenos radijskih signalov po optičnem vlaknu, zlivanje radijskih in optičnih tehnologij

Abstract — This article explains »Fiber-Wireless Integrated Networks for 5th Generation delivery« (FiWiN5G) project. The main theme of FiWiN5G is the expansion, in terms of both carrier frequency and bandwidth, of optically supported wireless networks by using opto-electronic technologies. The proposed approach can provide solutions that are especially suitable for high-capacity radio system based on millimeter-wave frequency bands, where the phase noise is one of the main limiting parameters. Besides the cost efficiency, these solutions can decrease the size and complexity of base-stations, the number of which will increase in 5th generation cellular networks due to a reduction in the cell size.

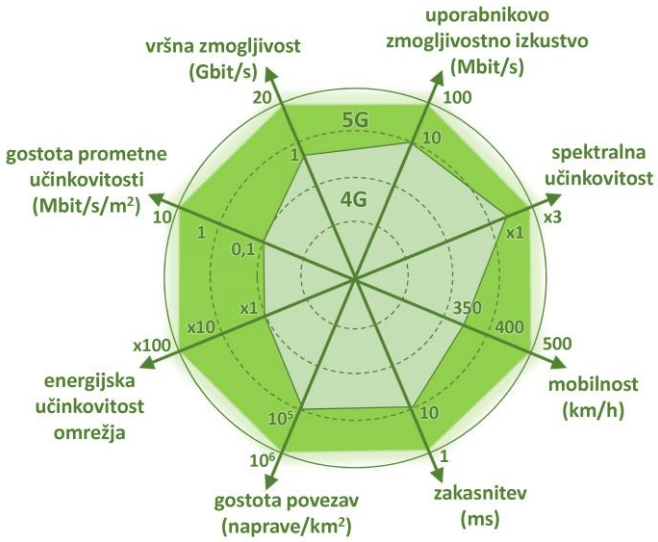
Keywords — wireless networks, cellular architecture, millimeter-wave, radio-over-fibre, convergence of radio and optical technologies

I. UVOD

Sektor za radiokomunikacije pri mednarodni zvezi za telekomunikacije (angl. Radiocommunication Sector of International Telecommunication Union – ITU-R) je septembra leta 2015 izdal svojo vizijo z zahtevami v mednarodnih mobilnih telekomunikacijah (angl. International Mobile Telecommunications – IMT) do in preko leta 2020. [1] Vizija je poznana pod oznako IMT-2020, kar se največkrat razume kot naslednja (peta) generacija (5G) mobilnih omrežij. Definiranih je bilo osem zahtev za mobilna omrežja 5G, katere prikazuje Slika 1. Seveda vse te zahteve narekujejo nove smernice v mobilnih omrežjih, kjer izstopajo okrepljena mobilna širokopasovnost, množična komunikacija med napravami in zanesljivost prenosa informacij z nizko zakasnitvijo.

Vse zahteve so naravna evolucija premikanja obstoječih tehnoloških meja, ki pa v tehnološkem pomenu ne zaslužijo poimenovanja nova generacija, saj se ohranjajo enake tehnološke rešitve, kot jih poznamo že v četrti generaciji (4G) mobilnih omrežij. Poleg tega se zahteve v nekaterih primerih med seboj tudi izključujejo, ker trenutne tehnološke rešitve niso zadovoljive za vse navedene zahteve. Pri vsem tem pa se je potrebno zavedati, da zahteve za mobilna omrežja 5G, določene s strani ITU-R, ne predvidevajo povečanja nosilne frekvence v področje milimetrskih valov (angl. millimetre wave – mmW), kjer je na razpolago več pasovne širine.

Namen tega prispevka je prikazati potencial v tehnologiji optoelektronike, ki z rešitvami na osnovi zlivanja optične in radijske tehnologije doprinese tehnološki preskok, ki bi si nedvomno zaslužil poimenovanje – nova generacija. Prispevek se predvsem posveča ciljem evropskega projekta FiWiN5G (angl. Fiber-Wireless Integrated Networks for 5th Generation delivery), ki razvija naslednje generacije konvergenčnega omrežja, zasnovanega na sodelovanju brezžičnih in optičnih tehnologij. [2] Glavna tehnološka cilja projekta FiWiN5G sta premik nosilne frekvence na višje frekvenčno področje in povečanje pasovne širine brezžičnih omrežij, ki so podprte z optično tehnologijo, tako v prenosu kot v napravah.



Slika 1: Zahteve prihajajočega mobilnega omrežja 5G v primerjavi s trenutnim omrežjem 4G

II. KONVERGENCA RADIJA IN OPTIKE

Optične komunikacijske zveze so takoj po odkritju steklenega optičnega vlaka začele zamenjevati električne žične zveze in radijske usmerjene zveze. Razlog za hitro uveljavite tiči v precej boljših lastnostih zveze preko optičnega vlakna v primerjavi z električnimi vrvicami in radijskimi zvezami v smislu parametrov, ki opisujejo kakovost telekomunikacijske zveze. [3] Prvi zelo pomemben parameter, ki igra vlogo predvsem pri izvedbi zvez na dolge razdalje, je doseg zveze, kjer prevladuje stekleno optično vlakno s časovno konstantnim slabljenjem 0,2 decibelov na

kilometer (dB/km) pri valovni dolžini 1550 nm. Drugi parameter za ovrednotenje telekomunikacijske zveze je njena zmogljivost, ki se podaja v količini prenesene informacije v časovni enoti in se pri današnjih številskih zvezah podaja v količini bitov prenesenih v časovni enoti (bit/s). Visoka zmogljivost optične zveze je posledica praktično skorajda neomejene pasovne širine optičnega vlakna, čeprav se po nekaterih predvidevanjih v medkontinentalnih zvezah počasi le približujemo tako imenovanemu »optičnemu zidu«. [4] Ta bojazen je zaenkrat več kot odveč v dostopovnih omrežjih in v optičnih zvezah, ki skrbijo za promet med centralo in baznimi postajami, čeprav se bodo potrebe po zmogljivostih zvez v tem segmentu enormno povečale.

Predpostavimo, da bo bodoči sistem 5G uporabil frekvenčno pasovno širino 200 MHz in 16×16 MIMO antenski sistem ter bo prostorsko pokrivanje ene bazne postaje razdeljeno v tri sektorje. Če se bo na zvezi med centralno enoto in bazno postajo uporabljal ustaljen radijski vmesnik (angl. Common Public Radio Interface – CPRI) z zmogljivostjo 1,2288 Gbit/s [5], ki za frekvenčno pasovno širino 20 MHz uporabljajo vzorčevalno frekvenco 30,72 MHz iz nizkošumnega oscilatorja, bo zahtevana zmogljivost na en sektor

$$1{,}2288\ Gbit/s \cdot 10 \cdot 16 = 196{,}608\ Gbit/s \qquad (1)$$

Zahtevana zmogljivost na celotno bazno postajo s tremi sektorji pa

$$196{,}608\ Gbit/s \cdot 3 = 589{,}824\ Gbit/s \qquad (2)$$

To pomeni, da bo na optični zvezi za prenos skupnega prometa 590 Gbit/s, ki uporablja modulacijo DP-QAM s spektralno učinkovitostjo 2,7 bit/s/Hz [6], potrebno zagotoviti 218 GHz optičnega spektra, kar nikakor ni zanemarljivo malo in kliče po uporabi tehnologije zgoščenega valovno-dolžinskega razvrščanja (angl. Dense Wavelength Division Multiplexing – DWDM) do vsake bazne postaje.

Zagato z visoko potrebo po pasovni širini je mogoče rešiti z zlivanjem radijskih in optičnih omrežij na fizičnem nivoju, ki vodi v povsem novo tehnološko področje, imenovano mikrovalovna fotonika [7], [8]. Ena od tehnoloških rešitev mikrovalovne fotonike je uporaba tehnologije, ki omogoča prenos analognih radijskih signalov po optičnem vlaknu (angl. Radio-over Fibre – RoF). [9] Osnovna ideja tehnologije RoF je v tem, da se za prenos signalov radijskih frekvenc (RF) uporabljajo optična vlakna in s tem izkorišča nizko slabljenje in veliko pasovno širino optičnega vlakna [10].

V primerjavi s sedanjimi tehnikami digitalnega prenosa med centralo in bazno postajo je analogni prenos RoF mnogo bolj učinkovit, saj ne zahteva dodatne nepotrebne režije (vzorčenja), kar pomeni, da nismo deležni zmanjšanja pasovne širine in povečanja zakasnitev. Za prej naveden primer sistema 5G, ki uporablja frekvenčno pasovno širino 200 MHz in antenski sistem 16x16 MIMO, se potrebna pasovna širina na sektor poveča zgolj na

$$200\ MHz \cdot 16 = 3{,}2\ GHz \qquad (3)$$

in ob upoštevanju treh sektorjev na

$$3{,}2\ GHz \cdot 3 = 9{,}6\ GHz \qquad (4)$$

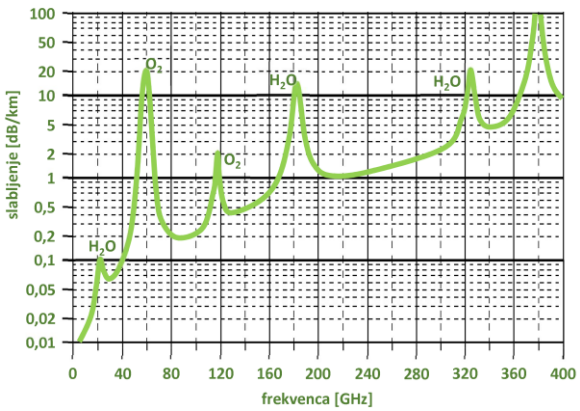
kar je za več kot dvajsetkrat nižja potreba po optični pasovni širini v primerjavi z uporabo ustaljenega CPRI. [11]

Ker ima stekleno optično vlakno veliko pasovno širino, z lahkoto omogoča prenos analognih radijskih signalov različnih frekvenc – tudi v mikrovalovnem in milimetrskem področju. Poznanih je več načinov za prenos radiofrekvenčnih signalov s tehnologijo RoF [12]. Najpreprostejši način za optičen prenos radijskega signala uporablja direktno modulacijo jakosti svetlobe laserske diode z radiofrekvenčnim signalom in direktno detekcijo na fotodiodi za sprejem oziroma demodulacijo radiofrekvenčnega signala.

Za prenos radijskih signalov višjih frekvenc, kot so npr. signali milimetrskih valov, pa direktna modulacija toka zaradi omejene pasovne širine polprevodniških laserjev ni mogoča. Na višjih frekvencah se zato intenzitetno modulacijo izvede z zunanjim modulatorjem. Kot zunanji modulator svetlobne jakosti se lahko uporabi elektroabsorbcijski modulator ali Mach-Zehnderjev modulator [13]. Po izvedeni intenzitetni modulaciji z radiofrekvenčnim signalom se svetlobni signal prenese po optičnem vlaknu. Na drugem koncu optičnega vlakna se dogaja optoelektronska pretvorba, pri čemer fotodioda sprejme optični signal in z metodo direktne detekcije izloči uporabni radiofrekvenčni signal iz optičnega signala.

III. PODROČJE MILIMETRSKIH VALOV

V splošnem je slabljenje signala na kilometer pri radijskih zvezah v področju milimetrskih valov precej večje kot pri optičnih vlakenskih zvezah. Slabljenje, ki ga povzroča absorpcija v ozračju, se generalno še povečuje s povečevanjem uporabljene nosilne frekvence [14], [15], [16], [17], [18], kot prikazuje Slika 2. Fizikalna slika razširjanja skozi ozračje razkriva nekaj področij, kjer je slabljenje radijskega valovanja zmanjšano, kar omogoča boljši brezžični prenos. Atmosferska okna se naravno pojavljajo pri frekvencah 35, 90, 140 in 220 GHz ter celo pri višjih frekvencah. Frekvence v področju 35 GHz se že pogosto uporabljajo za komercialne satelitske komunikacije in nekatere prizemne komunikacije. Milimetrski valovi v območju frekvenc 90 GHz pa se prav tako že dolgo izkoriščajo za vojaške komunikacije. V splošnem velja, da se je smiselno izogibati vodnim in kisikovim absorpcijskim vrhovom na 60, 119, 183 in 325 GHz, saj zelo omejujejo prenosne razdalje. Vendar pa okna med absorpcijskimi vrhovi pri približno 80, 140, in 220 GHz kažejo velik potencial za visoko zmogljive komunikacijske zveze, zaradi potencialno zelo velike pasovne širine, ki je na voljo med njimi.



Slika 2: Slabljenje ozračja na morski gladini v različnih frekvenčnih področjih milimetrskih valov

Visoko slabljenje v področju milimetrskih valov je problematično pri zvezah na dolge razdalje, ker je tam visoka absorpcija in sipanje signala zaradi vremenskih pojavov (dež, sneg, megla). Ker pa se v naslednjih generacijah mobilnih omrežij povečuje gostota prometne učinkovitosti, bo prišlo tudi do povečanja gostote baznih postaj, kar pomeni, da bo ena bazna postaja pokrivala manjše geografsko območje. Razširjanje radijskega signala bo s tem omejeno na relativno kratke razdalje – nekaj 100 metrov (piko celice) ali celo nekaj 10 metrov (femto celice). Krajše razdalje med bazno postajo in uporabnikom dovoljujejo uporabo nosilnih frekvenc v milimetrskem področju.

Poskusi uporabe milimetrskih valov za sodobna mobilna omrežja so že poznani [19] in avtorji največkrat navajajo osupljiva povečanja v zmogljivosti, kot je prikazano na Sliki 3 za deset uporabnikov na celico. Čeprav njihovi avtorji navajajo 25× povečanje zmogljivosti na celico in 10× povečanje zmogljivosti na uporabnika, se je potrebno zavedati, da je bilo za potrebo teh rezultatov zagotoviti 25× več frekvenčnega spektra, kot pri izvedbi zvez v mikrovalovnem področju, vse to zaradi dejstva, ker je spektralna učinkovitost v področju milimetrskih valov mnogo slabša kot v področju mikrovalov.

sistem	pasovna širina [MHz]	centralna frekvenca [GHz]	antena MIMO	celična zmogljivost [Mbit/s/celico]		uporabnikova zmogljivost [Mbit/s/uporabnika]	
				promet navzdol	promet navzgor	promet navzdol	promet navzgor
4G	20+20 FDD	2,5	2x2	53,8	47,2	1,80	1,94
5G	1000	28	4x4	1514	1468	28,5	19,9
		73	8x8	1435	1465	24,8	19,8

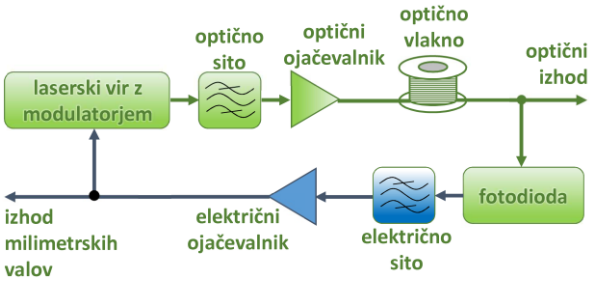
Slika 3: Primerjava zmogljivosti celic v sistemih 4G in 5G

Zato se za učinkovito rabo frekvenčnega spektra in povečanje zmogljivosti brezžičnega omrežja vpeljujejo nove modulacijske in združevalne tehnike [20], [21], [22]. V vseh naštetih primerih je jasno, da igra pomembno vlogo pri prenosu signala fazni šum [23]. Danes uporabljeni oddajniki in sprejemniki mobilnih sistemov imajo vgrajene nizkošumne oscilatorje za generiranje radijskih signalov, ki so potrebni za frekvenčno pretvorbo v sprejemno-oddajnih vezjih in za njihovo časovno sinhronizacijo.

Ko želimo uporabljati radijske vmesnike v območjih višjih frekvenc [24], je vzdrževanje nizkega faznega šuma veliko težje, kot je to pri nižjih frekvencah [25], ker je v fizikalni naravi danes dostopnih oscilatorjev, da se fazni šum poveča, če deluje oscilator na višjih frekvencah.

Po mnenju mnogih načrtovalcev sodobnih radijskih sistemov je nizkošumni frekvenčni oscilator kritičen element za razvoj mobilnih omrežij 5G na frekvencah milimetrskih valov, saj bo le tako mogoče ohraniti spektralno učinkovitost, ki jo poznamo na nižjih frekvencah.

Naprava, ki ni podrejena zgoraj opisanemu zakonu fizike, je optoelektronski oscilator (OEO) [26], katerega zgradba je prikazana na Sliki 4. Najpomembnejša komponenta OEO je maloizgubno optično vlakno, ki deluje kot zelo dolga zakasnilna linija. Največja prednost OEO je kakovost resonatorja Q, ki je sorazmerna produktu časovne zakasnitve optičnega vlakna in frekvence oscilatorja. Ker določa izgube optičnega vlakna valovna dolžina uporabljenega laserja, so te teoretično enake pri signalu katere koli mikrovalovne frekvence. To posledično pomeni, da se kakovost resonatorja (Q) poveča, če se poveča frekvenca oscilatorja. Ali z drugimi besedami, če se poveča dolžina optične zveze, se bo zmanjšal fazni šum OEO. To pojasni, zakaj se z večanjem frekvence signala optoelektronskemu oscilatorju ne veča fazni šum.



Slika 4: Enozančni optoelektronski oscilator (OEO) z izhodom za optični signal in radijski signal na območju milimetrskih valov

Na žalost je optoelektronski oscilator zaenkrat vsaj 100× dražji od običajnih kristalnih oscilatorjev, zato si ga nikakor ne moremo privoščiti v vsaki bazni postaji. Za znižanje stroškov in istočasno povečanje učinkovitosti mobilnega omrežja predlagamo, da si več baznih postaj deli en optoelektronski oscilator [27]. Vpeljava distribuiranega optelektronskega oscilatorja za milimetrske valove je možna preko topologije dobro poznanega pasivnega optičnega omrežja (angl. passive optical network – PON) [28].

Z integracijo OEO v sistem RoF močno poenostavimo in pocenimo izvedbo bazne postaje. Nizkošumni signal iz optičnega izhoda OEO se prenaša iz centralne enote do bazne postaje po enorodovnem optičnem vlaknu. Na oddaljeni bazni postaji fotodioda detektira optični signal in generira radiofrekvenčni signal, primeren za frekvenčno pretvorbo podatkovnega signala v mešalniku. Prepričani smo, da bi v omrežju z veliko baznimi postajami in eno centralno enoto, opisan način prenosa RoF pomenil velik finančni prihranek.

IV. SKLEP

Prispevek kritično ovrednoti tehnološki doprinos k mobilnemu delu 5G in predlaga optoelektorske rešitve, ki bi z lahkoto zadovoljile zahteve prihajajočega omrežja 5G. Čeprav lahko že z danes znanimi tehnologijami naredimo fizično manjše bazne postaje, ki bi s pokrivanjem manjših celic zadovoljile skorajda vse zahteve 5G, je težko zadostiti nekaterim kriterijem, ki se zahtevajo od prihodnje generacije baznih postaj, tj. znižanje energetske porabe, manjša kompleksnost in nižja cena. V projektu FiWiN5G predlagana rešitev zlivanja optične in radijske tehnologije in s tem prenos radiofrekvenčnega signala med centralno in bazno postajo za mnogokratnik zmanjša zahteve po optični pasovni širini v primerjavi z uporabo ustaljenega načina prenosa iz 4G.

Ker so nižji frekvenčni pasovi prekomerno zasedeni z obstoječimi tehnologijami, je v prihajajočih novih generacijah mobilnih omrežij smiselno razmišljati o uporabi prostih pasov v področju milimetrskih valov. V milimetrskem področju je na razpolago veliko pasovne širine, vendar trenutno za to področje še ne obstajajo oscilatorji z nizkim faznim šumom, ki bi omogočali spektralne učinkovitosti kot jih poznamo v 4G. V prispevku je predstavljana optoelektronska rešitev za izvedbo oscilatorja z izjemnimi lastnostmi v področju milimetrskih valov. Kot predlaga projekt FiWiN5G, bo vpeljava distribuiranega optoelektronskega oscilatorja z nizkim faznim šumom na področju milimetrskih valov omogočila spektralne učinkovitosti, ki jih poznamo v mobilnih omrežjih 4G.

ZAHVALA

Avtorji prispevka se zahvaljujejo podjetju InLambda BDT, optoelektronske rešitve d. o. o., za izposojo raziskovalno-razvojne opreme. Raziskovalno delo, opisano v tem prispevku, je nastalo v sodelovanju z ARRS raziskovalnim programom – Algoritmi in optimizacijski postopki v telekomunikacijskih in FiWIN5G – Innovative Training Network, ki je bilo sofinancirano iz sklada Marie Sklodowska-Curie (št. pogodbe 642355) v okviru EU Horizon 2020 – Research and Innovation Programme 2014–2018.

LITERATURA

[1] IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond. Recommendation ITU-R M.2083-0; 2015
[2] www.fiwin5g.eu
[3] M. Vidmar: Optical-fiber communications: Components and Systems, Inform. MIDEM, vol. 31, no. 4, pp. 246-251, 2001
[4] B. Batagelj, V. Janyani, S. Tomažič: Research challenges in optical communications towards 2020 and beyond, Inform. MIDEM, vol. 44, no. 3, pp. 177-184, 2014
[5] www.cpri.info
[6] B. Batagelj. Trendi v optičnih komunikacijah. Zbornik seminarja optičnih komunikacij (SOK 2017), Ljubljana: Založba FE, 2017, str. 11-19
[7] R. Waterhouse and D. Novack, "Realizing 5G: Microwave Photonics for 5G Mobile Wireless Systems," in IEEE Microwave Magazine, vol. 16, no. 8, pp. 84-92, Sept. 2015
[8] S. Iezekiel, M. Burla, J. Klamkin, D. Marpaung and J. Capmany, "RF Engineering Meets Optoelectronics: Progress in Integrated Microwave Photonics," in IEEE Microwave Magazine, vol. 16, no. 8, pp. 28-45, Sept. 2015
[9] T. R. Clark and R. Waterhouse, "Photonics for RF Front Ends," in IEEE Microwave Magazine, vol. 12, no. 3, pp. 87-95, May 2011.
[10] B. Batagelj, et al.: Convergence of fixed and mobile networks by radio over fibre technology, Inform. MIDEM, vol. 41, no. 2, pp. 144-149, June 2011
[11] Byung Gon Kim, S. H. Bae, H. Kim and Y. C. Chung, "Optical fronthaul technologies for next-generation mobile communications," 2016 18th International Conference on Transparent Optical Networks (ICTON), Trento, 2016, pp. 1-3
[12] John E. Mitchell: Radio-over-Fiber (RoF) Networks in Broadband Access Networks: Technologies and Deployments, Springer, 2009
[13] H. N. Parajuli and E. Udvary, "A Vestigial sideband modulation scheme in radio over fiber system using electro-optic modulators," 2016 18th International Conference on Transparent Optical Networks (ICTON), Trento, 2016, pp. 1-4
[14] Attenuation by Atmospheric Gases, ITU-R Standard P.676-6, 2005.
[15] The Use of the Radio Frequency Spectrum Above 30 GHz: A Consultative Document, Radiocommunications Div., U.K. Dept. Trade Industry, IBSN-1-870837-00-47, 1988
[16] J. Wells, "Faster than fiber: The future of multi-G/s wireless", IEEE Microw. Mag., vol. 10, no. 3, pp. 104-112, May 2009
[17] M. Marcus and B. Pattan, "Millimeter wave propagation; spectrum management implications," in IEEE Microwave Magazine, vol. 6, no. 2, pp. 54-62, June 2005
[18] G. R. MacCartney, Junhong Zhang, Shuai Nie and T. S. Rappaport, "Path loss models for 5G millimeter wave propagation channels in urban microcells," 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, 2013, pp. 3948-3953
[19] M. R. Akdeniz et al., "Millimeter Wave Channel Modeling and Cellular Capacity Evaluation," in IEEE Journal on Selected Areas in Communications, vol. 32, no. 6, pp. 1164-1179, June 2014
[20] J. Vihriala, N. Ermolova, E. Lahetkangas, O. Tirkkonen and K. Pajukoski: On the Waveforms for 5G Mobile Broadband Communications, 2015 IEEE 81st Vehicular Technology Conf., Glasgow, pp. 1-5, 2015
[21] R. G. Clegg, S. Isam, I. Kanaras and I. Darwazeh: A practical system for improved efficiency in frequency division multiplexed wireless networks, IET Commun., vol. 6, no. 4, pp. 449-457, March 6, 2012
[22] T. Xu and I. Darwazeh, "Spectrally efficient FDM: Spectrum saving technique for 5G?," 1st International Conference on 5G for Ubiquitous Connectivity, Akaslompolo, 2014, pp. 273-278
[23] P. Robertson and S. Kaiser: Analysis of the effects of phase-noise in orthogonal frequency division multiplex (OFDM) systems, IEEE Int. Conf. on Commun. ICC '95, Seattle, WA, pp. 1652-1657 vol. 3., 1995
[24] Z. Pi and F. Khan: An introduction to millimeter-wave mobile broadband systems: IEEE Commun. Mag., vol. 49, no. 6, pp. 101-107, June 2011
[25] Z. Pi, J. Choi and R. Heath: Millimeter-wave gigabit broadband evolution toward 5G: fixed access and backhaul, IEEE Commun. Mag., vol. 54, no. 4, pp. 138-144, April 2016
[26] B. Batagelj, L. Bogataj and M. Vidmar: Key properties and design issues for an opto-electronic oscillator, ICTON, pp. 1-4, Budapest, 2015
[27] T. Mlinar, B. Batagelj, M. A. Ilgaz. Prenos fazno stabilnega nizkošumnega oscilatorjevega signala v mobilnih omrežjih 5G s tehniko prenosa radijskih signalov po optičnem vlaknu. Zbornik petindvajsete mednarodne Elektrotehniške in računalniške konference ERK 2016, 19. - 21. september 2016, Portorož, Slovenija, zv. A, str. 65-68.
[28] B. Batagelj. Pasivno optično dostopovno omrežje s časovnim razvrščanjem. 1. izd. Ljubljana: Založba FE in FRI, 2011. 124 str.

Boštjan Batagelj je docent na Fakulteti za elektrotehniko Univerze v Ljubljani, kjer predava predmete satelitske komunikacije in navigacija, optične komunikacije in radijske komunikacije. Raziskovalno delo opravlja v Laboratoriju za sevanje in optiko, kjer se med drugim ukvarja s fizičnim nivojem prenosnih in dostopovnih telekomunikacijskih omrežjih zasnovanih na radijski in optični tehnologiji. Je avtor več kot 300 člankov, osmih patentnih prijav in sodeluje v domačih ter mednarodnih raziskovalnih projektih s področja optičnih in radijskih komunikacij.

Tomi Mlinar je doktoriral na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Redno je zaposlen na Inštitutu za EMS in dopolnilno na Fakulteti za elektrotehniko. Njegovo raziskovalno delo zajema vse vrste brezžičnih komunikacij. Dolga leta se je ukvarjal z elektromagnetnimi sevanji, v zadnjem času pa se posveča celostnim analizam telekomunikacijskih trgov, alternativnemu brezžičnemu dostopu in širokopasovnim komunikacijam. Je avtor ali soavtor številnih strokovnih in poljudnoznanstvenih prispevkov, urednik več zbornikov, urednik in soavtor knjige Elektromagnetna sevanja in dolgoletni organizator in programski vodja strokovnih seminarjev Radiokomunikacije.

Mehment Alp Ilgaz je podiplomski študent na Fakulteti za elektrotehniko Univerze v Ljubljani. Njegovo študijsko področje so sodobni radijski sistemi, mikrovalovna fotonika in opto-elektronski oscilatorji. Zaposlen je na projektu FiWiN5G, raziskovalno delo pa opravlja v Laboratoriju za sevanje in optiko.

Razvoj 5G

Matjaž Beričič, Patrik Ritoša, Pavel Kralj, Iztok Saje, Peter Zidar, Telekom Slovenije, Slovenija

Povzetek — Današnja mobilna omrežja četrte generacije (4G), ki že dosegajo zavidljive hitrosti prenosa podatkov, se bodo konec tega desetletja začela nadgrajevati v omrežja 5G. Nove tehnologije bodo prinesle veliko novosti. V mobilnih omrežjih se bodo še dodatno povečale kapacitete, hitrosti in odzivnosti prenosa podatkov, pri čemer naj bi se korenito zmanjšala poraba električne energije. Zagotoviti bo potrebno sobivanje generacij, predvsem pa dodaten frekvenčni prostor, ki bo omogočil migracijo in razvoj. Proizvajalci opreme že nestrpno čakajo na standarde, da bodo njihovi proizvodi lahko podpirali standardizirano verzijo 5G. Cilj je povečati skupno kapaciteto mobilnih omrežij za faktor 1000, v večji meri pa tudi podpreti možnost nadomestila za fiksni dostop. 5G bo odigral eno ključnih vlog pri digitalizaciji družbe preko omogočanja vertikal interneta stvari (IoT), saj bodo omrežja 5G zmogla povezati na milijarde različnih naprav. Prav tako 5G omogoča razvoj komunikacijskih rešitev za kritične aplikacije. Z uporabo obstoječe tehnologije, načina načrtovanja, izgradnje in upravljanja omrežja, so pričakovane omrežne zahteve težko ali sploh neizvedljive ter ekonomsko nesmotrne. Tudi Evropa na področju razvoja 5G ne želi zaostajati, zato v sklopu programa 5G-PPP in Akcijskega načrta podpira razvoj nove generacije omrežja. V članku so predstavljeni izsledki raziskav za področju dostopovnega mobilnega omrežja naslednje generacije 5G, ki so bile izvedene v okviru evropskih razvojnih projektov iCirrus in CHARISMA: centralizirana arhitektura radijskega dostopovnega omrežja, virtualizacija uporabniških terminalov, neposredna komunikacije med terminali ter vidik varnosti na omrežnih povezavah.

Ključne besede - LTE, 5G, Telekom Slovenije, IOT, Radijsko dostopovno omrežje v grozdu, neposredna komunikacija med terminali, storitve v oblaku, hierarhično ter virtualizirano in distribuirano jedrno omrežje

Abstract — 4th generation of mobile networks (4G) which are already reaching impressive data transfer speed will be upgraded at the end of this decade into 5G. New technologies will bring many new features. Additional to further increase in data transfer speeds and reduced latency, power efficiency of the network will improve substantially. Sufficient additional frequency spectrum is needed for deployment. Equipment manufacturers are waiting for 5G standards, to ensure their devices will support those standards. The goal is to increase capacity of networks by 1000 times and significantly support fixed access substitution. 5G will play major role in digitalization of society via enablement of IoT verticals, due to its capability to connect billions of different devices.

With the existing communication technology, network planning, deploying and maintenance strategy is become ineffective to achieve the expected network performance. Also EU is trying to motivate development and deployment of 5G through different initiatives. In this article we present research findings in 5G radio access network, conducted within European projects iCirrus and CHARISMA: cloud RAN architecture, mobile cloud, device-to-device communication and network security.

Keywords — 5G, Telekom Slovenije, LTE, Cloud Radio access network (C-RAN), device to device communication (D2D), mobile cloud clone service

I. UVOD

Omrežja 4G so v zadnjih letih izredno hitro postala prevladujoča mobilna tehnologija. Na svetu je že skoraj 600 omrežij 4G LTE. V pičlih nekaj letih večina terminalov že podpira LTE, prav tako je velika večina prometa že opravljenega preko LTE. Z nekoliko zakasnitve se postopoma uvaja tudi VoLTE. Obstoječa omrežja LTE-Advanced že danes omogočajo hitrosti prenosa podatkov, ki pri nekaterih operaterjih dosegajo 1 Gb/s. Tovrstne nadgradnje omrežja LTE uporabljajo nove tehnologije, ki izboljšujejo prepustnost omrežja, pri čemer se ne izgubi kompatibilnosti s starejšimi implementacijami omrežij LTE. Hkrati s pomočjo teh nadgradenj lahko v praksi dosežemo zakasnitve okoli 10 ms.

S pomočjo omrežij LTE-Advanced smo uspeli doseči že zelo dobre rezultate. Pomembno je upoštevati, da standard LTE trenutno predvideva dvajset različnih kategorij terminalov glede zmogljivosti, ki postopno prihajajo na trg. Na trgu je že prvi mobilni terminal, ki podpira hitrost 1 Gb/s in sicer mobilni usmerjevalnik MR1100, ki takšne hitrosti dosega s pomočjo tehnologije MIMO 4x4. Kljub temu so hitrosti v ostalih omrežjih LTE-Advanced po svetu večinoma precej nižje, saj so hitrosti okoli 1Gb/s dosegli samo v testnih omrežjih, ki pa naj bi v kratkem bila na voljo tudi za stranke. Med drugim opremo, ki s pomočjo tehnologij MIMO 4x4 in QAM-256 omogoča hitrosti okoli 1 Gb/s, preizkuša tudi Telekom Slovenije. Trenutno je najvišjo hitrost omrežja LTE vzpostavilo podjetje Nokia, ki je v omrežju operaterja SK Telecom s pomočjo združevanja desetih frekvenčnih območij doseglo prenosno hitrost 4 Gb/s.

Hitrost in delovanje omrežja se izboljšuje predvsem z uporabo naslednjih tehnologij:

- S pomočjo tehnologije CoMP (Coordinated MultiPoint) se izboljšuje delovanje na robovih celic.
- Več ločenih frekvenčnih območij je mogoče združiti za doseganje večje hitrosti prenosa podatkov.
- Tehnologije MIMO 8x8 in 256 QAM omogočajo boljšo spektralno učinkovitost, kar pomeni, da lahko na enako širokem frekvenčnem območju dosežemo višje hitrosti prenosa podatkov, kot prej.

Družbeno tehnični razvoj v zadnjih desetletjih je bil izrazito oblikovan pod vplivom telekomunikacij (oziroma IKT), zlasti mobilnih. Telekomunikacije so se globoko umestile v vrsto področij, tako v osebnem kot poslovnem življenju. Kaže se potencial nadaljnjega razvoja digitalizacije predvsem na področjih: proizvodnja, transport, oskrba z energijo, zdravje, multimedija in zabava. Te je srenja 5G opredelila tudi kot fokusne vertikale. Tudi EU zelo podpira razvoj nove generacije tehnologije.

Za vse našteto in v pričakovanem obsegu pa obstoječe telekomunikacijsko omrežje ni bilo načrtovano, zato ni ne tehnično niti stroškovno učinkovito.

Pričakovati je mogoče večje zahteve po prenosnih kapacitetah, večji odzivnosti omrežja, zanesljivosti ter bistveno večje število različnih komunikacijskih naprav [1-3].

Za tehnično zadostitev večjim zahtevam je potrebno omrežje preoblikovati ter vnesti nove tehnične koncepte ter rešitve, ki bi to omogočile. S tem se trenutno ukvarja več mednarodnih organizacij ter konzorcijev, ki želi na različnih področjih omrežja evidentirati šibke točke ter poiskati učinkovite tehnične rešitve. Ključni tehnološki trendi razvoja so:

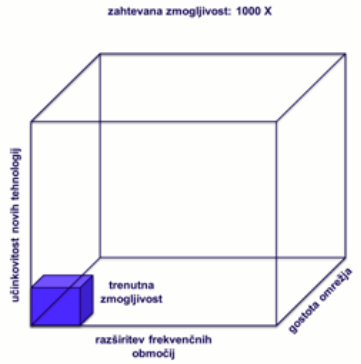
– gigabitne hitrosti na dostopu,
– virtualizacija, SDN, NFV,
– IOT, podprt s tehnologijo »Bigdata«,
– razvoj video vsebin,
– razvoj kibernetske varnosti in sistemov za kritične komunikacije.

Eden od teh je projekt iCirrus [4], ki ga sestavlja mednarodni konzorcij osmih evropskih partnerjev, z namenom raziskave razvoja na področju 5G-radijskega dostopovnega omrežja (RAN, Radio Access Network). Telekom Slovenije aktivno sodeluje v njem. Izsledki raziskav so predstavljeni v nadaljevanju.

II. SPLOŠNO O 5G

Med cilje mobilnih omrežij pete generacije (5G) spada tudi povečanje njihovih kapacitet v primerjavi s predhodniki za faktor 1000. To je mogoče narediti na več načinov. Lahko se poveča količina uporabljenega frekvenčnega prostora, število baznih postaj, se uvaja nove tehnologije in nadgradi hrbtenično omrežje.

Celotno povečanje zmogljivosti radijskega dela mobilnega omrežja lahko predstavimo kot produkt povečanja frekvenčnega prostora, ki je na voljo, izboljšanja hitrosti prenosa zaradi novih tehnologij (izboljšanje spektralne učinkovitosti) in povečanja gostote omrežja, kar lahko dosežemo s nameščanjem velike količine majhnih celic. Z novimi frekvenčnimi področji pod 6 GHz bomo v naslednjih letih vršno hitrost v omrežjih LTE povečali na nekaj Gb/s. V bližnji prihodnosti lahko objektivno pričakujemo za okoli dvakrat (do 6 GHz) do okoli 10-krat (nad 6 GHz) več frekvenčnega prostora in približno šestkratno povečanje zmogljivosti zaradi uvedbe novih tehnologij. Če bi želeli povečati kapacitete mobilnega omrežja za faktor 1.000, bi morali njegovo gostoto povečati za faktor, ki bo nekje med 16 in 83. Očitno bo povečanje zmogljivosti mobilnih omrežij slonelo predvsem na gradnji velikega števila majhnih celic. V prihodnosti bo pomembno tudi varčevanje z energijo, kar bo mogoče izvesti prav s pomočjo majhnih celic, ki bodo energijsko bolj učinkovite.



Slika 1: Zmogljivost mobilnih omrežij lahko povečamo na tri različne načine, katerih produkt nam da celotno povečanje kapacitete, ki ga lahko predstavimo z razliko v velikosti majhnega in velikega kvadra.

Peta generacija mobilnih omrežij še ni standardizirana, zato ne moremo govoriti o točno definiranih specifikacijah. Kljub temu je že jasno, kakšne lastnosti naj bi tovrstna mobilna omrežja imela. Hitrosti prenosa podatkov naj bi znašale med 10 Gb/s in 50 Gb/s, pri čemer bi zakasnitve padle pod 1 ms. Porabljena energija za prenos vsakega bita podatkov naj bi se zmanjšala za faktor 1000. Omrežja 5G bodo podpirala na milijarde povezanih naprav.

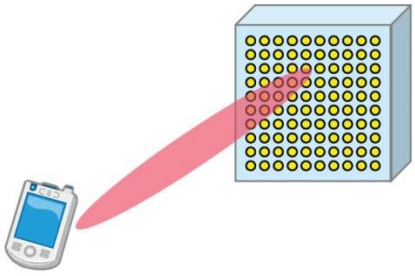
Prvi standardi za 5G naj bi bili pripravljeni v letu 2018, komercialno pa naj bi bila oprema in omrežja na voljo po letu 2020. Pot do 5G poteka preko standardov 3GPP, kjer se trenutno standardizirajo predvsem različne nadgradnje LTE. 3GPP približno vsako leto izda nov "release" standardov. LTE-Advanced je standardiziran od Release 10 naprej, LTE Advanced Pro pa od Release 13 naprej. V letu 2018 naj bi bil na voljo Release 15, ki bo vseboval prve funkcionalnosti 5G in bo namenjen za uporabo v prvih komercialnih 5G omrežjih, ki bodo na voljo leta 2020. Izpopolnjen Release 16, ki ga bodo pripravljali tekom leta 2019, bo na voljo za omrežja v letu 2021 in bo vsebovan v IMT 2020. Šele ta standard naj bi predstavljal pravi 5G.

5G bo slonel predvsem na naslednjih izboljšavah:

– tehnologiji Massive MIMO,
– uporabi visokih frekvenčnih pasov (6 – 100 GHz),
– ultra gostih omrežjih majhnih celic,
– tehnologiji 3D MIMO,
– uporabi Cloud RAN in MEC,
– uporabi kognitivnega radia in SDN,
– varčevanju z energijo.

Proizvajalci opreme pri tem napovedujejo hitrosti nad 10 Gb/s na uporabnika. Južna Koreja že namenja 1,5 milijarde USD za razvoj 5G, Evropa pa bo v okviru Horizon 2020 za 5G namenila okoli 700 milijonov EUR. Operaterji so sprejeli 5G manifest, GSMA združenje spodbuja razvoj »omrežja 2020«.

Ena od tehnologij, ki bo povečala izkoriščenost radijskega spektra in bo uporabljena v 5G, je tehnologija Massive MIMO, ki je še posebej uporabna na višjih frekvenčnih pasovih. Temelji na antenah, ki so sestavljene iz več kot 100 posameznih manjših anten, ki imajo lasten oddajnik in sprejemnik. S pomočjo SDR to omogoča oblikovanje zelo ozkega žarka, ki je usmerjen k posameznemu uporabniku. To zmanjša izgube na večjih razdaljah, ki sicer nastanejo pri višjih frekvencah. Antene namenjene višjim frekvencam se lahko minimizirajo, njihovo število pa se s tem lahko poveča. Zmanjšajo se tudi potrebe po dodatnih lokacijah za celice, manjša pa je tudi poraba elektrike, zato se zmanjšajo stroški obratovanja.



Slika 2: Tehnologija Massive MIMO bo znatno izboljšala prenosne hitrosti, zmanjšala porabo energije in zmanjšala potrebe po novih lokacijah baznih postaj.

Pomembno spremembo arhitekture bo prinesel Cloud RAN. Gre za centralizirano arhitekturo radijskega omrežja, v katerem je večino procesiranja izvedeno znotraj računalniškega oblaka. Centralna lokacija je izvedena kot računalniški oblak in znotraj nje se dogaja večina procesiranja, ki je bilo doslej izvedeno v okviru baznih postaj. Izvedba Cloud RAN temelji na uporabi anten Remote Radio Head (RRH) skupaj z izredno hitrimi optičnimi povezavami, pri katerih so zakasnitve zelo majhne. SK Telecom v Južni Koreji že uporablja centralizirano arhitekturo in virtualizacijo za njihova omrežja LTE. Cloud RAN gradi tudi NTT DoCoMo na Japonskem in China Mobile.

Na področju 5G so kljub nestandardiziranim rešitvam že pričeli dosegati hitrostne rekorde. Optus je v Avstraliji dosegel hitrost prenosa podatkov 35 Gb/s na frekvenčnem pasu 73 GHz, v laboratorijskih testih pa je Huawei dosegel hitrost 70 Gb/s. Različni operaterji in proizvajalci izvajajo testiranja, med katerimi je v praksi mogoče doseči hitrosti okoli 5 Gb/s.

Peta generacija mobilnih telekomunikacij bo še posebej primerna za internet stvari (IoT), saj bo povezala veliko število naprav. Te naprave bodo v omrežju povečale količino signalizacijskega prometa. Podatkovni promet v mobilnih omrežjih prihodnosti bo po napovedih vseboval vse več tovrstnega podatkovnega prometa med različnimi napravami povezanimi v internet, od pametnih avtomobilov, do pametnega doma, pametnih stavb, pametnih mest, telemedicinskih pripomočkov in drugih merilnih naprav in pripomočkov.

Rast hitrosti prenosa podatkov je pomembna za vse segmente prihodnjega ekosistema storitev, ki bodo glede tega vse zahtevnejše. Prihaja prenos videa v formatu 4K, ki zaradi večje ločljivosti zahteval drastično večjo prepustnost omrežja. To je še posebej pomembno pri organizaciji in prenosu športnih prireditev, kjer bo potreben ne samo prenos videa 4K ampak tudi zagotovitev spodobnega dostopa do interneta za obiskovalce, ki bi sicer preobremenili sedanje kapacitete mobilnega omrežja na kraju prireditve.

Prihajajo tudi tehnologije kot je navidezna resničnost (Virtual reality) in nadgrajena resničnost (Augmented reality), ki zahtevajo dobro odzivnost omrežja oziroma manjše zakasnitve.

III. CENTRALIZIRANO DOSTOPOVNO RADIJSKO OMREŽJE

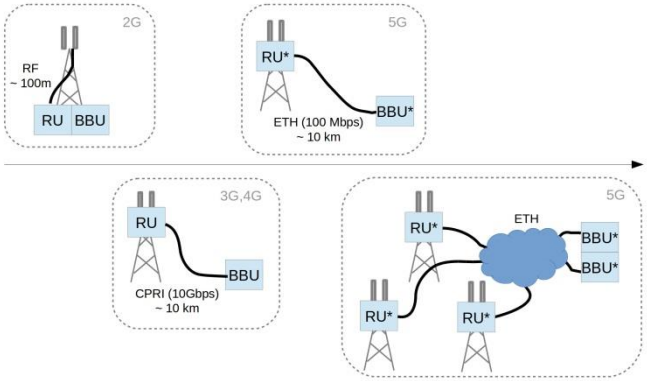
Z razvojem celičnih omrežij od 2G do 4G so si generacije sledile v razmiku desetih let. Z vsako naslednji generacijo se je povečal namenjen radijski spekter na celico (2G – leto 1990, BW=200 kHz, 3G – leto 2000, BW=5 MHz, 4G – leto 2010, BW=40 MHz). Trenutne smernice kažejo na to, da lahko podobno pričakujemo tudi pri prehodu na 5G.

Poleg uporabe čedalje večje radijske pasovne širine ter visoke stopnje modulacije (256 QAM), za povečanje razpoložljivih prenosnih kapacitet, se je pokazala potreba po novem konceptu zasnove zmogljivega dostopovnega mobilnega omrežja. Širitev frekvenčnega spektra v nedogled ni mogoče.

Z dodelitvijo čedalje večjega frekvenčnega spektra na eno celico, odpade frekvenčna ortogonalna delitev celic v omrežju. Kot se je pokazalo v sistemu 4G, kjer so vse celice v istem frekvenčnem pasu, je potrebna večja koordinacija med celicami za pravilno delovanje omrežja. V nasprotnem primeru motnje med celicami onemogočijo učinkovito izrabo danega frekvenčnega spektra.

Koordinacija celic v istem frekvenčnem spektru zahteva izredno sinhronizacijo in odzivnost med celicami ter zmogljivo obdelavo signalov. V nasprotnem primeru signale iz sosednjih baznih postaj ni mogoče učinkovito izločiti in predstavljano motnjo na isti frekvenci.

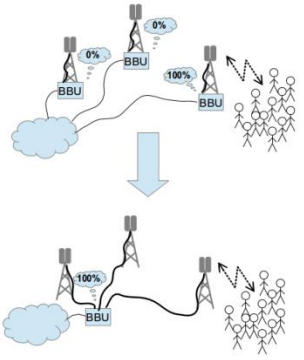
Zaradi takih zahtev se izkaže kot praktično izvedljivo koordinacija le v primeru, če so procesne enote v bližini, tako da ni zakasnitev v medsebojni komunikaciji. V 4G so tak primer sosednje celice na isti bazni postaji.



Slika 3: Razvoj elementov RAN: RU – radijski enota (angl. Radio unit), BBU – procesna enota (angl. Baseband unit), RF – visokofrekvenčna analogna povezava, CPRI – optična digitalna povezava (angl. Common public radio interface). RU*, BBU* - napredna 5G radijska in procesna enota

Možna rešitev za opisane zahteve koordinacije je centralizacija procesnih enot za večje število baznih postaj. Za grozd celic na omejenem področju, ki se deloma prekrivajo. Razmere so prikazane na sliki 3. V takem primeru so vse procesne enote na enem mestu in je zato koordinacija brez zakasnitev in učinkovita. V takem primeru bi bilo mogoče večje število posameznih procesnih enot nadomestiti z eno zmogljivejšo, tako da dobimo tako imenovano procesiranje v oblaku C-RAN (angl. Centralized, Cloud RAN) [5],[6].

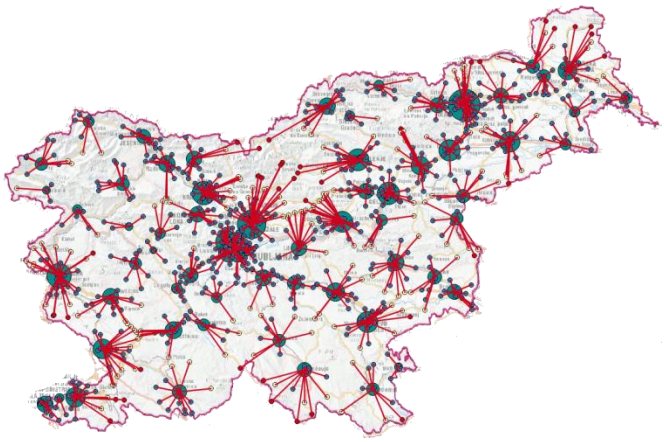
Topologija C-RAN omogoča poleg učinkovitega delovanja omrežja tudi optimizacijo omrežnih virov. Razmere so simbolično ponazorjene na sliki 4. Trenuten način izgradnje mobilnega omrežja zahteva načrtovanje celičnih kapacitet glede na trenutno največjo obremenitev celice (glavna prometna ura). Zaradi tega omrežje v povprečju deluje krepko pod največjo zmogljivostjo (20% – 30% od maksimalne prenosne kapacitete).



Slika 4: Simbolični prikaz statističnega multipleksa omrežnih virov

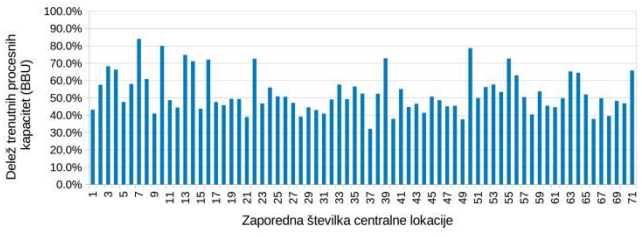
S centralizacijo in združitvijo procesnih kapacitet postane praktično mogoče izkoriščati časovno porazdelitev le-teh. Na ta način je mogoče dinamično dodeliti kapacitete trenutnim potrebam [9]. Zmanjša se celotno število potrebne opreme (procesnih virov) ter s tehničnega in ekonomskega stališča postane mogoče večja širitev posameznih celic (prireditve, ipd.).

Zaradi strogih zakasnitvenih zahtev na prenosnem delu omrežja, ni mogoče združiti vseh celic v en grozd [7],[8]. Prav tako ni tehnično potrebno, kajti oddaljene celice so radijsko ločene in ne potrebujejo koordinacije za nemoteno delovanje. Zaradi tega je smiselno združevati celice na zaključenih področjih. Primer je prikazan na sliki 5.



Slika 5: Primer združevanja celic (baznih postaj) v C-RAN arhitekturo. Manjši krogi ponazarjajo položaj bazne postaje, večji krogi so centralne lokacije (velikost odraža število priključenih baznih postaj).

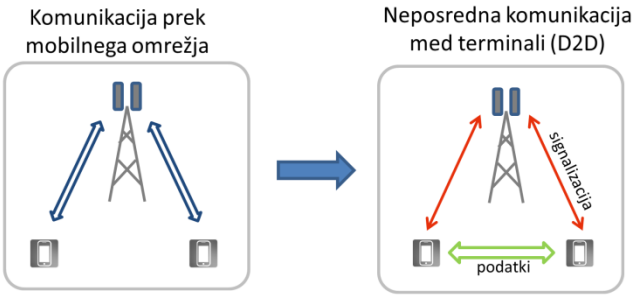
V primeru povezovanja celic v manjše grozde se zmanjša pričakovan izkoristek omrežnih virov iz naslova statističnega multipleksa. Za prikazan realističen primer so vrednosti prikazane na sliki 6. Razvidno je, da je mogoče tudi v realnem scenariju pričakovati znatno povečanje izkoristka opreme oz. optimizacija le-te. Velikost grozda se spreminja glede na gostoto celic na omejenem področju (urbano ali ruralno okolje).



Slika 6: Delež trenutnih procesnih virov (BBU) potrebnih za nemoteno delovanje v primeru združitve celic v grozd.

IV. NEPOSREDNA KOMUNIKACIJA MED TERMINALI

Poleg vedno večjih prednostnih kapacitet (večja pasovna širina in gostota celic) se v okviru razvoja 5G iščejo tudi rešitve, ki bi omogočale boljši izkoristek omrežnih virov in s tem celotnega omrežja. Kot ena možnost učinkovitejšega izkoristka omejenega radijskega spektra je neposredna komunikacija med uporabniškimi terminali. Osnovni koncept je prikazan na sliki 7. Gre za možnost vzpostavitve neposredne zveze med terminali (angl. Device to device – D2D), ki so se nahajajo na dovolj majhni razdalji [11]. V takem primeru ni potrebno prenašati podatkov po omrežju in s tem je mogoče do določene mere sprostiti dragoceni radijski spekter.

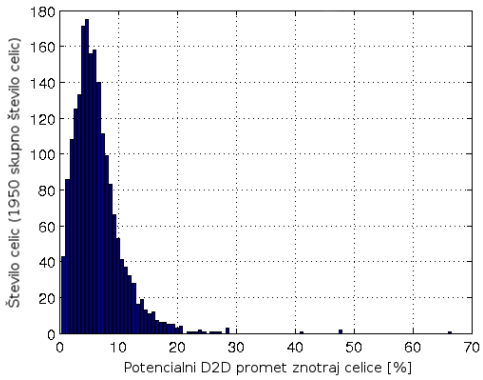


Slika 7: Neposredna komunikacija med terminali. Podatkovni promet poteka neposredno med terminali, za signalizacijo poskrbi krovno mobilno omrežje.

Za neposredni prenos med terminali se preučuje uporaba namenskega frekvenčnega spektra na višjih frekvencah, ki ne bi povzročalo interferenc z obstoječimi oz. frekvencami namenjenimi za klasični mobilni dostop. Visoke frekvence so za komunikacijo D2D zlasti primerne zaradi hitrejšega upadanja jakosti signala z razdaljo ter večjim vstavitvenim slabljenjem ozračja (npr. 60 GHz zaradi molekul vode). Na tak način je mogoče isti frekvenčni spekter pogosteje ponovno uporabiti.

Prednost predstavljene tehnologije z razliko od obstoječih možnosti na ročno neposredno povezovanje terminalov (npr. WiFi, BT) je v koordinaciji s strani omrežja. To vsebuje celoten nadzor, tako da uporabniku ni potrebno skrbeti za režim delovanja terminala.

Iz analize prometa v delujočem omrežju je mogoče sklepati, da obstaja dejanski potencial za D2D komunikacijo. Količina mobilnega prometa, ki se zaključuje znotraj iste celice je prikazana na sliki 8.

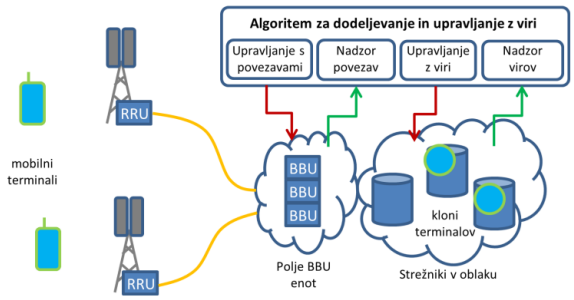


Slika 8: Količina prometa, ki se zaključuje znotraj iste celice, na podlagi katerega je mogoče oceniti D2D potencial.

V. VIRTUALIZACIJA TERMINALNE OPREME

Koncept virtualne terminalne opreme temelji na postavitvi zmogljivega strežniškega sistema na strani omrežja, ki služi kot podpora pri izvajanju zahtevnih operacij na strani mobilnih terminalov [12]. Na tak način lahko strežniki v oblaku za zahtevo terminala izvajajo procesorsko ter spominsko zahteven proces ter tako razbremenijo terminal oz. izboljšajo uporabniško izkušnjo (npr. večja navidezna zmogljivost ter avtonomija terminala) [10].

Za potrebe optimalnega delovanja se do določene mere uporabniški podatki ter nastavitve prenesejo na stran strežnikov, tako da se v teh ustvarijo tako imenovani mobilni kloni (angl. Mobile clones). Postavitev osnovnih elementov ter medsebojna komunikacija je ponazorjena na sliki 9.



Slika 9: Virtualizacija terminalne opreme z uvedbo mobilnih klonov.

Za pravilno delovanje oz. pričakovano uporabniško izkušnjo je ključnega pomena učinkovita komunikacija med terminalom in klonom ter učinkovitost algoritma za dodeljevanje virov. Ta odloči kdaj je smiselno določen proces izvajati lokalno in kdaj na klonu v oblaku. V odločitveni proces so zajete kompleksnost posameznega procesa ter zakasnitve pri prenosu zahtevka in podatkov do strežnikov.

VI. JEDRNO OMREŽJE

Arhitektura, ki nastaja v sklopu projekta je usmerjena k doseganju večine ključnih performančnih indikatorjev (KPI), ki jih definira program 5G-PPP za omrežja naslednje generacije 5G. Poudarek je v načrtovanju arhitekture, ki bo omogočala gradnjo nizko zakasnitvenih omrežij, ustrezno pokrivanje varnostnih vidikov in koncept odprtega dostopa oziroma gostovanja ali večnajemnosti, Koncept odprtega dostopa je ključen za učinkovito izrabo infrastrukturnih in omrežnih virov pri ponudnikih infrastrukture in omrežja pri telekomunikacijskih operaterjih, kot je Skupina Telekom Slovenije.

A. Nizka zakasnitev

Razvoj in implementacija omrežja 4G oziroma LTE je prispeval k večjim pasovnim širinam in seveda tudi veliko nižjim zakasnitvam. Kljub temu pa je v omrežjih 4G zakasnitev med končnima točkama še vedno odvisna od razdalje med podatkovnim centrom in točko stika omrežja 4G z Internetom. Posledično to pomeni tudi veliko večjo porabo pasovne širine zaradi multipliciranja podatkovnih tokov v primeru sočasnega in pogostega dostopanja do vsebine oziroma splošno do storitve pri ponudniku. Z arhitekturnega vidika je namen projekta CHARISMA univerzalna arhitekturna rešitev za propagiranje poslovne logike storitve proti robu omrežja (tudi v smeri naprav CPE) in zagotavljati optimalno podatkovno pot, deloma neodvisno od storitve. Funkcionalnost predpomnenja bi tako lahko zagotavljali na napravah CPE, baznih postajah in paketnem jedru.

B. Varnost in virtualizacija varnostnih funkcij

Visoka stopnja varnostni groženj in predvsem njihova pogostost zahteva avtomatizacijo in stabilno delovanje sistemov za odkrivanje in preprečevanje varnostnih groženj. Virtualizacija varnostnih funkcij omogoča centralni nazor nad varnostnimi funkcijami in hkrati tudi distribucijo uveljavljanja varnostne politike bližje nastanku same varnostne grožnje.

Predlagana arhitektura pristopa k varnostnim izzivom z inteligentnim upravljanjem, izolacijo virtualnih operaterjev, virtualizacijo varnostnih funkcij ter preverjanjem identitete in kontrolo dostopa. Prednost, ki jo prinaša virtualizacija varnostnih funkcij je agilnost, ki je dosežena z orkestracijo in upravljanjem razpoložljivih virov. Privzet pristop orkestracije je politika pravil. Orkestracija se izvaja na osnovi varnostnih pravil, kot jih predpiše upravljalec, slednja pa so lahko tudi rezultat spremljanja prometa za storitve in rezine, ki so že aktivne. Tako lahko orkestrator kreira nove, razširi obstoječe ali omrežne funkcije oziroma oplemeniti obstoječe omrežne funkcije z novo virtualizirano varnostno funkcijo za točno določeno varnostno grožnjo, ki jo zazna sistem za nadzor in analitiko prometnih tokov.

Ključne varnostne funkcije, ki so predmet razvoja na projektu, so odkrivanje varnostnih groženj, požarni zidovi in analiza paketnega prometa. Omrežje kot storitev ja lahko sestavljeno iz ene ali več varnostnih funkcij, glede na različne zahteve posameznih virtualnih operaterjev oziroma gleda na ponudbo in tudi zahteve ponudnika infrastrukture, nad katero je zgrajeno virtualizirano omrežje.

C. Odprti dostop

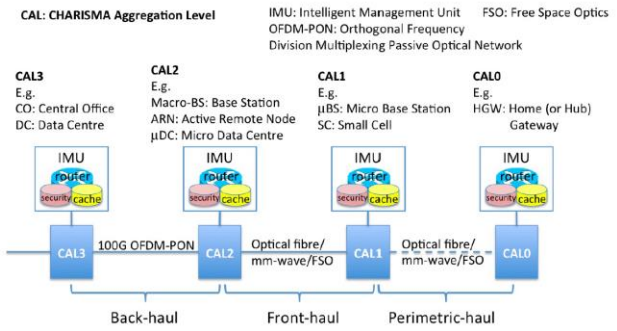
Konvergentna infrastruktura 5G ima sama po sebi značilnosti monopolistične naravne, tako da je zagotavljanje odprtega dostopa oziroma omogočanje gostovanja ključno za širše socialne, gospodarske in okoljske koristi. Seveda pa odpiranje dostopa pomeni tudi nove, cilju lastne, varnostne vidike in izzive za vse deležnike. Ti varnostni izzivi so obravnavani tudi znotraj projekta CHARISMA.

Nova arhitektura jedrnega omrežja omogoča virtualizacijo po rezinah in posledično odpravlja potrebo po namenskih fizičnih virih. Operaterji ponudniki lahko svojo infrastrukturo z uporabo virtualizacije zelo enostavno delijo med VNO-je in tudi upravljajo s presežki oziroma primanjkljaji, ki so pojavljajo pri posameznih VNO-jih. Vse to pa posledično kaže tudi na prihranke v smeri tako investicij kot tudi stroškov, in seveda bolj učinkovito, predvsem pa enotno upravljanje in nadzor nad vsemi vidiki infrastrukture. Omrežne funkcije so izdelane zgolj kot programske komponente nad enotno in virtualizirano infrastrukturo. Programska oprema pa predstavlja omrežne funkcije, ki jih tradicionalno opravljajo namenske fizične naprave. Vse skupaj pa na koncu temelji na standardni fizični opremi, ki ni specifična za posameznega ponudnika omrežnih funkcij.

VII. ARHITEKTURA JEDRNEGA OMREŽJA

Ključna arhitekturna novost oziroma inovacija projekta CHARISMA je uvedba sebi podobnega hierarhičnega pristopa aktivnih sredinskih omrežnih elementov med zalednimi sistemi (CO - Central Office) in končnimi uporabniki. Vsak aktivni omrežni element ima lastno inteligentno upravljalno enoto (IMU – Intelligent Management Unit), ki opravlja poslovno logiko, kot recimo predpomnjenje podatkov in usmerjanje podatkovnih podatkovnih tokov. Vsak aktivni omrežni element je vsebovan v več agregacijskih nivojih (CAL – CHARISMA Aggregation Layer).

V praksi to pomeni usmerjanje podatkovnih tokov, tam kjer je to smiselno oziroma možno, na najnižjem agregacijskem nivoju in na ta način omogoča doseganje nizkih zakasnitev med dvema končnima točkama.



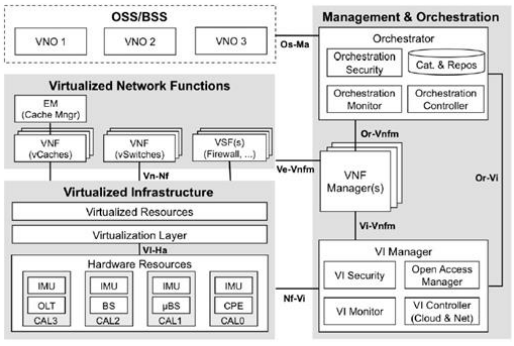
Slika 10: Hierarhični agregacijski nivoji CHARISMA

Ko govorimo o primeru dostave video vsebin, to pomeni da se izvaja predpomnjenje vsebine že na agregacijskem nivoju CAL0, to je omrežnem prehodu pri uporabniku, ko govorimo o stacionarnem uporabniku, in se celotni promet zaključi znotraj uporabnikovega domačega omrežja. V primeru mobilnega uporabnika, ki je prijavljen v javno mobilno omrežje, pa se predpomnenje lahko izvaja že na agregacijskem nivoju baznih postaj, to je CAL1 oziroma CAL2, odvisno od uporabnikove lokacije. V najslabšem primeru se predpomnenje oziroma dostava vsebine izvaja na nivoju CAL3, direktno v zalednem sistemu. Vse je odvisno od same arhitekture storitve in drugih zahtev, povezanih s samo storitvijo (e.g. specifike zaračunavanje storitve).

VIII. UPRAVLJANJE IN ORKESTRACIJA

Arhitektura nadzora, upravljanja in orkestracije sledi smernicam in arhitekturi ETSI NFV, slednja seveda predstavlja mednarodni standard, več letni razvoj na tem področju in je usmerjena v virtualizacijo in podporo gostovanju oziroma več najemnosti (multy-tenancy). Poleg tega ima arhitektura ETSI NFV tudi že razdelane varnostne in performančne vidike. Arhitektura obsega naslednje sklope:

– virtualna infrastruktura (VI – Virtualized Infrastructure),
– virtualizirane omrežne funkcije (VNF – Virtual Network Function),
– upravljanje in orkestracija (MANO – Management and Orchestration),
– upravljanje in vzdrževanje ter poslovna podpora (OSS/BSS).



Slika 11: Visoko nivojska slika upravljanja in orkestracije CHARISMA

Naloga nivoja VI je zgolj virtualizacija fizičnih virov (procesne enote, spomin, diskovni pomnilnik, omrežne kartice) z uporabo hipervizorja, ki skrbi za dodeljevanje fizičnih virov VNF-jem. Gruče različnih VNF-jev sestavljajo programsko opremo nad virtualizacijskim nivojem in v končni fazi del nekega IMU-ja. Projekt se primarno osredotoča na omrežne funkcije, kot so: predpomnenje, usmerjanje in varnostni mehanizmi. Sistem kot tak pa ni omejen na zgoraj omenjene, je odprt tudi za druge, kot na primer sistem za dostavo vsebin (CDN – Content Delivery Network). Nivo MANO vsebuje vse komponente, ki jih sistem potrebuje za orkestracijo posameznih komponent v omrežne funkcije in upravljanje življenjskega cikla slednjih. Nivo MANO pa komunicira s sistemi OSS in BSS, katerim sporoča stanje in od katerih prejema v izvedbo naročila.

IX. PREHOD NA 5G V SLOVENIJI

V prvi fazi bodo omrežja 5G uporabljala obstoječa omrežja LTE-A, nadgrajena z novimi funkcijami. Sočasno z nadgradnjo baznih postaj poteka tudi razvoj in nadgradnja prenosnih sistemov in jedrnega omrežja. Država napoveduje novo dražbo frekvenc, ki bodo omogočala višje vršne hitrosti in boljšo uporabniško izkušnjo na podeželju (700 MHz pas) ter v mestih (3.5 GHz). Z dražbo lahko pomembno vpliva na dinamiko razvoja. V primeru nerazumnih pogojev (visoka cena, prekratek čas možne izrabe ipd.) lahko tudi zaustavi razvoj, kar akcijski načrt EU implicitno skuša preprečiti, saj je korist za ekonomijo skozi pospešen razvoj in preprečitev razvojnega zaostanka Evrope za Ameriko in Azijo mnogo večja od kratkoročnih proračunskih potreb. Skozi prikrito obdavčitev (previsoke cene frekvenčnega prostora) lahko pričakujemo zamik uvedbe in tudi dvig cen za končne uporabnike 5G.

Za doseganje vršnih hitrosti nad 10 Gb/s obstoječi spekter ne zadošča. Zahtevane pasovne širine so dostopne le na mikrovalovnem pasu nad 6 GHz. Trenutno potekajo študije in analize, kateri frekvenčni pasovi so primerni za omrežja 5G in jih je lahko uskladiti po celem svetu. Na svetovni radijski konferenci (WRC) leta 2019 bodo določili ustrezen spekter. Tudi standardizacija v okviru 3GPP je trenutno usmerjena bolj v nadaljevanje izboljševanja obstoječih omrežij LTE in dodajanja novih funkcij. Primer je standard NB-IoT, ki ga nekateri proglašajo za tehnologijo 5G na omrežjih 4G.

Na frekvencah nad 6 GHz je previden povsem nov radijski vmesnik, primeren za radijske nosilce z širino več 100 MHz. Mikrovalovne frekvence danes uporabljamo predvsem za usmerjene linke in zveze z radijsko vidljivostjo. Nekaj sistemov je že namenjeno za zveze brez vidljivosti, kjer izkoriščamo odboj, uklon in razpršitev signala. S testiranji ter izkušnjami iz drugih sistemov (tudi WiGig na 60 GHz) bo omogočeno pravilno načrtovanje pravih sistemov 5G.

Ko bo izbran frekvenčni pas (leta 2019) in končana standardizacija, bosta verjetno potrebni še dve leti, da bo tehnologija (vključno s terminalno opremo) dozorela in bomo tudi v Sloveniji lahko intenzivno prešli na nadgradnjo sedanjih omrežij na 5G.

ZAHVALE

Raziskave, predstavljene v članku, so bile opravljene v okviru evropskih projektov iCIRRUS in CHARISMA, ki sta dobila sredstva iz evropskega programa Obzorje 2020 v

okviru pogodb št. 644526 in št. 671704 (angl. This projects have received funding from the European Union's Horizon 2020 research and innovation programme under grant agreements No 644526 and No 671704.)

LITERATURA

[1] IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond, ITU-R, September 2015
[2] 5G empowering vertical industries, 5GPPP, 2016
[3] NGMN 5G White paper, Februar 2015
[4] EU projekt iCirrus, http://www.icirrus-5gnet.eu/
[5] P. Chanclou, Z. Tayq, P. Turnbull, V. Jungnickel, L. Fernandez del Rosal, P.Assimakopoulos, N. Gomes, Y. Kai, H. Zhu, M. Parker, S. Walker, C. Magurawalage, K. Yang, H. Thomas, M. Castano Torres, I. Campos Rivera, F. Jesus Hidalgo Gonzalez, "D2.1 iCIRRUS – Intelligent C-RAN Architecture", 2015
[6] M. Georgiades, P. Michael, P. Chanclou, P. Ritosa, H. Thomas, S. Delaitre, N. Gomes, H. Zhu, P. Asimakopoulos, L. Fernandez del Rosal, K. Wang, "D2.2 Refined iCIRRUS architecture definitions and specifications", 2016
[7] P. Turnbull, H. Thomas, D. Venmani, P. Chanclou, V. Jungnickel, L. Fernandez del Rosal, M. Parker, P. Assimakopoulos, M. Kenan Al-Hares, N. Gomes, "D3.1 Verification of Ethernet as transport protocol for fronthaul / midhaul", 2016
[8] L. Fernandez del Rosal, V. Jungnickel, D. Muench, H. Griesser, P. Assimakopoulos, N. Gomes, Y. Kai, H. Thomas, M. Parker, C. Magurawalage, K. Wang, P. Chanclou, D. Philip Venmani, "D3.2 Preliminary Fronthaul Architecture Proposal", 2016
[9] H. Thomas, L. Fernandez del Rosal, P. Asimakopoulos, Y. Kai, K. Wang, P. Chanclou, D. Muench, "D3.3 SLA and SON Concept for iCIRRUS", 2016
[10] M. Parker, C. Magurawalage, G. Koczian, F. Adeyemi--Ejeye, S. Walker, S. Hadjitheophanous, Y. Kai, L. Fernandez del Rosal, V. Jungnickel, M. Castaño, "D4.1 User Equipment Offloading and Mobile Distributed Caching Definition for 60 GHz Networking", 2016
[11] C. Pan, Y. Kai, H. Zhu, L. Fernandez del Rosal, V. Jungnickel, S. Hadjitheophanous, P. Ritoša, G. Koczian, M. Parker,"D4.2 iCIRRUS UE D2D & D2I interfacing", 2016
[12] S. Delaitre, M. Castaño Torres, C. Magurawalage, K. Wang, P. Ritosa, P. Michael, M. Georgiades, "D4.3 Mobile Cloud Networking and Virtual Mobile", 2016
[13] Arthur D. Little, Connected Things, 2014
[14] Huawei, 5G: A Technology Vision, 2013
[15] 4G Americas, 4G Mobile Broadband Evolution, 3GPP Release 11 & Release 12 and Beyond, februar 2014.
[16] Ericsson, Orange, Telecom Italia, Telekom Slovenija, Telenor, PC on ECC/DEC/(11)06 Frequency arrangements in the 3.4-3.6 GHz band
[17] DAE Scoreboard 2013
[18] GSMA Intelligence, Global LTE network forecasts and assumptions, 2013–17, november 2013
[19] EU projekt CHARISMA: http://www.charisma5g.eu/
[20] Eduard Escalona, Amaia Legarrea, Shuaib Siddiqui, Kai Habel, Volker Jungnickel, Eleni Trouva, Oriol Riba, Marian Ulbricht, Andreas Foglar, Theodoros Rokkas, Ioannis Neokosmidis, Yaning Liu, Jean-Charles Point, Michael Parker, Geza Koczian, Terry Quinlan, Stuart Walker, George Lyberopoulos, Eleni Theodoropoulou, Konstantinos Filis, Spiros Spirou, Konstantinos Katsaros, Dimitrios Kritharidis, Konstantinos Chartsias, Blaž Peternel, Primož Jenko, Cláudio Rodrigues, Victor Marques, Eugene Zetserov, David Levi, Carolina Canales, Manuel Lorenzo, CHARISMA D1.1, CHARISMA intelligent, distributed low-latency security C-RAN/RRH architecture, 2016
[21] Kai Habel, Carolina Canales, Shuaib Siddiqui, Eduard Escalona, Eleni Trouva, Andreas Foglar, Marian Ulbricht, Yaning Liu, Mike Parker, Geza Koczian, Konstantinos Katsaros, Eugene Zetserov, George Lyberopoulos, Konstantinos Filis, CHARISMA D1.2, Refined architecture definitions and specifications, 2016
[22] Amaia Legarrea, Shuaib Siddiqui, Eduard Escalona, Eleni Trouva, Oriol Riba, Andreas Foglar, Marian Ulbricht, Yaning Liu, Mike Parker, Spiros Spirou, Eugene Zetserov, CHARISMA D3.1, V-Security Management Plane Design and Definition, 2016
[23] Shuaib Siddiqui, Amaia Legarrea, Eduard Escalona, Eleni Trouva, Yanos Angelopoulos, Oriol Riba, Andreas Foglar, Marian Ulbricht, Yaning Liu, Mike Parker, Geza Koczian, Stuart Walker, Spiros Spirou, Konstantinos Katsaros, Konstantinos Chartsias, Dimitrios Kritharidis, Eugene Zetserov, Carolina Canales, Victor Marques, Kai Habel, CHARISMA D3.2, Initial 5G multi-provider v-security realization: Orchestration and Management, 2016Yaning LIU, Matthias Sander Frigau, Eleni Trouva, Yanos Angelopoulos, Konstantinos Katsaros, Shuaib Siddiqui, Eugene Zetserov, Andreas Foglar, Michael Parker, CHARISMA D3.3, Initial Content Caching and Traffic Handling at SW Regex Integration, 2016

Mag. **Matjaž Beričič** je od marca 2017 direktor Jedrnega omrežja v Telekomu Slovenije. Od leta 1998, ko je na Univerzi v Ljubljani doštudiral elektrotehniko in telekomunikacije, leta 2002 pa je s tega področja tudi magistriral, je aktiven na področju mobilnih in fiksnih komunikacijskih tehnologij. V tem obdobju je bil aktiven v različnih vlogah s področja upravljanja, načrtovanja in vodenja projektov ali organizacij s področja mobilnih omrežij, jedrnih omrežij, sistemov za upravljanje zmogljivosti ter razvoju storitev omrežij pri operaterjih Simobil, Mobitel in v skupini Telekom Slovenije.

Dr. **Patrik Ritoša** je leta 2004 diplomiral in leta 2009 doktoriral na Fakulteti za elektrotehniko v Ljubljani na področju prilagodljivih antenskih skupin. Od leta 2009 je član razvojno raziskovalne skupine Telekoma Slovenije. Njegovo raziskovalno področje zajema: radijske in optične komunikacije ter računalniško (GIS) načrtovanje in optimizacijo radijskega omrežja. Osebna bibliografija vključuje: 10 izvirnih znanstvenih člankov, 1 patent ter več kot 30 znanstvenih prispevkov.

Pavel Kralj se je leta 2008 pridružil družbi Mobitel, prvemu slvenskemu mobilenmu operaterju. Oddelku za storitve z dodano vrednostjo se je pridružil kot analitik in arhitekt. Bil je vključen v načtovanje in razvoj portalske platforme za izdelavo portalov za mobilne terminale. Leta 2013 se je kot analitik in arhitekt pridružil oddelku za načrtovanje jedrnih sistemov. Danes je v Telekomu Slovenije vključen v strateško planiranje ter raziskave in razvoj jedrnega omrežja.

Iztok Saje se je z radiom spoznal kot mlad radioamater (S52D). Od leta 1992 se v Mobitelu ukvarja z načtovanjem, gradnjo in optimizacijo mobilnih omrežij. Sedaj je strateg za dostopovna omrežja v Telekomu Slovenije. Iztok je tudi predavatelj na VSŠ za telekomunikacije v Ljubljani.

Mag. **Peter Zidar** je vodja razvojnih projektov v Telekomu Slovenije. Ima več kot 22 let delovnih izkušenj na področju telekomunikacij in IT. Od leta 2000 je bil zaposlen pri Mobitelu, kjer je med drugim vodil projekte razvoja lokacijskih storitev, Uverture in postavitve spletnega portala Planet. Med leti 2003 in 2005 je vodil Sektor za projekte, od 2004 do 2010 pa je bil vodja Mobitelove raziskovalne skupine. Od leta 2008 do 2016 je bil predsednik operaterske skupine mednarodne organizacije UMTS Forum, v katerem je bil tudi član upravnega odbora. V vlogi predstavnika UMTS Foruma in Telekoma Slovenije je nastopil že na 30 mednarodnih konferencah po vsem svetu. Doslej je napisal že več kot 130 poljudno-znanstvenih člankov predvsem v reviji Življenje in tehnika, nekaj pa tudi v reviji GEA in prilogi Znanost časopisa Delo.

From Broadband to 5G

Damjan Slapar, Gašper Jezeršek, Ana Robnik, Iskratel, Slovenija

Abstract — According to requirements for 5G networks from various domains the upcoming 5G services are all about needs for high speed, ubiquitous availability, high reliability and ultra-low latency. The prevailing dilemmas operators are facing today are how to become great in customer satisfaction, what sort of services and applications to offer to residential, business and industrial users, and how to monetize these services and increase Average Revenue per User. The proposed technology enablers and built-in intelligence in multi-access/metro, edge and core networks within a coherent ecosystem of ICT and other industrial and governmental sectors are the key success factors. These technologies enable applications and services to be efficiently coupled with networks and information flows. We also tackle intensively the efficiency of different ownership models of the networks, business processes and automation, and encourage innovation and change in business models that bring the transformation of economics and social interactions. As standards and regulations have always been on the frontier of our work, we actively follow the ongoing 5G work carried out by main standardization bodies and open source communities, and use numerous results of their work.

Keywords — multi-access network, edge network, SDN, NFV, NG Core, C-RAN, MEC, VITEL 2017

Povzetek — Glede na zahteve različnih domen za omrežja 5G, potrebujejo prihajajoče storitve 5G visoke hitrosti, vseprisotno razpoložljivost, visoko zanesljivost in ultra nizke zakasnitve. Prevladujoče dileme, s katerimi se srečujejo dandanašnje operaterji, so: kako postati odlični v zadovoljstvu strank, kakšne vrste storitev in aplikacij ponuditi rezidenčnim, poslovnim in industrijskim uporabnikom in kako priti do prihodkov od teh storitev ter povečanja povprečnega prihodka na uporabnika. Predlagani tehnološki omogočevalniki in vgrajena inteligenca v večdosto-povnem in metro omrežju, omrežju na robu in jedrnem omrežju znotraj povezanega ekosistema IKT in drugih industrijskih sektorjev ter državnega sektorja so ključni faktorji uspeha. Te tehnologije omogočajo aplikacijam in storitvam učinkovitejšo spojenost z omrežji in informacijskimi tokovi. Dotikamo se tudi učinkovitosti različnih lastniških modelov omrežij, poslovnih procesov in avtomatizacije in spodbujamo inovativnost in spremembo poslovnih modelov, ki prinašajo preobrazbo gospodarstva in odnosov v družbi. Ker so bili standardi in regulativa vedno v ospredju našega dela, aktivno sledimo delu na področju standardizacije 5G in odprtokodnih skupnosti ter uporabljamo njihove rezultate dela.

Ključne besede — večdostopovno omrežje, omrežje na robu, SDN, NFV, NG Core, C-RAN, MEC, VITEL 2017

I. INTRODUCTION

The company Iskratel, d.o.o., Kranj, with its own brand, its own development and its own production, is traditionally present in the area of info-communication networks, services and applications. During the past 20 years we have based our product and solution portfolios on smooth transitions from circuit-switched to »All-IP« networks, supporting services differentiation and intelligence as near as possible to end users. With those transitions we have brought our customers into a journey of future-ready migrations of their networks and services. From the very beginning our power and customers' satisfaction has laid into data-driven approach and flexibility in order to provide an easy network adaptation and broader interoperability.

In accordance with our strategic guidelines in the last three years [1, 2], the company offers and will continue developing advanced solutions, not only in the field of 5G-ready networks, but also in the fields of rail and road transport, public safety and energy. We leverage our ICT expertise in delivering integrated solutions across telco, transport, public safety and energy industries, more and more with 5G-enablers as a common denominator. We believe that 5G networks and their technologies will enable the digitalization of society and economy, leading to the fourth industrial revolution, impacting the sectors mentioned before and broader society with solutions for home, communities and smart cities.

II. 5G NETWORK REQUIREMENTS

There is not a single "5G-ready networks" definition and their standardization is still an ongoing process. But we all know that with 5G networks we should and would get the converged, flexible, reliable, service-centric multiple network domains supporting application-driven business models.

The NGMN Alliance has attempted a definition of two general design principles [3], which we have taken into consideration:

- Provide expanded network capabilities: Figure 1 [4] shows the 5G key performance and capabilities targets as technology moves from International Mobile Telecommunications-Advanced (IMT-Advanced including LTE-Advanced, WiMAX release 2 and Internet access service) to IMT-2020 Networks. IMT-2020 supports services enhanced Mobile Broadband (eMBB), massive Machine Type Communications (mMTC) and ultra-reliable and low-latency communication (uRLLC).
- Design intelligent "poly-morfic" systems: provide a flexible system that can be tailored to services and application required by users with highest QoE possible. The network softwarization (e.a. virtualization of network functions, software defined networks, fog computing) will play a pivotal role in enabling such flexibility.

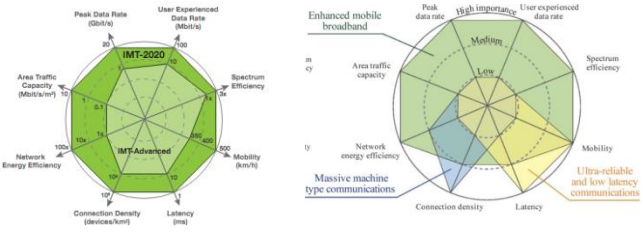


Figure 1: From IMT-Advanced to IMT-2020 [4]

Besides expected requirements for 5G networks that have been posted within NGMN Alliance [3] a plethora of use cases of industrial and other sectors and also consumers have been defined [5, 6, 7, 8].

Based on these high level service groups within IMT-2020, a wide range of actual use cases are listed in [4, 7], with specified most important requirements. Some of those use cases can be realized also by extending currently available LTE advanced Pro (4G) solutions. Special focus is on the use cases that are close to our market demands and incorporate the domains related to emergency communication, massive number of geographically dispersed devices, smart city, and broadband to the home. In the table below we have collected the most important use cases and their requirements, together with the desired values of performance and capabilities targets.

Table 1: Use cases and their requirements, together with the desired values

Use case	*Requirements*	*Desired values*
Emergency communication	Availability Energy efficiency	99.9 percent victim discovery rate One-week battery life
Broadband to the home	Connection density Traffic density	4,000 devices/km^2 60 Gb/s/km^2
Smart City	User throughput Traffic density Connection density	DL: 300 Mbps, UL: 60 Mbps 700 Gb/s/km^2 200,000 devices/km^2

An important aspect of 5G networks is to offer ubiquity of broadband connection with the user experience continuity from urban districts to rural areas. With digital divide a fast broadband connectivity is a commodity. The European Commission has clearly defined broadband speed targets for the year 2020 of 100 % population coverage with at least 30 Mbps, and 50 % with at least 100 Mbps and for a fully functional Digital Single Market for the year 2015 to ensure access to ubiquitous, very high-capacity fixed and mobile infrastructures with the Action Plan for 5G [9, 10, 11].

These targets put additional motivation and pressure on developing broadband access architectures and 5G networks that are capable of reducing connectivity costs in rural areas and compliant with open-access business models. In 5G ecosystems the customer is king and information is queen. Security and privacy are cornerstones for 5G to become a platform for the Networked Society and Digitized Industry. 5G will drive new requirements due to new business and trust models, innovative service delivery models, an evolved threat landscape and an increased concern for privacy.

Last but not least important is end-to-end QoS implementation and its assurance in future 5G networks. This will be facilitated by the development of open and programmable networks, based on the SDN paradigm, there are ongoing work among industry fora for delivery Broadband Assured Services. This is why the 5G networks are considered more and more as an end-to-end 5G system.

All these requirements will not stand the challenge of minor upgrades of today's networks. A new 5G vision and its realization [3], which already includes design principles that will support newly defined services and applications using 5G networks, is required.

III. ENABLING TECHNOLOGIES FOR 5G NETWORKS IN ISKRATEL PRODUCTS

A. LR-PON technology in Lumia supporting access-metro network consolidation

In order to reduce the complexity and hierarchical layers in traditional optical networks with separate access, metro and core networks, the Long-Reach PON (LR-PON [12]) architecture consolidates access and metro networks and supports the direct linkage of access fibre to a small-number of Metro-core nodes, which serve both the access network and the flat optical core. This new architecture will be more likely deployed in the Western Europe, especially in case of green field installations, but is not very likely used by our customers in the Common Independent Countries including Russia. This technology with new architecture reduces cost, both CAPEX and OPEX. It can be even more cost effective than Fibre to the Cabinet.

B. Lumia supporting multi-access technologies consolidation

With its intelligence and service-flow awareness as near as possible to users Lumia is ready for tomorrow's services already today. It has multi-provider environment support for wholesale and open access, and is ready to host NFV appliances.

The ultimate network access architecture can safely support the service requirements of the next decade and beyond, supporting same features regardless of current access technologies already today. Various subscriber-connectivity interfaces including GPON and point-to-point fiber (100 Mbps and 1 Gbps), VDSL2 with vectoring, ADSL2+, POTS, two-party POTS, ISDN in the same product ensure high infrastructure profitability. Several access scenarios are fully supported (FTTH, FTTC, FTTB, as well as DSL, POTS, ISDN from CO).

In the next years the residential users will be upgraded to XGS-PON [13] with one single channel operating with symmetric 10 Gbps rate due to the high initial cost of NG-PON2 [14]. NG-PON2 will be used for offering enhanced services and higher flexibility for business users and mobile cell interconnection (standard back/front- and cross-haul).

C. Cloud Services Platform supporting Cloud and Fog Computing with MANO capabilities

Cloud Services Platform (CSP) is the result of strategic considerations and outlines the concrete implementation approach of elastic infrastructure for services of today and tomorrow – not only in the telco segment, but also in segments of energy, intelligent transport and public safety.

CSP represents the infrastructure for a carrier-grade centralized or distributed cloud (Cloud and Fog Computing) and includes support for process automation, cloud management with full monitoring and alerting, as well as supervision of applications and system functions.

The system as a whole is managed by a Management and Orchestration (MANO) layer, also defined by ETSI [15, 16].

D. Next Generation Core

3GPP Release 14, which will be closed in June 2017, includes 400 pages study that will specify Next Generation (NG) Core for 5G [17] (new name instead of Evolved Packet

Core (EPC)). The study includes important aspects like Virtualization, Network Slicing, Control and User Plane Separation (CUPS), reconsideration of protocols and new approaches to the persistent topics of cellular networks such as security, mobility QoS and charging. It includes solution proposals that decompose the existing functions and recombine them for the different use cases that are part of 5G including enhanced MBB but also beyond MBB. Later releases 15 and 16 will further specify more advanced mesh and relay capabilities, access network selection mechanisms to determine the best available connectivity according to need or policy.

Beside these working groups 5G is attracting a lot of attention from different organizations which are working in turning the vision into reality. Vision for 5G is now established and supported worldwide.

It is still early to know how much from the existing EPC will remain in the NG Core, which will be the main system connecting subscribers over various access networks to services and applications.

The current EPC deployment on CSP and integration with Fault Monitoring System (FMS) can address many use cases on the market with unique requirements that are not of an interest to big EPC vendors.

In addition to EPC the voice applications (IMS and TAS), that are significant part for VoLTE and voice added services, play significant role. With strategic focus on IoT and Public safety infrastructure projects EPC is an important part at the cellular access networks. Current leadership position in Fixed Broadband access with support for Next Generation (NG) Core can provide cutting-edge fixed mobile convergence solutions.

E. Rich-set of VNFs on CSP

The key concept for NFV is the ability to run all network functions as software which is virtualized over a common pool of compute, storage and network resources. The operators defined their priorities in conjunction with VNFs in [22].

Software-defined IMS network functions (S/I/P/E-CSCF) are decoupled from the underlying HW through virtualization middleware and deployable on any x86-based hardware and supports also on-boarding on any KVM-based cloud platform. Cloud implementation enables hosting operators with new SaaS model for providing each tenant with its own, logically separated, virtual network, which can be deployed only for certain period of time.

EPC is as VNF deployed on Cloud Service Platform (CSP). While deploying EPC as VNF in the Cloud some challenges have appeared. The first key issue is performance. There is a performance cost of virtualization that can be problematic for UP functions, like SGW and PGW. Our solution relies on Intel's Data Plane Development Kit (DPDK) that increases and optimizes packet processing per second. Latency is another issue with the virtualization that affects MME, which requires tight time limitations to respond to procedures towards the access network and device.

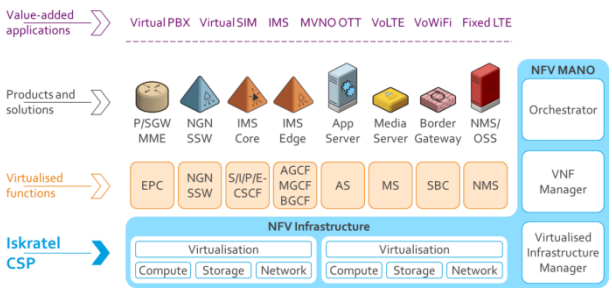


Figure 2: Cloud Network Portfolio and currently supported VNFs

The benefit from NFV to the operator is the agility of deployment and capability to scale. Network functions can be instantiated quickly and they can consume the exact amount of resources they need. NFV is also enabler for Network Slicing and Multi-access Edge Computing (MEC).

F. Lumia supporting SDN paradigm

Open and programmable networks, based on the Software Defined Networking allow service providers to quickly deploy new services in their infrastructure. Software Defined Networking (SDN) is an approach to simplify and make more flexible the management of large networks by decoupling control plane (CP) from user plane (UP). SDN for networks comes together with NFV. Virtualization decouples the software which performs network functions from the hardware. SDN provides higher level APIs that offer higher level applications to manage network infrastructure. Business vice SDN is bringing to the operator capability that business customers on top of residential customers purchase provision and manage their networking resources on demand.

SDN concepts are incorporated in Lumia. ISA (Intelligent Service Access) is our SDN/NFV based application that is QoS application for SDN.

Considering EPC and NG Core, then SDN together with VNF is enabler for Network slicing.

G. Network slicing

Network slicing allows creation of multiple logical networks (or slices) on top of the same physical infrastructure. Resources can be dedicated exclusively to a single slice or shared between different slices. There are different types of resources such as computing, storage, access equipment, transport, VNFs, and so on. Resources are completely managed as a pool of elements that can be grouped for specific use cases.

For example, with network slicing, a slice of the network, which includes resources at access, transport and core network, can provide service for:

- cMTC with highly reliable and secure low latency connectivity,
- another network slice provides mMTC service, that requires low bandwidth, high latency and high amount of sensors
- or another slice that only servers fixed sensors and does not need all the signaling overhead for mobility.

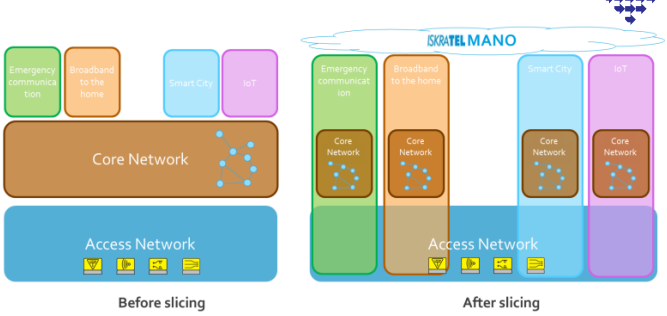


Figure 3: Architecture before and after network slicing applied

Network slicing requires management and orchestration that is provided by CSP and MANO VNF, which is based on ETSI compliant Open Baton framework. It requires management and control of all resources available in the network, programmability and dynamic re-configuration. Traffic isolation and security must be provided with proper management of different reliability requirements.

The business opportunity is huge, especially in cooperation with CSP and MANO, where Network slices can be instantiated either per service or per user specifics.

H. Compact EPC/IMS supporting MEC

Multi-access edge computing (MEC) provides cloud-computing capabilities within the access network or in close proximity to the subscribers. It brings the service nearer to the edge of the network. Regional and central data centers support the same type of services but can be accessed through the access network and the transport network. MEC can provide better service in terms of latency and resiliency. Due to localized traffic networks are offloaded with traffic at backhaul and transport.

An important challenge for MEC is that applications are light weight and optimized for running on the edge. EPC solution is lightweight enough to run for example on Atom based Raspberry Pi 2 and is suitable for distributed MEC architecture. Such architecture enables use cases for autonomous networks, public safety applications and cases for industrial internet with low latency requirements.

Lightweight Compact IMS can be inserted as VNF to MEC.

I. Cloud RAN

Important enabler for 5G networks is also a Cloud RAN (C-RAN), a deployment concept for the RAN which takes advantage of the general virtualization of telecommunications infrastructure and is fully in line with the 5G vision of NFV. In principle the equipment at the access of the network e.g. eNodeB can be divided ino two elements: the radio unit that requires hardware (i.e. the antenna and radio chipsets) and the Base Band Unit (BBU) that is only software. The BBU, being only software, can be deployed virtualized at a central location.

The main purpose of C-RAN is cost reduction of network operation and increased flexibility, since Software is moved to the Cloud as VNF.

C-RAN does not have direct effect to the EPC and NG Core, the network will continue to backhaul towards the core network, but C-RAN as VNF can coexist with NG Core VNF on the same decentralized location and this is another step for efficient end-to-end Network slicing.

C-RAN as VNF can be hosted at operator common CSP.

IV. STANDARDIZATION ACTIVITIES TOWARDS THE 5G DEPLOYMENT

The Next Generation Mobile Network Alliance was one of the first fora to come up with a set of use cases, architecture and technology propositions for 5G, together with business models.

The standardization bodies have been working intensively to evolve the current technologies towards 5G. For the technologies presented in the previous chapter we have collected roadmaps of the major standardization bodies, relevant to our work. We include some highlights from the roadmaps of the major bodies like ITU (ITU-R, ITU-T), IEEE, ETSI and 3GPP in the Figure 4 [17, 18, 19, 20, 21].

It is worth mentioning that the results of 5G PPP programs under EU's Horizon 2020 have been valuable inputs for standardization bodies. 5G PPP issued its 2016 annual journal with an update of these 17 programs and views of technology and spectrum for 5G [25].

ITU Radiocommunication Sector (ITU-R) is active in standardizing radio aspects of 5G trough the IMT-2000 programme. It works in close collaboration with 3GPP.

3GPP system standards Related to 5G are centered on the strategic areas like "Enhancing LTE radio", "Enhancing standards to make LTE and EPC available to new business" and introducing improvements for system robustness, especially for handling exponential smart phone traffic growth. Releases 13 and 14 (a part of LTE-Advanced framework) introduced 5G enhancements (Full Dimension – Multiple Input Multiple Output, Licensed-Assisted Access, enhanced carried aggregation to increase the number of carriers). Releases 15 and 16 will further specify more advanced mesh and relay capabilities, access network selection mechanisms to determine the best available connectivity according to need or policy. They will complete 5G Phase 1 and 5G Phase 2. Release 14 and 15 include Critical Communications Features and Mission Critical Enhancements (MC Voice, MC Video among others).

The complete IMT-2020 specification will be available with Release 16 by 2020 (new air interface for operations above 6 GHz in addition to evolutions that are backward compatible with LTE below 6 GHz, Vehicle-to-X with studies on improving robustness, latency and capacity of the mobile communication system).

ITU-T has standardized the XGS-PON (cost effective delivery of symmetric 10 Gbps to the residential market) and NG-PON2 (up to 80 Gbps symmetric rates over 8 10 Gbps wavelength channels).

IEEE SDN Initiative published White paper in 2016 (Network Softwarization, Open Mobile Edge Cloud, security and policy, potential role of open source communities, socio-economic impact).

IEEE also works on 802.11ax/ac/ad (labeled High efficiency Wi-Fi, 10 Gb/s access point, frequency bands between 1 and 6 GHz,) and on update of 10 Gb/s PON with 802.3ca with possible physical layer data rates of 25, 50 and 100 Gbps by the end of 2019.

ETSI has been active on Network Function Virtualisation from its emergence (ETSI NFV ISG) and published two releases in 2014 (an infrastructure overview, an architectural framework, descriptions of the compute, hypervisor and network domains of the infrastructure) and 2016 (NFVI hypervisor requirements, MANO, VNF Manager). The third

release targets charging, billing, accounting, policy and VNF lifecycle management and more. In April 2017 ETSI's Open Source MANO (OSM) group has announced the availability of its OSM Release TWO, an open source Management and Orchestration (MANO) software stack closely aligned with ETSI NFV.

ETSI NGP ISG (Next Generation Protocol) released a document with the key scenarios to evolve the current Internet Protocol (IP) in 2016.

ONF is the reference consortium for the standardization with the release of Open Flow 1.5 and accelerator of adoption of the SDN and NFV paradigm. The merger of ON.Lab with ONF and the CORD® and ONOS® open source projects create an Open Innovation Pipeline in close collaboration with the leading network operators.

In 2016 IETF released 3 new documents looking at network slicing, virtualization and ID location splits in 5G Networks.

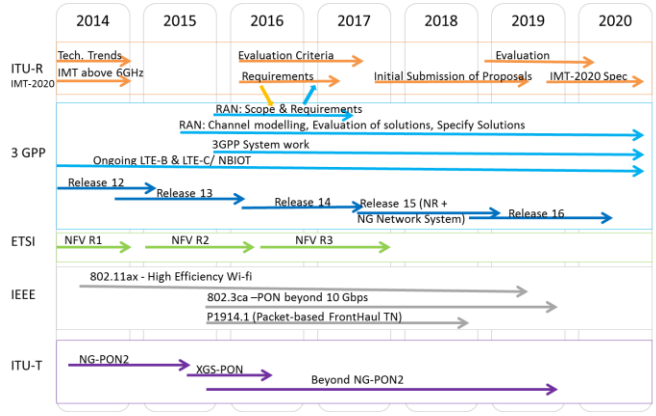


Figure 4: Roadmaps of the relevant SDOs [17, 18, 19, 20, 21]

V. OWNERSHIP MODELS AND MULTI-TENANCY, BUSINESS MODELS

In their pursuit of business sustainability, network operators and service providers carefully evaluate the business value of vendor-provided solutions. Business-related expectations dictate the choice of technology for providing advanced solutions, while the range of applicable use cases defines the implementation of (hardware, cloud and network) infrastructure layers.

Not only should these layers use modern technologies like software-defined networking or network-function virtualisation; they must assure high elasticity of the platform, be able to provide future high-value services, and prove useful in innovative business models.

We have studied thoroughly the FTTH business models [23] while introducing Intelligent Service Architecture in Lumia, which already supports wholesale model and open access.

According to FTTH business guide the following three layers of network ownership domains support multi-tenancy principles:

– the passive network infrastructure (ducts, fibre with any passive splitter element, and copper on legacy networks),
– the active network infrastructure: transmission and switching equipment,
– the service layer: service provisioning to the end users.

Out of this layering we got various business models and regulations as shown in the Figure 5. Active network sharing allows (retail) service providers to sell also bandwidth services with some QoS differentiation, but they could not fully customize services for business and industrial sector because of lack of network infrastructure control. Open access of the active network infrastructure is required in order to share infrastructure costs and open market to better competition.

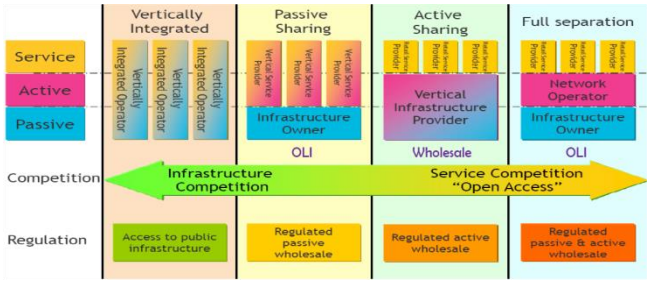


Figure 5: FTTH Business models [23]

The next step in increasing the control of service providers over the access network through virtualisation is the ownership model proposed by Fixed Access Network Sharing study group from Broadband Forum [24], which differentiates between:

– An Infrastructure Provider (IP) that owns and maintains physical networking infrastructure (e.a. passive and/or active), enables physical resource and network virtualisation, and provides virtual resources controlling APIs for Virtual Network Operator (VNO),
– A Virtual Network Operator that operates, manages and controls its assigned virtual network instance and its own virtual networks with highly-customized services.

Based on this ownership model the IP and VNO could introduce innovative network and digital services, especially for business and industrial sectors. It is also a base for disruptive business models, in which they monetize not only time- and volume-based resources, technologies and services, but also engage their customers in a monetizing process (knowledge out of data, intelligent products, etc.) and/or build an ecosystem of partners in a value chain. The latter business models offer endless opportunities for ARPU and revenue increase using monetizing models like One-time Charges, Pay-for-Results, Freemium, Subscription, Pay-as-You-Go. These business models are closely connected with innovative, intelligent and knowledge-based services and applications on 5G networks, and rely on long-term partnerships.

REFERENCES

[1] Business Strategy and Vision, documentation on Iskratel Intranet .
[2] Reports from technology analysts (IDC, Gartner, OVUM, MIT Sloan, SDX Central , …).
[3] NGMN 5G White Paper V1.0 by NGMN Alliance, 16.4.2016 s strani https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf .
[4] Recommendation ITU-R M.2083-0. (09/2015). IMT Vision Framework and overall objectives of the future development of. IMT for 2020 and beyond..
[5] Home page 5G PPP https://5g-ppp.eu .
[6] 5G PPP 5G Architecture – (White Paper) Updated July 2016.
[7] Ericsson, White paper UEN 284 23-3251.
[8] DRAFT NEW REPORT ITU-R M.[IMT-2020.TECH PERF REQ], 22.2.2017.

[9] Comission, European., 2010: A Digital Agenda for Europe.
[10] Comission, European. (14.9.2016´). COM(2016) 587 final: Connectivity for a Competitive Digital Single Market – Towards a European Gigabit Society, Brussels.
[11] Comission, European. (14. 9 2016). COM(2016) 588 final: 5G for Europe: An Action Plan {SWD(2016) 306 final}. Brussels.
[12] Recommendation ITU-T G.984.re: Long-Reach PON.
[13] Recommendation G.989.2, "40-Gigabit-capable passive optical networks 2 (NGPON2): Physical media dependent (PMD) layer specification", ITU-T, December 2014, http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12097.
[14] Recommendation ITU-T G.9807.1 "10-Gigabit-capable symmetric passive optical network (XGS-PON).
[15] ESTI white paper, Network Functions Virtualisation (NFV). October2013, available at http://portal.etsi.org/NFV/NFV_White_Paper2.pdf[25].
[16] ESTI white paper, Network Functions Virtualisation (NFV). October2014, available at http://portal.etsi.org/NFV/NFV_White_Paper3.pdf .
[17] ITU-T Recommendations, available at www.itu.int/ITU-T/recommendations/ .
[18] ITU-R recommendations, available at www.itu.int/pub/R-REC.
[19] ETSI standards, available at: http://www.etsi.org/standards .
[20] 3GPP specifications, available at: http://www.3gpp.org/specifications/releases .
[21] IEEE standards: available at: https://standards.ieee.org/ .
[22] Network Functions Virtualisation – White Paper on NFV priorities for 5G, 21.2.2017, available at: http://portal.etsi.org/NFV/NFV_White_Paper_5G.pdf
[23] FTTH Council, FTTH Business Guide, Edition 5, Financing Committee, Feb. 2016. Available at: http://www.ftthcouncil.eu/documents/Publications/FTTH_Business_Guide_V5.pdf
[24] Fixed Access Network Sharing (FANS), Broadband Forum, WT-370 and WT-386.
[25] 5G PPP - The European 5G Annual Journal/2016. Available at https://bscw.5g-ppp.eu/pub/bscw.cgi/d117642/Euro%205G%20Annual%20Journal%202016.pdf

Damjan Slapar is Chief Technology Officer at Iskratel. He has more than 25 years of experience in Cloud applications and computing, software services and platforms, software architecture, development methodologies, business development and strategic technology planning. He is also acting change manager – reshaping and transitioning individuals, teams and organizations. Before joining Iskratel, the leading European infocommunications provider, Damjan was a co-founder and CTO in Marg and before that Chief Software Architect in HERMES SoftLab. For more information, please email damjan.slapar@iskratel.com or connect on LinkedIn.

Gašper Jezeršek is program manager for Evolved Packet Core at Iskratel. He has 17 years of experience in telecommunication industry, WiMAX, Micro/Millimeter wave radio technology, Carrier Ethernet, manufacturing automatization and IT, Electronic manufacturing technology, Quality audit for corporate processes and productions. For more information, please email gasper.jezersek@iskratel.com or connect on LinkedIn.

Ana Robnik is a telecommunications consultant, coordinates work in standardization organisations at Iskratel and leads the Research group ISKRATEL. She graduated in applied mathematics from the Faculty of Mathematics, Physics and Mechanics, University of Ljubljana, in 1985. She earned her master's degree in computer science from the Faculty of Computer and Information Science, University of Ljubljana in 1989. She started her career in the Research Department of Iskra Kibernetika and continued in IT department of Iskratel. Until 2009 she worked as a head of the sector for the development of a system for the management and monitoring of network elements from the Iskratel portfolio.

5G Systems: Enabling the Transformation of Industry and Society

László Szilágyi[i], Ericsson Hungary

Abstract — In this paper we have a look at 5G use cases first. The use cases can be classified in terms of requirements for three essential types of communication with vastly different objectives: massive machine type communication (mMTC), critical MTC, and extreme or enhanced mobile broadband (eMBB). The three types that can be also designed as 5G services are discussed next. The evolution of the network components toward 5G is then presented, followed by a description of the 5G system. Finally, the 5G system is exemplified through three concrete use cases: Massive Number of Geographically Dispersed Devices, Virtual and Augmented Reality and Factory Automation.

Keywords — 5G, IoT, MTC, URLLC, eMBB, Network Slicing

I. INTRODUCTION

A digital transformation, enabled by mobility, cloud and broadband, is taking place in almost every industry, disrupting and making us rethink our ways of working. With the dawn of the 5G era, new use cases for the technology are emerging as consumers and enterprises set to work on identifying processes and channels that will boost the efficiency of their lives and their business. Wireless connectivity is at the center of this technological revolution. New business opportunities are opening up – both for those that have traditionally participated in the value chain, such as telecom operators, and for newcomers from other industries. Even the value chains themselves are undergoing a transformation, with content and end-to-end services becoming ever more important. New business models are being created with a focus on distributed cloud services and programmability of networks toward the edge. An unprecedented ability and willingness to share information is leading to a greater degree of collaboration between people and all kinds of different industries. Solutions that involve many areas of expertise are being created, overturning traditional business models and redefining ecosystems in the process.

This cross-industry transformation has created a need to evolve the concept of wireless connectivity for the fifth generation of mobile technology (5G), to enable new ways of defining performance monitoring and assurance as well as quality of service and level of user experience [1-2]. Compared with previous generations of wireless communications technology, including 4G, the rationale for 5G development is to expand the broadband capability of mobile networks, and to provide specific capabilities not only for consumers but also for various industries and society at large, hence unleashing the potential of the Internet of Things (IoT).

In this paper, the 5G use cases are outlined first. The evolution of the network components toward 5G is then presented, followed by a description of the 5G system. Finally, the 5G system is exemplified through three concrete use cases.

II. 5G USE CASES

Several industry bodies have set the requirements in terms of what 5G actually is. Here we explore a number of promising use cases that represent various key sectors [3]: namely the automotive industry, construction, energy, health, manufacturing, media, retail and transport.

- Autonomous vehicle control enables an increase in autonomous driving, assisting humans, for instance, and bringing a number of benefits such as an improvement in traffic safety, increased productivity, improved quality of life and so on.
- Intelligent transportation systems (ITSs) facilitate efficient traffic management, dynamic traffic rerouting, traffic light control and so on.
- Emergency communication needs a reliable network that can help with the search and rescue of humans, and the identification and rectification of catastrophic problems involving machinery – even if parts of a network have been damaged in a disaster.
- Factory cell automation is a system including devices in an assembly line communicating with control units with a sufficiently high level of reliability and sufficiently low latency to be able to support critical applications. This may be associated with cloud robotics.
- Passengers traveling in a high-speed train are able to utilize the travel time for leisure or business activities while enjoying a user experience of the same quality as when they are either stationary or moving at a much slower speed.
- Large outdoor events held for a limited period in a defined area may be attended by a significant number of people. Such events include sports tournaments, exhibitions, concerts, festivals, fireworks displays and so on.
- A system that is able to communicate to and from massive numbers of geographically dispersed devices. Such a system can sense data, analyze it, make decisions, and control actuation – providing surveillance, for example, or implementing distributed feedback control and monitoring critical components, and so on.
- Media on demand supports an individual user's desire to be able to enjoy media content (such as audio and video) anytime and anywhere.
- Remote medical examination and surgery enables very low latency for telehaptic control so the surgeon gets tactile feedback that is designed to be indistinguishable from or better than manual operative techniques.

– Shopping malls can allow delivery of personalized shopping experiences.
– Smart city networks include remote monitoring of city infrastructure, real-time traffic information and public safety alerts for improved emergency response times.
– Stadium networks can offer audiences a blend of physical and virtual experiences during concerts and sporting events, and allow crowd sourcing through the sharing of personal points of view.
– Teleprotection in a smart grid network is the ability to react to rapid changes in the supply or usage of resources (such as electricity, water and gas) to avoid transient system failures that can damage equipment or cause customers the inconvenience of power outages.
– Traffic jam enables motorists or passengers to use travel time profitably for leisure or business activities, with the same level of experience they enjoy at home or at work.
– Virtual and augmented reality enable users to interact with one another as if they are in the same location. While virtual reality completely replaces a user's audio and visual sensory experience, augmented reality enriches it by providing additional information that is relevant to the surrounding environment.
– Broadband to the home bringing fixed wireless access (FWA) to a household by using cellular technologies the over last mile, while a router usually provides indoor access.

Even though 5G systems will have to address a wide range of use cases as illustrated above, in some of these, the requirements can be met by simply extending the 4G technical solutions already available. A detailed explanation of the requirements can be found in [3-7].

A. 5G Services

The 5G use cases can be classified in terms of requirements for three essential types of communication with vastly different objectives (Figure 1): massive machine type communication (mMTC), critical MTC, and extreme or enhanced mobile broadband (eMBB). The three types that can be also designed as 5G services are discussed in the following.

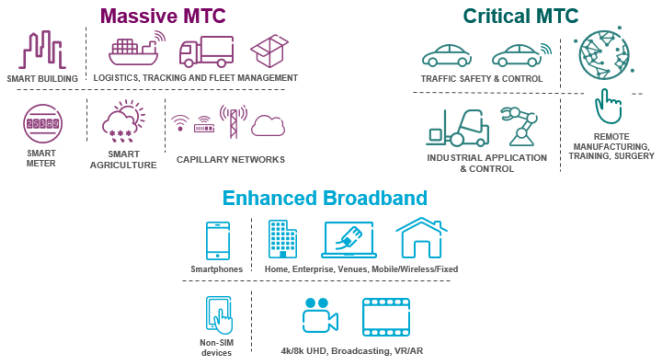


Figure 1: Use case drivers for 5G

i. Massive machine type communication

Otherwise known as Massive IoT, mMTC is designed to provide wide area coverage and deep penetration for hundreds of thousands of devices per square kilometer of coverage. An additional objective of mMTC is to provide ubiquitous connectivity with relatively low software and hardware complexity and low-energy operation. Many of the devices supported are battery powered or driven by alternative energy supplies, have small payloads, and might rarely be active, so they tend to be relatively delay tolerant for the most part. While the devices typically have a long lifespan, services and software need to scale and be swapped out relatively quickly to address new business opportunities. Examples that fall into this service category include the monitoring and automation of buildings and infrastructure, smart agriculture, logistics, tracking and fleet management.

ii. Critical MTC or URLLC

The second category of application being addressed is that of cMTC, which is also called Critical IoT. In this type of application, monitoring and control occur in real time, E2E latency requirements are very low (at millisecond levels), and the need for reliability is great. The performance objectives of cMTC will be applied to workflows such as the automation of energy distribution in a smart grid, in industrial process control and sensor networking where there are stringent requirements in terms of reliability and low latency at the application layer. These are sometimes referred to as ultra-reliable low-latency communications (URLLC) requirements. Careful attention will need to be paid to security in the case of both mMTC and cMTC. While higher network and device complexity is more readily acceptable in critical communication, mMTC will have to address cyber-security assurance with low-complexity devices. A hierarchical approach to the network is necessary to progressively improve security so end-to-end security assurance can be guaranteed.

iii. Extreme mobile broadband

Providing both extreme high data-rate and low latency communications, extreme mobile broadband (eMBB) [3] also offers extreme coverage – well beyond that provided by 4G. Connectivity and bandwidth are more uniform over the coverage area, and performance degrades gradually as the number of users increases.

III. Main 5G components

The 5G system will imply major changes in the implementation and deployment of networking infrastructure, based on software-defined networking (SDN) and network functions virtualization (NFV). Network operations and services are becoming cloud-enabled in almost every industry, and the telecommunications industry is no exception – though it is distinct from other industries owing to the distributed nature of network operations. This creates an obvious opportunity to generate value from distributed storage and cloud computing towards specific clients and services as well. The main domains of the 5G system are wireless access, transport, cloud, applications, and management including orchestration. We outline below how these will evolve towards a full-fledged 5G system (also exemplified in Figure 2).

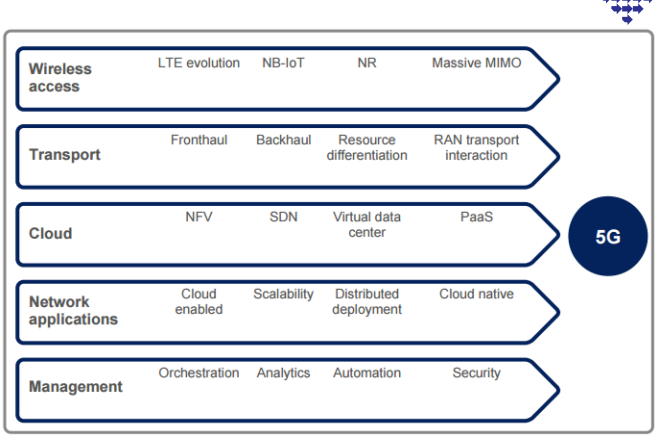


Figure 2: The 5G main components and their evolution

A. *Wireless Access*

One key component of 5G radio access is an innovative air interface called New Radio (NR), which is designed primarily for new spectrum bands. In industry and academia it is generally understood that the success of 5G will depend on a diversity of spectrum assets which span low, medium and high spectrum bands. During discussions in WRC-15 [8] emphasis has generally been placed on high spectrum bands such as millimeter wave bands, although many administrations also realize that low bands below 6GHz will be key to providing the necessary coverage and bandwidth. LTE will of course continue to evolve, including advancements such as LTE-M and narrowband IoT (NB-IoT), and will be an important part of the overall 5G wireless access solution. Many administrations seem to equate 5G with bands above 24GHz. This is the case in the WRC-15 vision for IMT-2020, and for the FCC which has expressed an intent to release the 28GHz and 39GHz bands. NR is expected to migrate to bands below 6GHz in the near term, eventually occupying existing mobile bands below 3GHz.

Key technology components for the 5G radio access solution include:

- Advanced multi-antenna technologies such as massive MIMO and beamforming with phased antenna arrays
- Ultra-lean transmission to reduce interference caused by common signalling resources and to maximize resource efficiency
- Flexible duplex in certain isolated local network deployments
- Access/backhaul integration, where access and (wireless) backhaul share the same technology and the same overall spectrum pool
- Well-integrated device-to-device communication

B. *Transport*

The transport domain delivers connectivity between remote sites and equipment/devices. Backhaul serves both ends of the transmission – for example, to connect a base station (BS) to an access network or a central office – while fronthaul is a term used when the BS antennas are connected to a remote integrated radio frequency (RF) unit, or to a centrally located baseband (BB) unit. In addition to providing bulk connectivity for the operator's mobile network fronthaul and backhaul, the transport domain may offer different types of customer facing connectivity services, such as a Layer 2 or Layer 3 VPN.

5G RAN technology puts new requirements on the bandwidth and latency of transport networks. Consequently, a high degree of automation and coordination within and cross network domains will be required. A concept known as RAN transport interaction (RTI) introduces coordination between the radio, transport and packet core layers of an operator's mobile network, providing network-wide optimization and service assurance.

C. *Cloud*

Network functions (as well as other types of applications) in 5G will increasingly be deployed as virtualized software instances running in data centers. This pattern of deployment, which has been characterized as cloud deployed SDN/NFV, simplifies scaling and management of network infrastructure such as deep packet inspection engines and firewalls. SDN is about the separation of the network control traffic (control plane) and the user specific traffic (data plane). SDN is based on the centralization of configuration and control, while ensuring a simple data plane architecture. NFV is about virtualizing network functions (by implementing them in software) and the functions that can run on a range of standard hardware.

The cloud allows infrastructure to scale in or out and automatically; in other words, when an application needs more resources, the cloud automatically spins up another instance of that application, and removes an instance when load decreases. Such flexible scaling is impossible to achieve when the application is implemented with dedicated hardware. Data security in a virtualized cloud environment will ensure that only authorized access is allowed to the infrastructure application's data store. In addition to this, the infrastructure application may be deployed in a virtual data center (DC) that is distributed between many physical data centers. A VDC is a collection of virtual machines, virtual network connectivity and associated storage that regards the infrastructure applications as a data center. One way to simplify provisioning and control of an application across a VDC will be to define a network slice as a virtual network and let the owner of the slice manage it themselves, within constraints placed by the network provider. The cloud will offer an increasing number of comprehensive platforms as a service (PaaS) to make it easy to develop new applications.

D. *Network Applications*

Network applications such as Evolved Packet Core (EPC), voice over LTE (VoLTE), and future 5G core network functions will be cloud enabled: that is, they will have the ability to execute in the SDN/NFV cloud environment. Consequently, the applications will have the advantage of being automatically scalable as well as flexible in terms of where in the network they can be deployed (centrally, distributed or a combination of the two).

For example, the complete core network can be deployed in a local server in a factory to support exceptionally short response times. At the same time, it should be possible to support the factory with communication services from a centrally placed VoLTE installation, for example.

Another example is the case of media distribution, where the media delivery may be optimized for bandwidth, latency and cost by deploying a content distribution network very close to the edge. In this way, customers can experience

virtual reality and augmented reality productions within latency and bandwidth constraints.

New applications are increasingly designed to be cloud native. Instead of designing applications with integral aspects and functions, applications rather use services offered by the cloud PaaS.

E. Management

Network management of entities in 5G systems will be able to automate and orchestrate a range of lifecycle management processes, and will be capable of coordinating complex dynamic systems of applications, cloud, transport and access resources.

Network management in 5G systems requires additional work to include VNFs deployed in cloud data centers. In cloud-deployed systems, orchestration is needed to arrange and coordinate automated tasks and allocated resources through centralized management. The result is a workflow to provide the desired network behavior. Management entities evolve from ordering explicit configurations (configuring a router or a server, for example) to distributing policies, KPIs and target goals that each subsystem optimizes autonomously and locally.

Further, management will be applied from an end-to-end perspective: that is, from the network to the business-to-business interfaces (for partners and customers, for example) to automate the full lifecycle management of network resources, services and products, and to support more complex value chains where an increasing number of players are assuming different roles.

Finally, it should be noted that analysis and security are essential functions that can be considered part of 5G network management.

Analytics is a key tool for increasing automation of operations by providing prediction insights that can be applied automatically.

Security and privacy in 5G networks will be characterized by new trust and service delivery models, an evolved threat landscape, and increased privacy concerns. In particular, 5G networks will have to manage the following key pillars: security assurance, identity management, radio network security, flexible and scalable security architecture, energy efficient security and cloud security.

IV. THE 5G SYSTEM

The 5G system, which is shown in Figure 3, will be built on “flexible” radio access nodes, distributed and centralized data centers allowing for flexible allocation of workloads. These nodes and data centers are connected via programmable transport networks. The transport networks are connected via backbone nodes that carry the information from the access nodes to the data centers where most of the data is stored and the network is managed. Figure 2 illustrates that all applications, including many network applications, are run on top of a cloud with exception of dedicated functions in the access nodes. The applications can be centralized (App 3 and App 4) or distributed (App 1, App 2), depending on the requirements.

In addition to this, the management of applications, cloud, transport and access resources are shown centrally in the data center but can of course also be flexibly allocated as necessary.

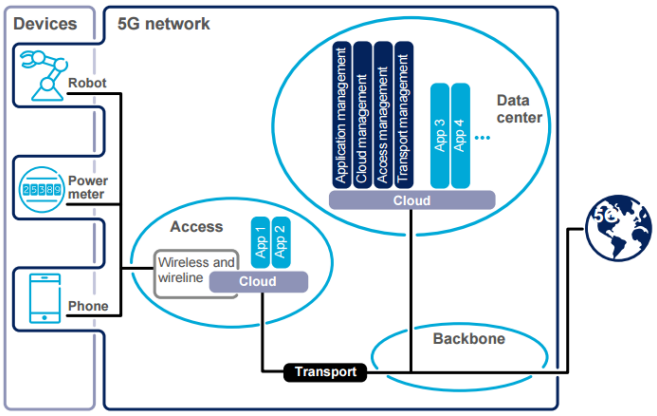


Figure 3: The 5G system

The 5G system will fully support the concept of network programmability for all types of services. A service can be flexibly allocated anywhere in the network, at a network node, end-user device or external host. A service may not be confined to an operator’s network, and may originate from outside the network domain.

E2E orchestration is needed to match external business offerings with network efficiency. For example, to optimize content delivery in eMBB service, orchestration would place virtualized network functions on resources that are physically close to the subscriber.

A. Network Slicing

The technique of network slicing allows for the definition of multiple logical networks (or slices) on top of the same physical infrastructure. Resources can be dedicated exclusively to a single slice or shared between different slices. There are different types of resources such as computing, storage, access equipment, transport, VNFs, and so on.

A network slice is built to address a desired behaviour from the network. Such behaviour can be associated with security, data-flow isolation, quality of service, reliability, independent charging and so on. A network slice may support one or many services, and can be used to create a virtual operator network and may provide customized service characteristics. Network slicing can be used for several purposes: a complete private network, a copy of a public network to test a new service, or a dedicated network for a specific service.

For instance, when setting up a private network in the form of a network slice that can be an end-to-end virtually isolated part of the public network, the network exposes a set of capabilities in terms of bandwidth, latency, availability and so on. Thereafter, a newly created slice can be locally managed by the slice owner who will perceive the network slice as his or her own network complete with transport nodes, processing and storage. The resources allocated to a slice can be a mix of centrally located and distributed resources. The slice owner can initiate applications from his or her management center, and applications will simply execute and store data, either centrally, in a distributed management system or a combination of both.

B. *An Example of a 5G System: An Architecture That Can Be Adapted to Services*

The support for the wide range of 5G services will dictate a flexible 5G architecture for the access and core networks. In particular, a software-configurable purpose built architecture [9], [10] and [11] with flexible deployment alternatives will be needed to provide the required overall cost efficiency.

To illustrate the flexibility of the 5G system architecture, the realization of three use cases will be considered, each corresponding to a different 5G service. The first, massive numbers of geographically dispersed devices requires the mMTC (Massive IoT) service. The second is virtual reality, and will use the 5G eMBB service. The third is factory automation, and this is realized by the cMTC (Critical IoT) service. The deployment architecture corresponding to these cases is shown in Figure 3, realized here by separate network slices supporting each service. Network slicing provides multiple benefits including the possibility to optimize the functional deployment and the network function configuration. It is also beneficial for independent operations and lifecycle management of each network slice.

In the following, we will explain the main architectural components of each case. It is important to note that several intermediate nodes (at regional sites, for example) may exist between the access and the primary data center site, but they have been omitted for the sake of simplicity. Further, the radio access technology functionality is divided between the antenna location (RF part) and BS site (BB part), representing the split architecture in 5G RAN [11].

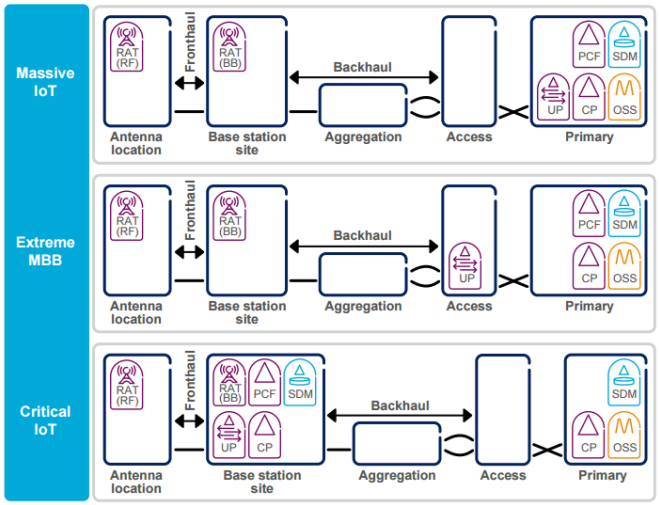


Figure 4: The 5G adaptable architecture

i. *Massive Number of Geographically Dispersed Devices*

A generic use case, the massive number of geographically dispersed devices falls under the mMTC service. It may be a question of devices connected to parking meters in a city, or asset tracking in an industrial site, for example. Most of these devices are characterized by low cost/ complexity (half duplex, low power, single antenna), long battery life (more than 10 years) and have significantly improved coverage (a 15-20dB better link margin than LTE). They are mostly static and largely generate traffic on the uplink. Recently, NB-IoT was finalized by the 3GPP in 2016, and it addresses most of these requirements. The basic architecture for mMTC looks simple. The main challenges arise from the very large number of devices to be supported, leading to a substantial increase in the control signaling relative to the user plane traffic. In addition, the mobility tracking can further increase the burden on the network. From the top of Figure 4, it can be seen that the radio access is executed at the base station close to the devices, while the other main functional components such as the control plane (CP) that also includes the mobility management, subscriber data management (SDM), and the user plane (UP) are conducted in the central primary site. From a business perspective, it is recommended that mMTC is separated from the eMBB network instance in order to simplify the subscription management and Business Support System (BSS) due to different business and go-to-market models. The main technology techniques required to provide an mMTC service are Extended DRX (to extend the battery life), time repetition (to improve the coverage), enterprise managed devices (identity management outside the network/operator control), and E2E security for payload data.

ii. *Virtual and Augmented Reality (From An Entertainment Perspective)*

The high data capacity and low latency requirements of virtual reality will require a separation of the control and user data plane where the user plane is being distributed closer to the user (for example, the UP is placed in the access site while the CP is kept in the primary data center), as illustrated in the middle of Figure 4. This will allow to optimize the access to applications in terms of capacity and latency, assuming service applications are distributed as well. The other functions such as SDM, operations support systems (OSS) and policy control function (PCF) will be executed in the primary data center. The main characteristics of eMBB such as high data capacity can be achieved, for example, using advanced multi-antenna technologies (MIMO and beamforming) as well as distribution of the optimized UP of the core network.

iii. *Factory Automation*

The factory automation use case requires cMTC services. The most stringent requirements are very low latency and high reliability since jitter is not tolerated for precise operation such as the cell automation in a factory. In practical terms, one of the most significant challenges will be to support cMTC business services where high-grade network slices need to provide the required levels of availability, robustness and resilience to attacks.

The ultra-low latency for the cMTC service will have implications for the 5G architecture functions. In particular, there will be a need to:

- Push application processing to the mobile edge
- Or potentially have local deployment – for example, local break-out in the factory where parts of the core network such as the PCF, UP, CP and SDM are placed or duplicated to support standalone system operation
- Provide a robust radio perimeter security.

An example of the high-level architecture of the cMTC service is shown at the bottom of Figure 4, where the UP and CP have been placed on the BS site along with a “duplication” of some the core functions such the PCF and SDM.

The main technology components that allow the low latency and high reliability requirements to be met are high

frequency or space diversity, a very short transmission timeframe, and distributed processing. Further, with regard to security, non-SIM-based authentication (AAA) and enterprise managed devices (identity management outside the network or beyond the operator's control) are envisaged.

V. CONCLUSION

With connectivity at the heart of industry transformation, 5G systems have a significant role to play – not just in the evolution of communication but in the evolution of businesses and society as a whole. 5G will build on and extend the public network, making it viable for any type of applications. Consequently, 5G will be the major enabler of the Internet of Things and the Networked Society. As a natural evolution of current network architecture, broken up into building blocks through access, transport, cloud (including SDN and NFV), network applications and management (including orchestration and automation), 5G systems will provide a higher level of abstraction that will simplify the management. The 5G architecture will not only be cost-efficient to operate, it will have the agile and flexible mechanisms in place for the swift introduction of services. These properties are required to enable new business models that can rapidly generate new revenue opportunities. For that reason, 5G systems will be built in the form of programmable platforms that provide functionality on an "as-a-service" basis. Network slices are key to delivering differentiated offerings, as they can provide a complete solution environment that is adapted for specific application usage – and they do this in a way that uses network resources efficiently. The 5G transformation has already started with NB-IoT, NFV and management automation, for example. It is an incremental process, enhancing the current network in a step-by-step fashion. As the process unfolds, global partnerships will prove essential to enabling a cross-industry engagement in defining and building the 5G system.

ACKNOWLEDGMENTS

I'd like to express my special thanks to my colleagues at Ericsson Research and at Ericsson Network Society Lab for their support and the creation of the 5G Systems: Enabling the Transformation of Industry and Society white paper [12] which is the source of this paper.

REFERENCES

[1] Ericsson, NUMBER THEORIES: WHAT 100 OPERATORS REALLY THINK ABOUT 5G, Ericsson Business Review, no. 1, 2016, https://www.ericsson.com/thecompany/our_publications/ericsson_business_review/issue1_2016/what-100-operators-really-think-about-5g

[2] Ericsson, "Opportunities in 5G: The View from Eight Industries", 2016, https://app-eu. clickdimensions.com/blob/ericssoncom-ar0ma/files/5g_industry_survey_report_final.pdf

[3] Afif Osseiran, Jose F. Monserrat and Patrick Marsch, 5G Mobile and Wireless Communications Technology, Cambridge University Press, 2016

[4] ICT-317669 METIS project, "Scenarios, requirements and KPIs for 5G mobile and wireless system," Deliverable D1.1, April 2013, https://www.metis2020.com/wp-content/uploads/deliverables/METIS_D1.1_v1.pdf

[5] ICT-317669 METIS project, "Updated scenarios, requirements and KPIs for 5G mobile and wireless system with recommendations for future investigations," Deliverable D1.5, April 2015, https://www.metis2020.com/wp-content/uploads/deliverables/METIS_D1.5_v1.pdf

[6] NGMN Alliance, "NGMN 5G White paper," February 2015, www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf

[7] 3GPP TR 22.862 V2.0.0, "Feasibility Study on New Services and Markets Technology Enablers Critical Communications; Stage 1," Technical Report, TR 22.862 V2.0.0, Technical Specification Group GSM/EDGE Radio Access Network, June 2016.

[8] International Telecommunications Union Radiocommunication Sector (ITU-R), "Framework and overall objectives of the future development of IMT for 2020 and beyond," Recommendation ITU-R M.2083, September 2015, www.itu.int/rec/R-REC-M.2083

[9] Lars Frid et al., "A vision of the 5G Core," Ericsson Technology Review, vol. 93 no. 2, 2016, http://www.ericsson.com/res/thecompany/docs/publications/ericsson_review/2016/etr-5G-corevision.pdf

[10] Peter Öhlén et al., "FLEXIBILITY IN 5G TRANSPORT NETWORKS," Ericsson Technology Review, vol. 92 no. 8, 2015, http://www.ericsson.com/res/thecompany/docs/publications/ericsson_review/2015/etr-5g-transport-networks.pdf

[11] Erik Westerberg, "4G/5G RAN ARCHITECTURE: HOW A SPLIT CAN MAKE THE DIFFERENCE," Ericsson Technology Review, vol. 93 no. 6, June 2016, https://www.ericsson.com/thecompany/our_publications/ericsson_technology_review/archive/4g-5g-ran-architecture-how-a-split-makesa-difference

[12] Ericsson, "5G systems: Enabling the Transformation of Industry and Society", 2017, https://www.ericsson.com/res/docs/whitepapers/wp-5g-systems.pdf

László Szilágyi (MsC, Electrical Engineering) works as the Innovation Program Manager of Ericsson Hungary formulating and driving projects aiming to reveal business potential in IoT and 5G. In Ericsson Garage in Budapest companies, universities, network operators and Ericsson can work together in a lean startup fashion to validate new use cases based on novel technologies in a very iterative and agile fashion. One of his projects targets edge computing, where in collaboration with ELTE (Eötvös Loránd University) various service enablers are implemented and tested in such distributed computing environment. He's also driving the NB-IoT pilot with a major Hungarian telecom operator with the involvement of the local tech ecosystem to reveal cellular LPWAN use cases and evangelise the technology.

[i] Presenter of 5G Systems: Enabling the Transformation of Industry and Society Ericsson white paper [12].

5G Use Cases, Requirements and Radio Network Evolution

Vladimir Petrić, Nokia

Abstract — This article provides brief insight in use cases and requirements driving development and standardization of next generation wireless networks. Overview of key technology components and architecture evolution being adopted by 5G to achieve desired network performance will be also shown.

Keywords — 3GPP, 5G, LTE, Radio network, IoT (Internet of Things), Spectrum, MIMO, Cloud

I. INTRODUCTION

5G is one of the most important technological shifts that will drive a fundamental change in our communications infrastructure.

With subscriber penetration peaking, 5G comes at a time when many operators are being forced to diversify and expand beyond their traditional business of connecting consumers.

At the same time, many other industries are also facing fundamental disruptions that demand they transform their underlying business model. From media and entertainment to manufacturing and transportation, companies must find new ways of working and increase their performance. Many face intense and growing competitive pressure in dynamic markets where the lifecycle of new products and service introductions is constantly shrinking.

5G has the potential to help operators and other companies meet their ambitions.

The biggest difference between 5G and legacy design requirements is the diversity of use-cases that 5G networks must support compared to today's networks that were designed primarily to deliver initially voice and later high speed mobile broadband to the humans.

5G targets are illustrated in Figure 1.

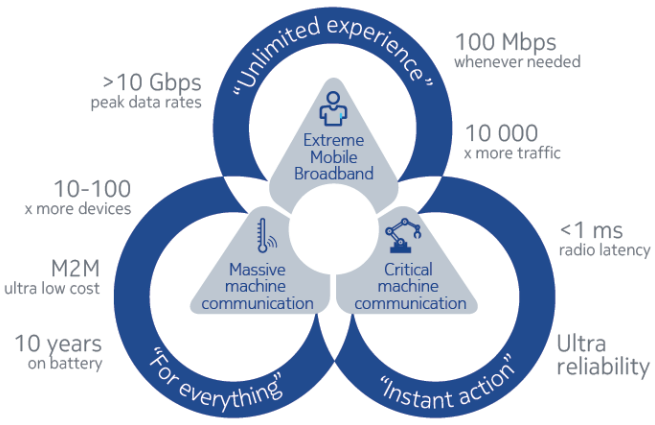


Figure 1: Heterogeneous use cases – diverse requirements

5G will be about people and things that can be broadly split into three use-case categories:

– Massive broadband that delivers gigabytes of bandwidth on demand
– Massive machine-type communication (MTC) that connects billions of sensors and machines
– Critical machine-type communication (MTC) that demands immediate, synchronized eye-to-hand feedback to remotely control robots and deliver the tactile Internet

II. USE CASES

So far, the mobile networks have mainly provided connectivity for the smartphones, tablets and laptops. 5G will take the traditional mobile broadband to the extreme in terms of data rates, capacity and availability. Additionally, 5G will enable further capabilities including massive Internet of Things (IoT) connectivity and critical communication.

There have been a number of initiatives by various international organizations, standardization bodies and industry alliances to define the requirements for further development of next generation wireless communication networks. ITU issued the Recommendation that defines the framework and overall objectives of the future development of International Mobile Telecommunications (IMT) for 2020 and beyond in light of the roles that IMT could play to better serve the needs of the networked society [1]. Operators created NGMN (Next Generation Mobile Networks) Alliance and issued white paper with 5G targets [2]. There is also European project 5G-PPP (5G Infrastructure Public Private Partnership) which is a joint initiative between European industry and European Commission. 5G-PPP has created general 5G architecture and target documents [3].

The future of mobile communications is likely to be very different to that which we are used to today. While demand for mobile broadband will continue to increase, largely driven by ultra-high definition video and better screens, we are already seeing the growing impact of the human possibilities of technology as the things around us become ever more connected. Objects ranging from cars and factory machines, appliances to watches and apparel, will learn and organize themselves to fulfil our needs by automatically adapting to our behaviour, environment or business processes.

New uses will arise, many not yet conceived, creating novel requirements that communications networks must be able to meet flexibly and cost effectively in order to support operator profitability and the wider ecosystem. The way

– how we travel and experience our environment (real world mobility)
– how we can control remote environments (virtual mobility)

– how the infrastructure around supports us (high performance infrastructure)
– how we produce goods (4th industrial revolution)

will completely change.

As a result, this creates a highly dynamic and innovative environment. This chapter summarizes possible used cases that are most likely to be supported by initial 5G networks. However, technology revolution will create virtually unlimited possibilities and additional use cases and applications will emerge in the future.

A. *Mobile broadband*

Mobile broadband is the key use case today and it is expected to continue to be one of the key use cases driving the requirements for 5G. It goes far beyond basic mobile Internet access and covers rich interactive work, media and entertainment applications in the cloud or reality augmentations.

The main drivers for the increased traffic volume are the increase in size of content and the number of applications requiring high data rates. Factors include increases in camera resolution, the rise in screen resolution with the recent introduction of 4K (8K is already expected beyond 2020) and the developments in 3D video. Streaming services (audio & video), interactive video and mobile Internet connectivity will continue to be used more broadly as more devices connect to the Internet. Another very interesting but also very demanding use case is augmented reality for entertainment and information retrieval, which requires very low latencies and significant instant data volumes.

B. *Automotive*

The automotive sector is expected to be a very important new driver for 5G, with many use cases for mobile communications for vehicles.

For example, entertainment for passengers requires simultaneous high capacity and high mobility mobile broadband or augmented reality dashboards displaying overlay information on top of what a driver is seeing through the front window, identifying objects in the dark and telling the driver about the distances and movements of the objects.

The previous two use cases are related to content provisioning for the car users, but the cars themselves will also be also connected. Many car manufacturers are already adding driver assistance systems based on 3D imaging and built-in sensors. In the future, wireless modules will enable communication between vehicles themselves, information exchange between vehicles and supporting infrastructure and between vehicles and other connected devices, for example, those carried by pedestrians.

The next phase will be remotely controlled or even self-driven vehicles, which will require ultra-reliable and very fast communication between different self-driving cars and between cars and infrastructure. In a plausible future, a self-driving car takes care of all driving activity, allowing the driver to rest and concentrate only on traffic anomalies that the car itself cannot identify.

C. *Smart Society*

Smart cities and smart homes, often referred to as smart society, will be embedded with dense wireless sensor networks. Distributed networks of intelligent sensors will enable cost- and energy-efficient maintenance of the city or home. Many of these sensors are typically low data rate, low power and low cost, but for example, real time HD video may be required in some types of devices for surveillance. The task for 5G will be to integrate the management of these very diverse connected devices.

D. *Smart grids*

The consumption and distribution of energy, including heat or gas, is becoming highly decentralized, creating the need for automated control of a very distributed sensor network. A smart grid interconnects such sensors, using digital information and communications technology to gather and act on information. This information can include the behaviours of suppliers and consumers, allowing the smart grid to improve the efficiency, reliability, economics and sustainability of the production and distribution of fuels such as electricity in an automated fashion.

E. *Health*

The health sector has many applications that can benefit from mobile communications. Communications systems enable telemedicine, which provides clinical health care at a distance. It helps eliminate distance barriers and can improve access to medical services that would often not be consistently available in all areas. It is also used to save lives in critical care and emergency situations.

F. *Industrial*

Wireless and mobile communications are becoming increasingly important for industrial application. Wires are expensive to install and maintain and the possibility of replacing cables with reconfigurable wireless links is a tempting opportunity for many industries. However, achieving this requires that the wireless connection works with a similar delay, reliability and capacity as cables and that its management is simplified. Low delays and very low error probabilities are new requirements that will be addressed with 5G.

III. REQUIREMENTS

Diverse use case, described in previous chapter, lead to set of requirements future 5G system should meet.

Enormous growth in radio network capacity will be a must. It is expected 10,000 times more traffic will need to be carried through all mobile broadband technologies at some point between 2020 and 2030.

Peak data rates of a 5G system will be higher than 10 Gbps. Even more importantly, the cell-edge data rate (for 95% of users) should be at least 100 Mbit/s, which will allow the use of the mobile Internet as a reliable replacement for cable wherever needed.

Latency target of 1ms, ten times less compared to current LTE networks, will have to be met to satisfy new use cases such as automotive safety, the tactile Internet or real time control.

A battery life of 10 years will be required for IoT devices. Also, reduced power consumption and increased battery life will also be very important for more complex devices, such as smartphones, tablets or laptops. Part of this lifetime extension will come from the evolution of battery technology

but part will come from efficient handling of user traffic in the 5G system.

The possibility to handle devices with very low cost has to be ensured, especially for IoT devices. 5G will need to be flexible enough to handle efficiently very simple devices that only send small, rare bursts of data, but also handle advanced ones that send large amounts of data quickly.

Accurate positioning of the device shall also be possible with 5G, indoors as well as outdoors. Location-based services are becoming more important and will be followed by location-based reality augmentations.

Finally, security will be a very important requirement for 5G and the trend is already visible and addressed now. In the new system, not only security of sensitive personal data, but also safety from inserting false information to the system should be ensured, with procedures made as simple as possible.

IV. TECHNOLOGY COMPONENTS

High and diverse targets to be met by 5G networks will lead to a number of new technologies being adopted in the future radio networks. Concepts currently being used or just being introduced in existing mobile networks, mainly LTE, will be more widely adopted, while also new technological solution will be developed for 5G. The main new technology components are shown in Figure 2.

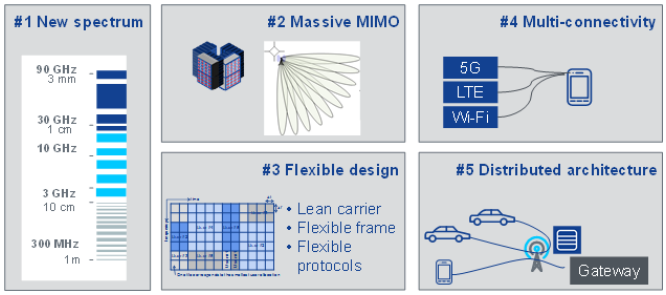


Figure 2: Key 5G technology components

A. *New spectrum*

The very high data rates, over 10Gbps and even up to 20 Gbps, require bandwidth up to 1 GHz which is available at higher frequency bands. 5G is the first radio technology that is designed to operate on any frequency bands between 450 MHz and 90 GHz. The low bands are needed for wider coverage and the high bands for high data rates and capacity.

Dialogue between interested parties is ongoing with the aim to define spectrum to be used by 5G. Lower bands, such as Band 28 (700 MHz) is being proposed by many European operators. Also, Band 42/43 (3.4-3.8GHz) is being identified as 5G band in Europe. 3.5GHz and 4.5GHz are being considered for Japan, China and Korea markets. In higher spectrum, European operators are proposing 24GHz band, while 28GHz and 39GHz spectrum are already planned for initial pre-standard 5G trials in US and Korea. Japanese operators are even considering parts of the spectrum above 70MHz.

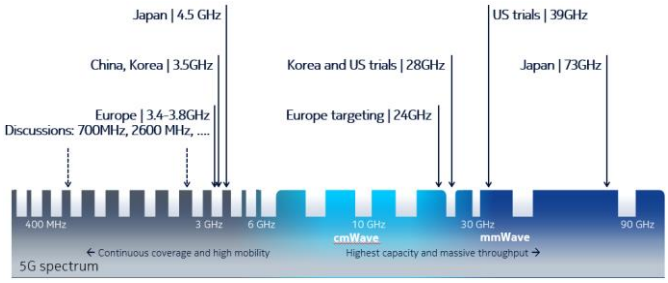


Figure 3: 5G frequency bands

It should be also noted that agenda item for WRC 2019 will be to identify spectrum for IMT2020. Ongoing studies will focus on following bands:

– 24.25–27.5 GHz
– 37–40.5 GHz
– 42.5–43.5 GHz
– 45.5–47 GHz
– 47.2–50.2 GHz
– 50.4–52.6 GHz
– 66–76 GHz
– 81–86 GHz

B. *Massive MIMO*

Spectrum is the key asset for the mobile operators, and it tends to be highly expensive. Thus, there is a clear motivation for improving spectral efficiency to provide more capacity within limited spectrum resources. The spectral efficiency can be improved mainly by two solutions: more efficient inter-cell interference mitigation and more efficient beamforming antennas.

Massive MIMO with beamforming can increase the spectral efficiency and network coverage substantially. Some calculations show that 5G with beamforming at 3.5 GHz will be able to provide spectral efficiency higher than 10 bps/Hz/cell, which is an excellent starting point for providing high capacities and high data rates.

Beamforming comes more practical at higher frequencies because the antenna size is relative to the wavelength. In practice, massive MIMO can be utilized at frequencies above 2 GHz in the base stations and at millimetre waves even in the devices.

User specific beamforming was not supported by 3GPP Release 8/9 LTE devices, but was only included in Release 10 for 8 transmit antennas and was further enhanced in Release 13/14. Beamforming has not been widely utilized so far in commercial LTE networks because there was no urgent capacity need, there was no device support and the active antenna implementation was not commercially feasible.

All these factors are changing now and beamforming is actually making it to commercial networks. Massive MIMO will be part of 5G from day one, with at least 64TX on BTS side. This will also help avoiding any legacy device problems, currently present in LTE networks.

C. *Flexible air interface design*

Unlike LTE, which initially introduced fixed radio interface structure and protocols, 5G is to introduce flexibility in different areas, aiming to improve network efficiency and minimize latency.

For example, in LTE each cell must transmit Reference signals (RS) four times every millisecond even if there are no

data transmission or any connected users. Reference signals make typically 10% of the base station maximum transmission power in the case of 2x2MIMO, and even more with 4x4MIMO leading to high reference signal overhead. The target in 5G is to make the reference signal design more flexible so that lower transmission frequency can be utilized dynamically in the case of no or low loading. This approach where the unnecessary common channel transmissions are minimized is called lean carrier. It brings number of benefits, such as lower interference, lower power consumption and better support for user specific beamforming.

With the aim to further increase 5G system capacity, 3GPP is also studying the option of 'Flexible Duplex' which aims to make TDD more adaptive and dynamic and provide convergence between FDD and TDD, finally allowing the transmission direction to be adjusted dynamically according to instantaneous traffic variations. It will enable different cells in the network employing different uplink-downlink splits based on the traffic load for their cell.

On the other side, lower latency is another important factor in improving end user performance in addition to the higher data rates. The target in 5G radio is to provide a sub-1 millisecond round trip time. This is a challenging target, knowing that High Speed Packet Access (HSPA) networks can provide 20 ms latency in the best case and the current LTE networks typically provide 10 ms latency.

Air interface delay is directly proportional to TTI (Transmission Time Interval). Thus, shortening the TTI by a short frame duration and an adaptive frame structure is the most promising approach when seeking to reduce air interface latency. 5G specification is to include flexible frame structure, where every sub-frame can be dynamically selected to carry UL or DL data and control signals present in every sub-frame for low latency scheduling.

Another delay component that need to be addressed in 5G radio is control plane latency. In LTE, transition from Idle to Connected state, or sending capacity request for uplink transmission when already in RRC Connected state can take dozens of milliseconds. 5G considers concepts such as connected inactive solution and contention based solution that can provide substantially lower latency for the first packets to be sent.

D. Multi-connectivity

While 5G can be deployed as a standalone system, in most cases 5G will be deployed together with LTE. The 5G device will support simultaneous connections to 5G and LTE.

Multi-connectivity supports the smooth introduction of 5G on top of LTE networks and enables 4G/5G real-time radio resource management with dynamic inter-RAT load balancing to maximize output. The technology also provides seamless mobility by eliminating handover interruption delays and errors, and optimizes capacity, coverage and mobility for devices connected in a heterogeneous network.

Multi-connectivity with other technologies, such as Wi-Fi is also under study.

E. Distributed architecture with cloud flexibility

Final target for 5G is to support deployment as a standalone solution without LTE, using new 5G packet core. A new 5G packet core is designed to support network slicing, flexible QoS and connectionless mechanism.

However, initially 5G will also support non-standalone solution with dual connectivity to LTE utilizing dual connectivity approach and existing Evolved Packet Core (EPC). In this scenario, the 5G radio can have user plane connectivity to EPC either directly or via the LTE eNB and control plane connectivity towards EPC via the LTE eNB.

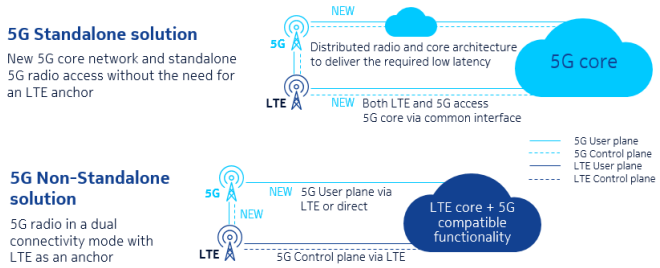


Figure 4: 5G architecture options

Today's mobile networks are built in a way that makes it very hard or even impossible to dedicate parts of them to a specific usage. The same network has to support all thinkable use cases, which in practice means that one size has to fit all.

5G will introduce the concept of network slicing, meaning that the network can be split into slices that are dedicated and optimized for specific purposes. There might, for instance, be a slice optimized for smartphones and tablets taking into account the likelihood of massive content downloading and video streaming. Other network slices could be optimized for critical machine type communication, such as autonomous driving, focusing on the need for ultra-low latency and extreme reliability. Network slices dedicated to specific industries or even individual enterprises could offer operators totally new business opportunities, such as Network-as-a-Service. Efficient implementation of network slicing will be enabled by virtualization and cloud technology.

Considering that highly centralized network architecture that is the norm today will not be able to fulfil 5G latency requirements, it is quite clear the need for ultra-low latency and fast traffic forwarding in 5G will have a profound impact on the architecture. The low latency requires to bring the content close to the radio which leads to local break out or Mobile Edge Computing (MEC). MEC was already demonstrated by Nokia on in existing LTE networks, showing that local content and/or content cashing are examples of how MEC can improve the customer experience and reduce overhead and costs in content downloading and streaming.

Finally, the scalability requires to bring the cloud benefits to the radio networks with edge cloud and local cloud architecture. 5G is expected to support different radio deployment scenarios:

- 5G Cloud BTS, where baseband (BB) processing is split on real time (RT) baseband in dedicated hardware unit on BTS antenna location and non-real time (NRT) baseband in radio cloud;
- 5G Cloud optimized BTS, where baseband (BB) processing is split on real time (RT) baseband (with RT BB and RF/antenna merged into single hardware unit) and non-real time (NRT) baseband in radio cloud;
- 5G classical BTS, following legacy base station design where complete baseband is located on BTS location, close to antenna;

– 5G All in One (AiO) BTS, providing cost and volume/weight optimized BTS with all elements integrated in single compact unit, mainly intended for dense radio deployments, presently known as small cells.

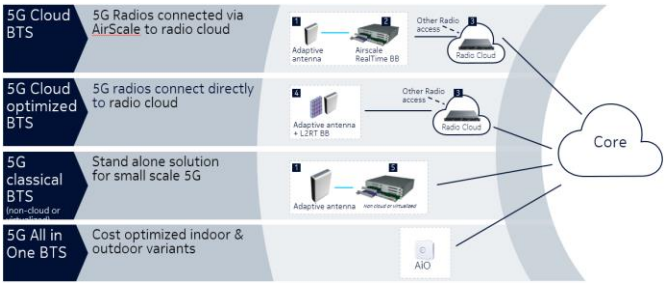


Figure 5: 5G radio access deployment scenarios

V. SUMMARY

5G needs to address the predicted large increase in data traffic and will have to fulfil the capacity, data rate and latency requirements of next-generation devices. 5G is not only a new air interface but the new generation of radio systems and network architecture in which different radios (legacy and new) work together perfectly. Progress has been rapid, with proofs of concept for many of the technological advances that will be a crucial part of the forthcoming 5G standard.

To enable the capacity and data rate requirements for 5G, new spectrum bands are required, along with the massive densification of small cells. The design needs to be flexible enough so that the system could be deployed in bands ranging from 2 GHz up to 80 GHz, supporting set of common features such as dynamic TDD, massive MIMO/beam forming, device-to-device communications and a frame structure with low overhead and shorter frame size. Flexibility is also required to support a wide range of services and requirements, such as extreme reliability for critical communications (for example in vehicle-to-vehicle communications) or very loose reliability, but low cost for Internet of Things applications (for example reports from various sensors). The final challenge will be to combine the vast variety of solutions for the many 5G use cases as well as multiple previous generation network layers into a uniform user experience with unified control of the network operation. Different layers of 5G will be integrated into one system together with other existing radio technologies and their evolution. All of these radio access layers will collaborate tightly with each other to ensure the best user experience.

5G will provide new assets to operators that they will be able to monetize: an entirely new level of network performance, the huge amount of transactional data in the network and dedicated virtual subnetworks that can be instantiated and managed independently from each other.

REFERENCES

[1] Recommendation ITU-R M.2083-0 “IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond” https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf

[2] NGMN 5G White Paper https://www.ngmn.org/fileadmin/ngmn/content/downloads/Technical/2015/NGMN_5G_White_Paper_V1_0.pdf

[3] 5G-PPP, 5G architecture and target documents https://5g-ppp.eu/white-papers/

[4] Nokia White Paper, 5G masterplan https://pages.nokia.com/5g-master-plan.html

[5] Nokia White Paper, 5G use cases and requirements https://pages.nokia.com/GC200010.html

[6] Nokia White Paper, 5G Radio Access System Design Aspects https://pages.nokia.com/GC200009.html

[7] Nokia White Paper, The 5G advantage in real network scenarios https://pages.nokia.com/9285.The.5G.advantage.in.real.network.scenarios.html

Vladimir Petrić graduated from University of Belgrade, School of Electrical Engineering in 2007. He joined then Nokia Siemens Networks in 2008, and currently he takes Sales Solution Manager position in Nokia, being responsible for radio access networks marketing and sales.

5G in smart grids: a use case for deployment and economical aspects

Maja Kernjak-Jager, Tomaž Mohar, Radovan Sernec, Andrej Souvent, EIMV, Slovenija

Abstract – 5G mobile technology is widely regarded also as a solution for M2M/IoT communications. Future smart grids with requirements for dense deployment of end terminals and multiple service types is an interesting fit for 5G, too. Smart grid interest for 5G originates from its capabilities, in particular: native support for dense M2M/IoT networks, low latency of communication, device-to-device communication (D2D), decomposed cloud RAN architecture (RRH-BBU), low power consumption at RRH and reliability. Future smart grids will evolve into fully observable systems, well beyond the smart meter billing service used today, thus increasing the need for information exchange in distribution network. These services include: distributed generation and energy storage monitoring and control, electric vehicle charging, demand response/side management, ancillary services for grid stability (e.g. reactive power regulation), integration with micro/nanogrid islands, system security, planning of future network investments, direct involvement of consumers in their energy usage. 5G may impact also grid features that require most reliable and lowest latency responses, e.g. protection switching. Communication latency requirement of IEC and IEEE standards for smart grid services is also compared to 5G capabilities. We made an empirical case study of requirements for 5G deployment on a real large grid network. Analysis presents specifics of grid network topology characteristics (e.g. density distribution and distance metrics of transformer stations). Economical parameters for deployment are also evaluated. Preliminary results show that much denser transformer station placement offers opportunity for RRH deployment, great coverage, and economic synergies between utility and telecom operators at least on the RRH location sharing level.

Key words – 5G, smart grid, economic analysis, services

Povzetek – Mobilna tehnologija 5G velja tudi za komunikacijsko tehnološko rešitev za M2M/IoT. Prihodnja pametna omrežja z veliko gostoto končnih terminalov so zanimiva za 5G, predvsem zaradi naslednjih zmogljivosti: vgrajena podpora za gosta omrežja M2M/IoT, nizke komunikacijske zakasnitve, komunikacija naprava–naprava, razčlenjena arhitektura antene–bazna enota v oblaku, nizka poraba moči in zanesljivost. Prihodnje storitve v pametnih omrežjih vključujejo: spremljanje porazdeljene proizvodnje in porabe energije, polnjenje električnih vozil, upravljanje odjema, stabilnost omrežja (npr. regulacija jalove moči), integracijo z mikro/nano otočnimi omrežji, varnost sistema, načrtovanje prihodnjih naložb v omrežje, neposredno vključevanje potrošnikov z njihovo porabo energije. Preliminarna empirična študija vključuje značilnosti topologije pametnih omrežij in vključuje ekonomske parametre. Začetni rezultati kažejo, da gosta postavitev transformatorskih postaj ponuja priložnost za postavitev anten, dobro pokritost in ekonomske sinergije med upravljavci pametnih omrežij in telekomunikacijskimi operaterji.

Ključne besede – 5G, pametna omrežja, ekonomska analiza, storitve

I. INTRODUCTION

Smart grids evolution is dependent on communications to the end node/edge device, i.e. near/field area network (NAN/FAN), while much has already been done on wide area network (WAN) fiber coverage between substations and utility (distribution system operator (DSO)) management centres.

Basic requirements for smart grid communications include: secure, reliable, low latency (< 10 ms), higher bandwidths (> 1 Mbps) for some applications, guaranteed transport quality of service and driving towards high density deployments of edge nodes.

5G promises to advance cellular communications for everyday users in terms of high speed access and also enhanced quality of service (QoS) on massive events. Native support for massive numbers of end points per antenna/sector (> 10 K), low communication latency (1–5 ms) and direct device-to-device communication (D2D) are specifically designed in for machine-to-machine/Internet of Things (M2M/IoT) applications [1]. These are of particular interest for smart types of applications and smart grid in particular. Architecture and implementation of 5G cellular network as a decomposed cloud radio access network (C-RAN) with remote radio heads/antennas fiber connected to base band units (RRH/RRA-BBU), its low power consumption at RRH (< 50 W) and increased reliability may prove decisive factors for fast take-up in smart grid domain. The important implication of 5G is that cell sizes will be much smaller compared to 4G, implying much more required RRH locations. This will result in severe physical installation costs. It is our preliminary conjecture that utility TS grid network is much denser (at least on the order of 10x) compared to 4G eNB. It is this existing TS density that offers most promises for physical infrastructure sharing and lower 5G deployment costs.

Fiber connection from RRH to BBU and from BBU to mobile core has a direct analogy in smart grids (Figure 1). It is also possible that 5G can be exploited in D2D mode also for multihop TS-TS (RRH-RRH) for multihop communication, but this is very dependent on radio propagation constrains within 3D micro topology of TS neighborhoods, since D2D is planned to operate in higher GHz bands (> 6 GHz). To realize full potential of C-RAN we must assure fiber connection from RRH/TS to BBU/substation pairs. Some of such infrastructure is already built. All substations are also readily fiber connected to WAN backbone, not incurring additional Capex investment. Analyzing the collocation of RRH and BBU at TS and substation within distribution grid (MV/LV) is the objective of the paper.

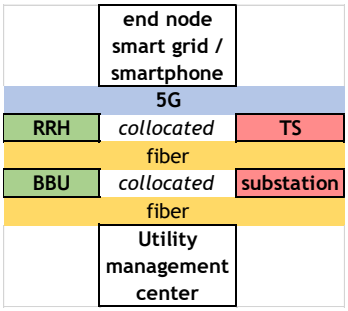


Figure 1: Collocating RRH to TS and BBU to substation with 5G to end nodes.

We claim that telecom operators and utilities must seize the opportunity and make 5G a case of cooperative action for lower cost of deployment and operations, assure wider coverage and common good. Are there any potential cross segment hindrances to be expected between telecom operator and utility? We think not, keeping in mind that core businesses of each are separate and that utilities will have much to work to bring future smart grid services in concerted operations, while telecoms will struggle to retain customer base, while potentially seeking new segments – and smart grid related M2M is opportunity not to be lost.

The following analysis presents the opportunities of sharing the infrastructure from both telecom and utility for each to achieve their specific objectives with lower costs and shorter time to market. EU has recognized the opportunity as well by publishing Directive 2014/61/EU on measures to reduce the cost of deploying high-speed electronic communications networks, while similar publication has been issued by FCC in USA [2], [3].

A. *Utility special requirements*

It must be clearly stated at the beginning that any possible cooperation for mutual benefit of both stakeholders must take into full account the specific requirements utilities have that are very different from types of communications services telecom operators used to offer to wider public (i.e. sporadic high bandwidth smartphone downloaded multimedia). Telecom operators will have to adapt to different communications requirements (e.g. continuous traffic patterns from M2M end nodes) and enforced rigorous SLA.

B. *Use case*

Real time communications are the major component and enabler of end-to-end digitalization of grid infrastructure. New types of devices at the grid edge enable novel applications and services are added to already present smart meters, e.g.: grid monitoring, control and protection (WAMPAC), demand side management (DSM), flexibility nodes, distributed generator sources (DG). Much higher density of utility / smart grid node types demand M2M communications with predefined QoS and high levels of availability. Grid operators have dense installation of poles (carrying overhead electrical cables) and transformer stations (medium-low voltage). This utility infrastructure can be retrofitted with RRH and BBU to offer 5G services. 5G is offered to utility and telecom customers and carries specific traffic for both service segments.

Models of *physical infrastructure sharing ⇔ communication solution* between telecom operator & utility that are objectives of this analysis include:

– physical locations ⇔ RRH & BBU placement
– ducts ⇔ fiber, power cabling
– rights of way ⇔ fiber & RRH placement.

Sharing of active equipment (e.g. fiber WDM splitters, λ, Ethernet switch/routers, radio spectrum, spectrum purchase) is part of ongoing analysis.

II. COMMUNICATION REQUIREMENTS FOR SMART GRIDS

Smart grids communications carry different services each with specific data traffic type: grid monitoring, control, and protection, non-control grid (e.g. asset management), physical safety and security (e.g. video), remote worker access to corporate applications (e.g. maps), NAN backhaul for smart metering, distribution grid management.

A list of communication requirements to sustain these services includes: IP to end node, constant and predictable key performance metrics (e.g. latency), monitoring services end-to-end of active and passive grid equipment, unified communications architecture and solutions, mix of fiber and wireless technologies, full support for existing grid communications protocols (e.g. IEC 61850, OPC UA) and semantics (e.g. IEC 61968 CIM), time synchronization (e.g. IEEE 1588v2), multicast, QoS mapping, scalability, path and equipment resilience with fast restoration and convergence (e.g. 1+1), stringent service level agreements (SLA) enforcement and monitoring, secured on multiple layers (e.g. ITU-T X.805) [4], [5].

A summary of smart grid per service communication requirements is in Table 1. AMI is today practically sole service in distribution part of grid (medium (MV) to low voltage). However, near future will bring many of listed services also on distribution grid, resulting in higher bandwidth-density (Mbps/km^2).

Table 1: Communication requirements for some smart grid services

Criteria / Service	One way delay	Bandwidth	Topology	Availability	Accurate timing	Redundancy	Packet loss
Teleprotection	5-10 ms	64 kbps	P2P, P2MP	99,9999	Yes	Yes	0,1 - 1 %
WAMPAC	50 ms	100 kbps	P2P, P2MP, MP2MP	99,9999	Yes	Yes	1 %
PMU	50 ms	1 Mbps	P2P, P2MP	99,999	Yes	Yes	1 %
SCADA HV	10 ms	64 kbps	P2P, P2MP	99,9999	Yes	Yes	1 %
SCADA MV	100 ms	64 kbps	P2P, P2MP	99,999	Yes	Yes	> 1 %
Fault isolation MV	80 ms	64 kbps	P2P, P2MP, MP2MP	99,9999	Yes	Yes	0,1 %
DG	100 ms	64 kbps	P2P, P2MP	99,99	No	No	> 1 %
DLR	200 ms	64 kbps	P2P	99,9	No	Yes	> 1 %
LFC/AGC	500 ms	32 kbps	P2P	99,999	Yes	Yes	1 %
Wind turbine	500 ms	3.5 Mbps	P2P	99,99	Yes	Yes	> 1 %
AMI	> 1000 ms	< 1 kbps	P2P	95	No	No	> 10 %
Notes:	P2P = point-to-point, P2MP = point-to-multipoint,						
	MP2MP = multipoint-to-multipoint, DLR = dynamic line rating,						
	LFC = load frequency control						

III. SMART GRID NETWORK ANALYSIS

Distribution power grid is a network where nodes (or "vertices") are stations (e.g. transformer, generator, substation, pole, consumer) and links ("edges") correspond to MV and LV distribution lines between nodes. Network can be represented mathematically by graph, G = (N, L), where N

represents the set of nodes (or vertices) and L denotes the set of links (edges). Graph information can be augmented to contain detailed information about links (e.g. impedance, current carrying capacity), which can be represented by weighted links. Power grids belong to complex networks types (also Internet), with heterogeneous topology where most nodes have only a few connections and only a few nodes (e.g. substation) connect to a high number of links (Figure 2). Such networks have no scale, are called scale-free.

We limit our analysis to undirected graph for which the relationship between pairs of nodes are symmetric (i.e. without directional character). The focus is to degree of node, i.e. the number of links connecting with any other node.

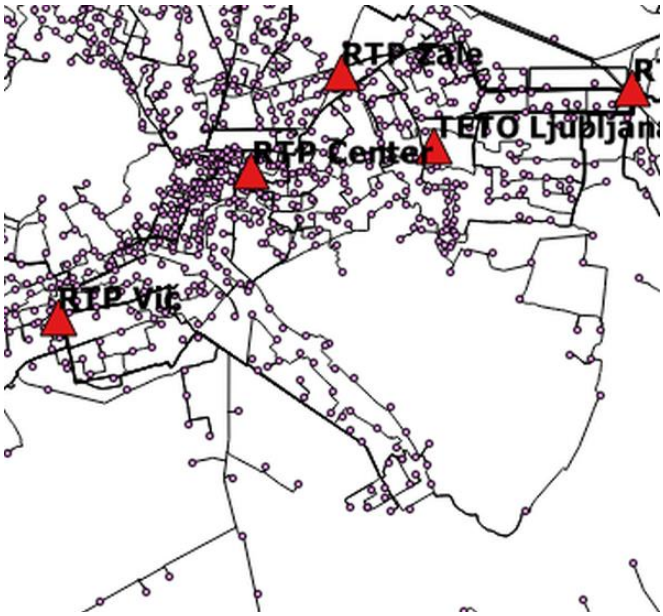


Figure 2: Grid network topology example (triangle = substation, circle = TS)

A. *Methods*

Geographical information systems (GIS) are vital analytical tools for grids development and analysis. We use software package Gredos [6] that is distinguished by an efficient I/O data exchange interfaces, analytics and optimization modules (e.g. power flow, reliability) and integration with advanced metering infrastructure (AMI) and other GIS systems (e.g. ArcGIS) installed at utilities. System allows for effective identification of static (lengths, loops) and dynamic (supply continuity, phasors) grid technical parameters.

B. *Metrics*

We use selected metrics on grid network that reveal its key topology characteristics:

– number of TS (MV/LV) per substation (HV/MV)
– line of sight distance from TS to substation
– line of sight distance from TS to other TS
– grid connection density per TS
– grid connection density within TS radius

TS to TS distances and grid connection densities are parameters most influencing the placement of RRH to achieve required radio coverage of end nodes or population. TS to substation distance is crucial check the RRH-BBU distance limitation of 10–15 km to stay within 5G clock jitter limits.

Furthermore, we are able to overlay customer end nodes connections to particular TS with 100 m x 100 m grid resolution, to study potential coverage from TS/RRH installations (Figure 4).

C. *Analysis and results*

Data was gathered for the complete distribution grid (MV/LV) containing approximately 90 substations (HV/MV) and 16.000 TS (MV/LV). Cable grid length from all substations to TS is > 15.000 km. This length is input into fiber deployment cost model (Chapter IV A).

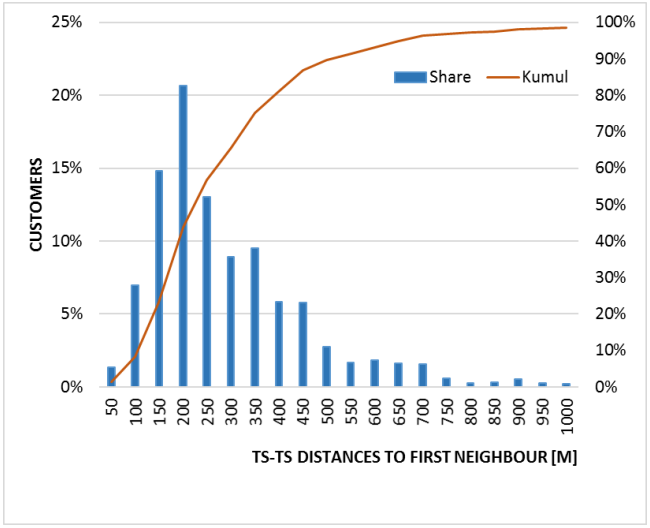


Figure 3: TS–TS distances and customer coverage within radius (sample utility only)

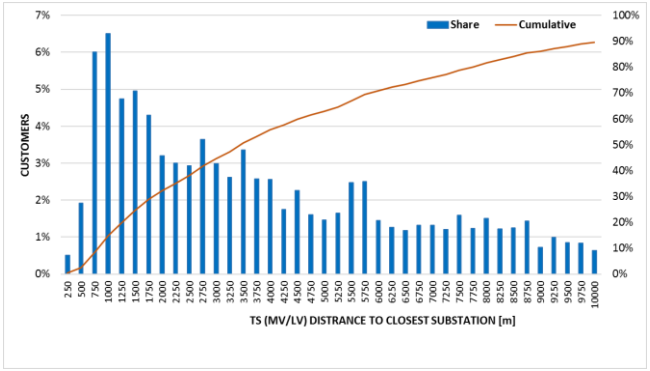


Figure 4: TS–RTP distances and cumulative end customer coverage achieved in the region (sample utility only)

The real determining factor how to share the utility infrastructure and put it into use for 5G is the potential customer coverage from existing TS locations. Additional metric are distances from TS to substations, as a limiting factor for 5G deployment and largest cost influence in fiber to RRH deployment. For each of five utilities there are differences in distribution distances (Figure 3, Figure 4), due to different geography and resultant customer positioning (e.g. dense urban, spread rural, valley). For "last mile", access 5G coverage of end nodes (customers) is limited by smaller cells sizes. We have studies cases of 250 m and 500 m cell radiuses as reported in literature. Summary of results (Table 2) show that coverage easily crosses 65 % even for smaller cell 250 m radius, whereas for 500 m we reach beyond 95th

percentile. These short distances imply that it may be possible also to use D2D for direct TS–TS communication in some cases.

Table 2: Summary analysis of distances and customer coverage for all utilities

Metric / Utility	Distances		Customer coverage	
	Average distance [m] TS-subst	Average distance [m] TS-TS	End customers from TS radius 250 m	End customers from TS radius 500 m
Utility 1	3.733	398	98,6%	98,5%
Utility 2	5.428	456	79,9%	97,2%
Utility 3	5.967	473	80,2%	95,9%
Utility 4	5.455	504	65,1%	96,9%
Utility 5	5.746	507	65,2%	95,1%

IV. REDUCED COST COMMUNICATIONS NETWORK DEPLOYMENTS

Sharing costs creating or updating communications infrastructure offers opportunities in physical part of infrastructure (site and infrastructure sharing), active equipment and management, the so called full sharing (Figure 5) [7]. We are focusing on site and infrastructure sharing.

Considered costs and benefits for both telecom operator and utilities are summarized in Table 3.

Table 3: Costs and benefits for telecom operator and utility

Cost types	Telecom operator	Utility
Site acquisition costs	Benefit	Cost
Site preparation costs	Benefit	Cost
Site rental costs	Benefit	Benefit
Site administration costs	Benefit	Benefit
Basic site maintenance costs	Benefit	Benefit
Infrastructure costs	Benefit	Cost
Electricity costs	Benefit	Benefit
Further site maintenance costs	Benefit	Benefit
Infrastructure rental/hosting	Cost (hosting)	Benefit (rental)

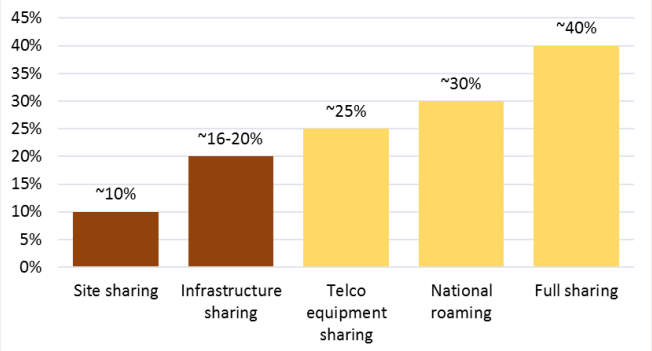


Figure 5: Network sharing – order of savings.

A. *Preliminary analysis and results*

We have reviewed network of existing TS. The main output was a coverage of the population achieved with RRH deployment. There were two different radiuses (r_1=500 m, r_2=250 m) taken into account. RRH need to be served by optical fiber as it is at TS. Based on the several American and European IT studies we did estimate the costs of individual parts of the investment.

As number of TS and length of the line from GIS is known, we can do arbitrary-precision analysis for telecom operator or utility. The preliminary analysis shows the need for additional investment of > 300 M€ in case of building a separate fiber optic infrastructure for telecom operators. The distribution of these costs by stakeholders is shown in Figure 6. These costs are only the difference of investment needed for 5G deployment incurred if no sharing of infrastructure takes place, and without Capex for active equipment [8]. This is why this part of investment should be considered as a benefit of infrastructure sharing.

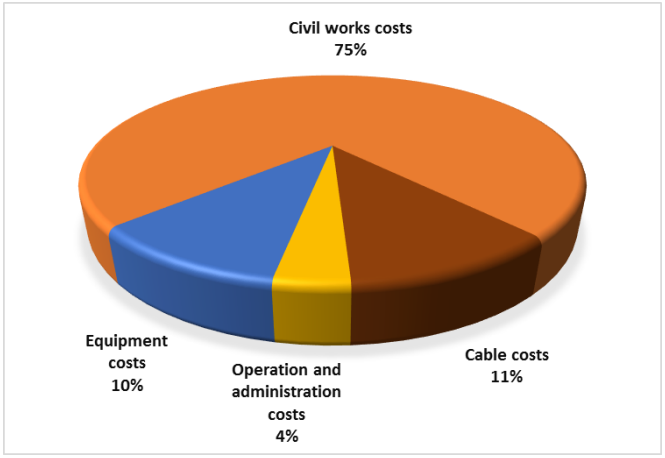


Figure 6: Fiber to TP investment costs sharing as a benefit of grid hosting

The analysis shows obvious savings of grid hosting. Our assessment of > 300 M€ gives us a rough estimate of saving for fiber optic per km: 20.000 €. Some American, European and Korean studies have shown a similar assessment of fiber optic cost per km.

Further potential cooperation models include the exploitation of fiber-cellular infrastructure over their life cycles, that bring up lower Opex and offers business model innovation potential, e.g.: sharing spectrum, RRH, backhaul links (λ in DWDM PON).

V. CONCLUSION

Utilities will increasingly require more communications capabilities for future development of smart grids and services on top. This fits with planned telecom upgrades to 5G. However, such expansion cannot be achieved without major installation costs for new 5G cell sites. Therefore, telecom operators may host part of utility owned existing infrastructures (TS, fiber) and achieve required denser 5G RRH/BBU deployments with lower Capex. We have analyzed this possibility through the benefits perspective.

Telecom operators, to cover the area with fiber optic that is already covered by utilities, would need several hundred million € besides the remaining investment costs to achieve full coverage. This estimated value is considered as a benefit of hosting a fiber optic grid at utilities. Furthermore, the RRH deployment at TS serves also utilities for reliable smart grid services communications channel. Additional benefits appear with cooperation and sharing (e.g. lower costs of maintenance, support) which is why both market players should consider the future collaboration/infrastructure sharing.

Further work is ongoing on the detailed cost analysis on a per utility and city basis, also taking into account elaborate radio propagation models.

ACKNOWLEDGEMENTS

This paper is based upon work partially funded by EU & Horizon 2020 under project FutureFlow, Designing eTrading Solutions for Electricity Balancing and Redispatching in Europe, GA # 691777.

LITERATURE

[1] 5G radio access, Ericsson, 4.2016.
[2] DIRECTIVE 2014/61/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures to reduce the cost of deploying high-speed electronic communications networks, 5.2014.
[3] Federal Communications Commission, In the Matter of Protecting and Promoting the Open Internet, 2.2015.
[4] IEC TR 61850-90-12:2015, Communication networks and systems for power utility automation – Part 90–12: Wide rea network engineering guidelines.
[5] M. Ahmed, Communication Network Architectures for Smart-Wind Power Farms, 2014.
[6] Načrtovanje razvoja distribucijskega sistema – REDOS 2040, 2016.
[7] The State of Broadband 2014: broadband for all – a report by the broadband commission. September 2014.
[8] J. P. R. Pereira, Infrastructure Sharing as an Opportunity to Promote Competition in Local Access Networks. Journal of Computer Networks and Communications. May 2012.

Maja Kernjak Jager holds a MSc (2010) of economics from University of Ljubljana, Faculty of Economics. She works as a researcher at EIMV. Her main fields of work are economic, cost benefit analyses and business process modeling in power engineering.

Tomaž Mohar received his MSc in electrical engineering from University of Ljubljana (2010). Since 1992 he has been working as researcher at EIMV. His professional interests span load flow a reliability analysis, distribution planning and network structure optimization. He is co-author of GIS Gredos software.

Radovan Sernec joined Electric Power System Control and Operation department at EIMV in 2016 as a researcher on smart grids, communication technologies and EU H2020 projects. His background spans process automation, ICT and innovation management.

Andrej Souvent received the M.Sc. degree in electrical engineering from University of Ljubljana, Ljubljana, Slovenia in 2016. He is head of Electric Power System Control and Operation department at EIMV. His research interests include smart grid concepts, technologies and solutions.

Samovozeča vozila

Roman Šimenc, Autocommerce d.o.o / Daimler AG, Slovenija

Povzetek — mnenja o tem, kako daleč smo od avtonomne vožnje, so različna, razna uspešna testiranja pa potrjujejo, da tehnika napreduje zelo hitro in da ta pri vsem skupaj sploh ni več glavna ovira. Na vse zadnje so razni sistemi, ki omogočajo vsaj delno avtonomno vožnjo že danes nekaj povsem vsakdanjega. Novice o testiranjih takšnih in drugačnih sistemov pri tovornih ali osebnih vozilih na testnih stezah ali ob posebnih dovoljenjih tudi v realnem prometu, so postale nekaj vsakdanjega in res ni več daleč dan, ko bomo vsi v avtomobilih zgolj potniki, vozili pa bodo ti kar sami.

Ključne besede — avtonomna vožnja, samovozeča vozila, asistenčni sistem

Abstract – opinions on when autonomous driving will become a reality differ, while numerous successful tests have confirmed that the technology is advancing rapidly and that it is no longer the main obstacle in this matter. After all, various systems for partially autonomous driving are fairly common these days. The news about testing diverse systems of this kind, be it for trucks or passenger cars, on test tracks or in real traffic with special permits, has become commonplace. It seems that we are soon to become mere passengers, traveling in vehicles that will do all the driving.

Keywords – autonomous driving, self-driving cars, driver-assistance systems

I. UVOD

Avtonomno vožnjo z vozili običajno povežemo z letali v avtopilotnem načinu, ki vzdržujejo smer vožnje brez človeškega posega v krmiljenje, vizualni nadzor in nadzor pospeševanja ali zaviranja. Avtonomno vožnjo (včasih navedeno tudi kot avtomatizirana vožnja ali avtopilot) razumemo kot premikanje vozil, transportnih vozil brez voznika in mobilnih robotov, ki v veliki meri delujejo samostojno. Samovozeče vozilo je zmožno zaznavati okolico in voditi brez človeškega vpliva. Mnoga takšna vozila so že bila razvita, toda do maja 2017 avtomatiziranim vozilom ni dovoljeno voziti polno avtonomno vožnjo na javnih cestah. Na letošnjem sejmu zabavne elektronike v Las Vegasu v začetku leta, sta bila predstavljena samovozeči Audi A7, ki je skoraj 900 km dolgo pot od Silicijeve doline do prizorišča prevozil brez voznika in Mercedes–Benzov koncept F 015 luxury in motion, kateri bo po navedbah principala čez približno 15 let prevzel funkcijo vožnje. Avtomobili preraščajo vlogo prevoznega sredstva kot takšnega in bodo v prihodnosti postali mobilni življenjski prostor. Naši samovozeči avtomobili bodo ljudem ponudili natanko to, F 015 pa je prvo konkretno dejanje v to smer, je dejal prvi mož Daimlerja Dieter Zetsche.

II. STOPNJE AVTONOMNE VOŽNJE

V Evropi in tudi v ZDA razvrščamo avtonomno vožnjo v 6 stopenj:

- **Stopnja 0:** »samo voznik«, voznik sam upravlja s krmilnim sistemom, dodaja plin, zavira, itd.
- **Stopnja 1:** posamični asistenčni sistemi pomagajo pri upravljanju vozila (npr. aktivni tempomat).
- **Stopnja 2:** delna avtomatizacija. Asistenčni sistemi prevzamejo med drugim avtomatizirano parkiranje, držanje smeri vožnje, asistenco preprečitve naleta, asistenco ob zgoščenem prometu, asistenco nadzora razdalje pospeševanja in zaviranja, itd.
- **Stopnja 3:** visoka avtomatizacija. Vozniku ni potrebno trajno nadzirati sistema. Vozilo krmili samostojno funkcije kot so aktivacija smernika, menjava voznega pasu, ter držanja smeri. Voznik lahko namenja svojo pozornost drugim stvarem, toda mora biti sposoben pri zahtevi in predhodnem obvestilu sistema vozila prevzeti vodenje. Ta avtonomija je tehnično smiselna za avtocestni način vožnje. Zakonodaja dela trenutno na tem, da bo dopustila vožnjo stopnje 3 do leta 2020.
- **Stopnja 4:** popolna avtomatizacija. Vodenje vozila je popolnoma prepuščeno sistemu. Če sistem ne bo več opravljal naloge vožnje, bo voznik pozvan za prevzem nadzora vožnje.
- **Stopnja 5:** voznik ni potreben. Razen določitve sistemu o začetku ter cilju ni potrebnega človeškega posega.

III. TEHNIČNI RAZVOJ

Tehnično se je avtonomna vožnja razvila iz voznih asistenčnih sistemov. Najzgodnejši sega v leto (1958) in sicer od Chryslerja razviti tako imenovani tempomat, ki samodejno regulira vzdolžno pospeševanje, brez zaznavanja okoliških vozil. Polno samodejno vzdolžno vodenje (aktivni tempomat) pa upošteva promet in s tem predstavlja obliko delno avtonomne vožnje. Avtonomna vožnja velja kot menjava vzorca in je kot tak revolucionarni proces. Pogoj za to je, da so v vozilu prisotni senzorji, kot so radar, kamera, laser, aktuatorji za krmiljenje motorja, krmila, zavore. Avtonomnost zagotavlja krmilna enota, ki zbira senzorske podatke in ustvari sliko okolice, ustvari odločitev o avtomatskem načinu vožnje in vse to pošilja odgovornim aktuatorjem. Za reševanje velikih količin podatkov, npr. pri zaznavi voznih znakov, se pogosto uporablja v vozilih t.i. strojno učenje.

IV. ASISTENČNI SISTEMI

Asistenčni sistemi so osnova za delno avtonomno vožnjo, toda so samo asistent upravljavcu vozila in kot taki ne ponujajo popolne avtomatizacije. V veliki meri današnjih višje cenovnih vozil se srečujemo s stopnjo 2 avtonomne vožnje. Naj naštejem nekaj asistenčnih sistemov v serijskih vozilih Mercedes–Benz:

- **Aktivni asistent omejitve hitrosti,** samodejno nastavi vozilo na predpisano hitrost. V kombinaciji z COMAND Online lahko opcijsko voznik nastavi funkcijo asistenta

voznih znakov, t.i. aktivni asistent omejitve hitrosti. Aktivni asistent razdalje lahko nastavi predpisano hitrost, ki jo zazna z branjem znakov preko kamere, vključno z znaki za popravila na cestišču. Samodejno lahko prilagodi tempomat na hitrost shranjeno v navigacijskem sistemu, npr. v Nemčiji 50 km/h v mestih ali 100 km/h na podeželskih cestah. V posameznih primerih je lahko hitrost proaktivna. Na cestah brez omejitve hitrosti, npr. na delih avtocestnih odsekov v Nemčiji, je nastavljena hitrost 130 km/h kot priporočena hitrost. Lahko se spremeni na želeno hitrost voznika in ostane nastavljena dokler ni omejitve ali vozilo ne zapusti avtoceste oziroma se izključi upravljanje vozila (kontakt).

– **Aktivni asistent menjave voznega pasu,** podpira krmiljenje na sovoznikov pas. Asistent podpira voznika pri menjavi pasu na več pasovnih cestah. Razbremenjuje voznika in lahko pomaga s sodelovanjem drugih asistenčnih sistemov preprečiti nezgodo. Če voznik aktivira smernik, aktivni asistent podpre krmiljenje krmilnega sistema pri menjavi pasu na sovoznikov pas. Menjava pasu levo ali desno je možna v okviru desetih sekund samo, če senzorika sistema ne zazna nobenega vozila v varnostnem območju. Radar dolgega dometa in več-funkcijska stereo kamera zaznavata območje pred vozilom, območje za in ob strani vozila pa je stalno nadzorovano preko dveh več - načinskih radarjev. Zahteva ter aktivacija aktivne menjave pasu je prikazana na kombiniranem instrumentu in opcijsko projicirana na vetrobransko steklo.

  Kriteriji za izvedbo aktivne menjave pasu:

  – aktivni asistent krmilnega droga je aktiven,
  – aktiviran je smernik,
  – zaznava razpoložljivega časovnega okvira za menjavo pasu znotraj desetih sekund,
  – trenutno zaznana vožnja na večpasovni cesti preko navigacijskega sistema COMAND Online in stereo kamere,
  – sosednji pas je ločen s prekinjeno črto,
  – hitrost vožnje je med 80 in 180 km/h.

  Sistem prekine z aktivno menjavo pasu, ko senzorika zazna oviro, ne zaznava več cestnih označb, voznik zavije v nasprotno stran, aktivira nasprotni smernik ali izklopi asistenta za aktivno krmiljenje.

– **Aktivni asistent razdalje (DISTRONIC) z aktivnim krmilnim asistentom,** kooperativna vožnja z vzdolžno in prečno pomočjo. Na vseh vrstah cest, avtocestah, lokalnih cestah kot tudi mestnih cestah, inteligentni sistem ni zmožen samo vzdrževati razdalje pred vozilom s sistemom aktivni asistent razdalje (DISTRONIC), temveč lahko tudi sledi prometu. Sistem podpira voznika pri normalni vožnji s posredovanjem pri dodajanju plina ali zaviranju, kot tudi pri krmiljenju krmilnega droga v bolj ostre ovinke. Do hitrosti 130 km/h sistemu ni potrebno zaznavati jasno označenih cestnih označb. Lahko ostane aktiven tudi če označbe niso jasne, npr. delo na cesti. Sistem lahko učinkovito pomaga vozniku predvsem pri gneči in zastojih.
– **Aktivni asistent zasilne ustavitve,** če voznik ni zmožen odreagirati. Aktivni asistent zasilne ustavitve zavre vozilo do popolne ustavitve na njegovem pasu, če voznik ne reagira, ko je aktiven asistent za krmilo. Če po predvidenem času ni premika krmilnega obroča, sistem informira voznika preko vizualnega ter akustičnega opozorila, da položi roke na krmilni obroč. Po nekajkratnih vizualnih ter akustičnih opozorilih in če še vedno ni odzivnosti voznika preko volanskega obroča, dodajanjem plina, zaviranjem,ali upravljanjem gumbov na volanskem obroču, vozilo samodejno zavre na njegovem pasu do mirovanja. Pri hitrosti pod 60 km/h vozilo opozori ostali promet z aktivacijo vseh štirih smernikov. Ko se vozilo popolnoma ustavi, se samodejno aktivira parkirna zavora in aktivira se Mercedes–Benzov klic v sili. Vozilo ostane odklenjeno z namenom dostopa prve pomoči. Funkcija se lahko prekine preko voznikovega posega v kontrole vozila.
– **Prilagoditev hitrosti glede na v naprej nastavljeno pot**, proaktivna podpora. Če je aktivni asistent za razdaljo aktiven, se bo hitrost samodejno prilagodila cestnim dogodkom pred nami, kot so ovinki, T- križišča, krožišča in izvozi. V naprej izbrani cestni odsek bo izpeljan glede na izbran način vožnje, energijsko varčni, komfortni ali dinamični način vožnje. Po izpeljanem odseku se hitrost povrne v naprej nastavljeno območje. Prilagoditev hitrosti ne upošteva pravil ceste, naloga nadzora ostane pri vozniku. Pri zaznani zahtevi za spremembo smeri v križišču na sosednji pas ali odstavni pas se bo hitrost prilagodila z aktivacijo smernika. Pri aktivnem vodenju preko navigacijskega sistema COMAND Online se prilagoditev izvede avtomatično.

V. PRAVNE ZADEVE

Glavna težava samodejne vožnje niso več avtomobili, temveč odgovornost v primeru nesreče in vprašanje, kakšnih pravil se bo potrebno držati. Avtonomna vožnja nam postavi težko pravno-odgovorno vprašanje, na katerega moramo odgovoriti etično in pravno-filozofsko. Tema je bila večkrat izpostavljena na nemških prometnih pravnih dnevih. Komisija je na 53. nemških prometnih pravnih dnevih januarja 2015 zaključila, da tehnični napredek pomembno pripomore k izboljšanju varnosti in pretočnosti v prometu. Zaradi trenutnih pravnih možnosti pa ne dovoljujejo popolne in trajne vpeljave avtomatizacije sistema. Določili so, da mora biti voznik sam zmožen odločati o uporabi sistema (možnost izklopa). V vsakem trenutku mora biti informiran o stopnji avtomatizacije. Voznika pa se mora oprostiti sankcij in odgovornosti za vožnjo v visoko avtomatiziranem voznem načinu. 54. nemški prometni pravni dnevi januarja 2016 so se končali z nestrinjanjem o avtonomni vožnji. Ključna točka diskusije je bila družbena odobritev ter etnični vidik (kako naj reagirajo algoritmi v tako imenovani »situaciji dileme«).

Od poletja 2016 je Nemško zvezno ministrstvo za promet delalo na osnutku zakona za avtomatizirano vožnjo. Ključna točka osnutka se nanašala na obveznosti upravljavca vozila. Dovoljeno mu je, da odvrne pozornost od vožnje, toda samo toliko, da je vsak trenutek zmožen takoj prevzeti nadzor nad avtomatiko vožnje ter krmilnim sistemom. Nadaljnja ključna točka je tudi nova odredba odgovornosti tveganja. Poraja se vprašanje, če lahko upravljavec vozila brezskrbno zaupa upravljanju, kadar ne zaupa popolnoma v vgrajeno tehniko v vozilu. 25. januarja 2017 je nemška zvezna vlada izdala osnutek odloka, da je avtonomna vožnja na nemških cestah dovoljena pod določenimi predpogoji, 30. marca pa je bil ta odlok sprejet. S tem je dovoljeno upravljavcu vozila v ustrezno opremljenem vozilu med vožnjo visoko oziroma

popolno avtomatizirana funkcija vožnje. Upravljavec lahko odvrne pozornost pogleda na vozišče in od krmilnega sistema, toda mora ostati v stanju zaznavanja – to je njegova obveza. V vozilo se vgradi »blackbox«, ki snema vse ustrezne podatke. Ti podatki se shranjujejo 6 mesecev, razen v primeru, če je bilo vozilo udeleženo v prometno nezgodo, takrat pa podatki ostanejo shranjeni z namenom analize poteka nezgode.

Kalifornijski urad za vozila DMV (California department of motor vehicle) v Združenih državah Amerike je decembra 2015 določil, da je avtonomna vožnja dovoljena pod pogojem, da je avtonomno vozilo opremljeno s krmilom in stopalkami. Voznik mora imeti dovoljenje za vožnjo in mora biti v vsakem trenutku pripravljen prevzeti nadzor nad vožnjo.

VI. VARNOST

Združene države Amerike so pionir preizkusa avtonomnih voženj. V letu 2015 je bilo 48 osebnim vozilom dovoljeno voziti v odprtem prometu. Vse nezgode so bile prijavljene, toda statistika ni javno dostopna. Googlova polno avtonomna vozila so bila udeležena v nesrečah v več primerih, večinoma znotraj mest. V enem od znanih primerov je bil vzrok za nesrečo avtonomni algoritem. 7. maja 2016 je prišlo do smrtne nezgode z vozilom Tesla S. Teslin voznik je umrl pri naletu v nasproti vozeče vlečno vozilo, ki je zavijalo levo, brez da bi »avtopilot« ali voznik upravljal z zavoro.

VII. ZAKLJUČEK

Testiranja posameznih vozil na posameznih odsekih so eno, vsakdanja in vsaj v večjem delu avtonomna vožnja pa nekaj drugega. Od popolnoma avtonomne vožnje, ko voznik v cestnem prometu ne bo več potreben, smo še daleč. Po mojem predvidevanju je potrebno še desetletje za realizacijo avtonomne vožnje v vsakdanjem prometu. V današnjih vozilih so številni napredni sistemi, ki omogočajo delno avtonomno vožnjo, res da večinoma v vozilih višjega cenovnega razreda, ki pa jim ne gre popolnoma zaupati. To so sistemi, ki delujejo na osnovi senzorjev (čutil) v vozilu, ter radijske komunikacije med vozili. Vsi so seveda sinhroniziranimi z vsemi drugimi sistemi v avtomobilu, ki krmilijo in posledično upravljajo vozilo. Danes je delež avtonomne vožnje odvisen od modusa vožnje. Če veliko vozimo po avtocesti in je veliko gostega prometa, vozilo lahko do hitrosti 60 km/h vozi popolnoma avtonomno, brez časovne omejitve. V drugih pogojih vožnje je tega bistveno manj. A vseeno bi rekel, da smo, kar zadeva tehnologijo vozila v povezavi s samodejno vožnjo, na točki razvoja že presegli mejo 50 odstotkov. Uporabniki, po mojih izkušnjah, takšne sisteme, ko jih enkrat preizkusijo in jim zaupajo, tudi z veseljem uporabljajo. Popolnoma zaupati tovrstnemu sistemu pa še ne moremo, saj še vedno prihaja do omejitev »čutil« vozila. Stereo kamera ima, npr. težave pri močnem deževju, megli ali pri upadu sončnega žarka naravnost na njo in v teh razmerah, tako kot naše oko, ne more opraviti svojega dela. Seveda je že v pripravi novejša izpopolnjena kamera, ki bo zmanjšala tovrstne omejitve. Še vedno pa velja tudi, da smo vozniki odgovorni za vse, kar se dogaja v prometu in so ti sistemi samo asistenčni in nam služijo kot pomoč. To, da smo vozniki odgovorni za vse, se zdi v tem trenutku celo večja ovira na poti do avtonomne vožnje vozil, kot sama tehnika, saj je ta zelo napredovala. Odgovornost v primeru nezgode bo področje pri katerem bo zakonodaja pred izzivom. Poudaril bi pa še eno težavo, to je infrastruktura. Od nje je namreč v veliki meri odvisna radijska komunikacija med vozili. Njena sprememba, nadgradnja pa predstavlja tudi velik strošek. Vozilo mora komunicirati s križišči in obcestnimi postajami, ter seveda z drugimi vozili, če hočemo gospodarno ter varno upravljati promet. Dodatni strošek pri nakupu vozila s paketom voznih asistenc je danes ocenjen na 4 tisoč €, vložek v infrastrukturo pa bo moral biti znatno višji.

LITERATURA

[1] Autonomes Fahren Technische, rechtliche und gesellschaftliche Aspekte; Markus Maurer - J. Christian Gerdes – Barbara Lenz – Hermann Winner Hrsg.
[2] https://de.wikipedia.org/wiki/Autonomes_Fahren
[3] http://media.daimler.com/marsMediaSite/

Roman Šimenc je v podjetju Autocommerce d.o.o. zaposlen že 22 let. Najprej je bila njegova zadolžitev v podjetju reševanje težjih tehničnih problemov v povezavi z znamko Mercedes–Benz ter komunikacija s principalom. Zadnjih 15 let je zadolžen za izobraževanje znotraj podjetja, zadnjih pet let pa vodi oddelek izobraževalnega centra Mercedes–Benz Slovenija. Je tudi s strani principala certificirani trener za področje osebnih vozil Mercedes–Benz.

5G in multimedijske vsebine na področju javne varnosti

Franc Dolenc, Mirko Orehek, Roman Uršič, Mediainteractive
Mitja Mohor, Zdravstveni Dom Kranj

Povzetek — Članek opisuje potrebe in rešitve pri prenosu različnih vsebin na področju delovanja služb Nujne medicinske pomoči v primeru množičnih nesreč in rednih intervencij

Ključne besede — 4G, 5G, Nujna Medicinska Pomoč, Video, Videokonferenca, WebRTC

Abstract — The article is focused on transport of different data and media types in communications scenario in the field of Mass Accidents and daily Urgent Medicine operations

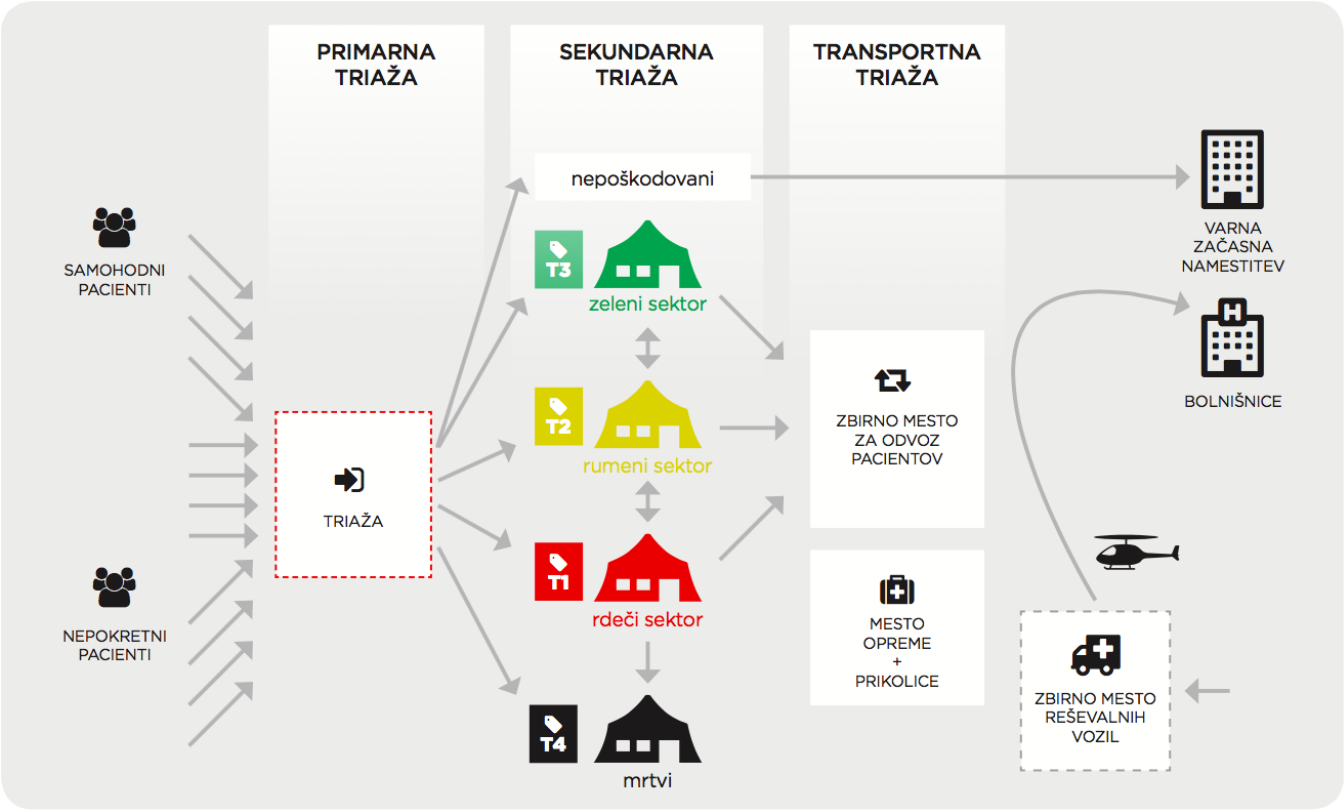
Keywords — 4G, 5G, Public Safety, Video, Videoconferencing, WebRTC

I. UVOD

Razvoj mobilnih komunikacijskih omrežij, naprav in aplikacij prinaša izjemne priložnosti v razvoju komunikacijskih rešitev za podporo delovanju službe Nujne medicinske pomoči (NMP). V Sloveniji imamo izjemno dobro razvito službo z odličnimi izvajalci, dobro organiziranimi delovnimi procesi in modernimi medicinskimi orodji in s tem vzpostavljeno primerno okolje za razvoj specializiranih komunikacijskih rešitev.

V podjetju Mediainteractive smo v sodelovanju s sodelavci Nujne medicinske pomoči na Gorenjskem zasnovali napredno okolje za komunikacijo in kolaboracijo, ki lahko bistveno prispeva k učinkovitosti medsebojnega informiranja, odločanja, operativnega sodelovanja in s tem lahko prispeva k reševanju človeških življenj in optimizaciji stroškov delovanja NMP.

Komunikacijski sistem povezuje vse dejavnike v procesu vzpostavitve in delovanja službe za NMP v primeru množične nesreče. Za svoje delovanje uporablja najmodernejše razpoložljive tehnologije, kot so mobilno omrežje 4G in WiFi, zmogljive mobilne naprave, tehnologijo WebRTC in HLS z naprednimi kodeki za potrebe video komunikacije ter hitro in zanesljivo interno komunikacijsko jedro.



Slika 1: Shema delovišč in delovnih procesov služb NMP pri množični nesreči.

Pridobljene izkušnje iz poskusnega delovanja so odlična osnova za načrtovanje potreb po bodočih transportnih tehnologijah, kot so LTE Advanced, LTE Advanced Pro in 5G.

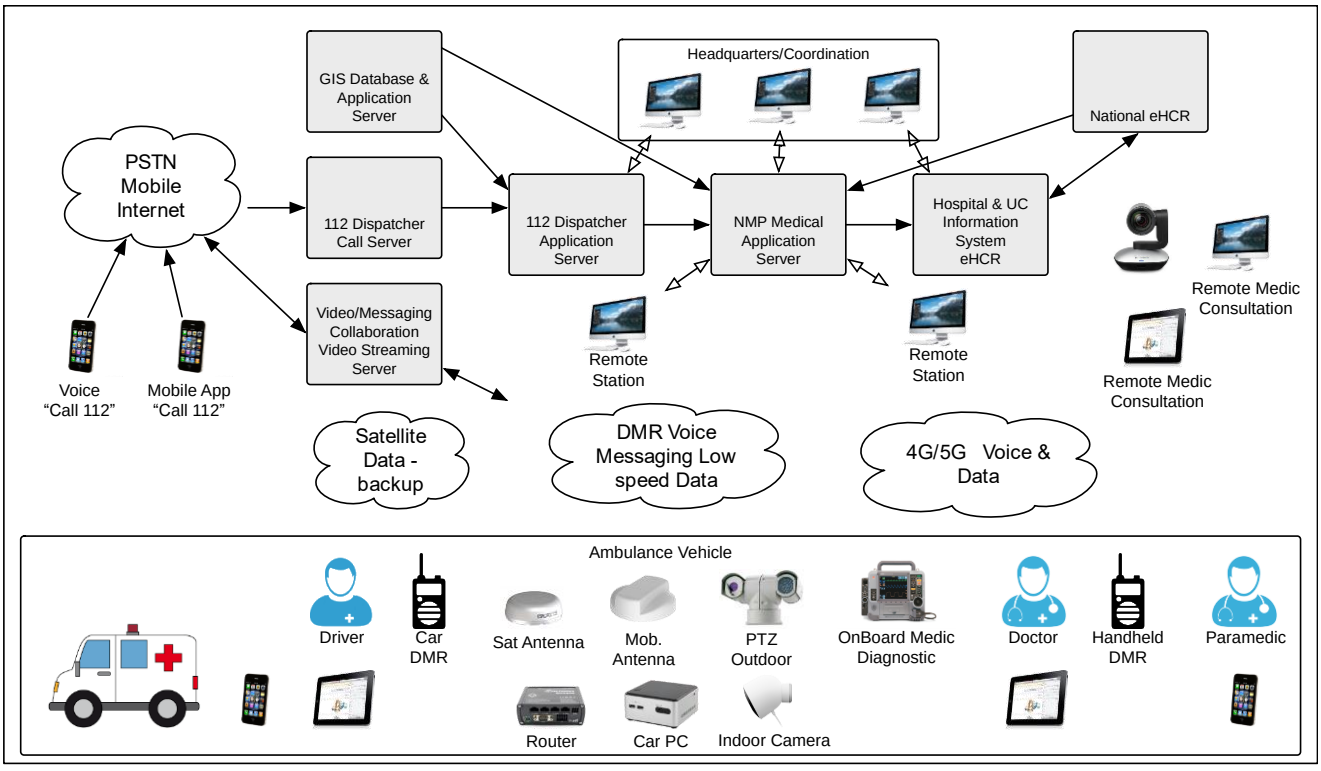
Obenem so odlična osnova za načrtovanje komunikacijskih sistemov za druge intervencijske službe, kot so gasilci, civilna zaščita in podobno, ki bodo predstavljali celotno okostje za podporo učinkovitemu reševanju življenj in premoženja v Sloveniji. Naloge in delovni procesi teh služb so drugačni od NMP, v izgradnji komunikacijske infrastrukture imajo pa večino elementov skupnih.

II. CILJI PROJEKTA PROGRAM ZA NMP

Podatki in zaključki v tem članku so zasnovani na izkušnjah projekta *Program za NMP*, ki smo ga izvajali v preteklih letih. Programska oprema PNMP pokriva različne scenarije podpore Nujne medicinske pomoči od dnevne uporabe do množičnih nesreč in vključuje klasično reševalno vozilo, reševalca z motorjem in helikoptersko nujno medicinsko pomoč. Jedro sistema je zasnovano na potrebah množičnih nesreč, ki je najbolj zahteven scenarij.

Slika 2: Prikazana je simultana uporaba videokonferenčnega sistema, sporočilnega sistema, prenosa s kamere za video opazovanje in vnosni obrazec na mobilni napravi. Na videokonferenčnem sistemu je slika pacienta in slika oddaljenega svetovalca. Kamera za video opazovanje, montirana na komandnem vozilu, prikazuje pogled na prizorišče nesreče.

Slika 3: Prikazana je simultana uporaba videokonferenčnega sistema in agregirano dinamično stanje pacientov. Na podlagi tega pregleda glede na napotitev v bolnišnice, ki ga uporabljajo v vodstvu intervencije, se izbire optimalno vrsto transporta. Viden je tudi lokalni pogled na več pacientov na enem delovišču na mobilni napravi.



Slika 4: Možni komunikacijski kanali. Nekateri prikazani kanali še niso aktivni.

III. KOMUNIKACIJSKI SCENARIJ VELIKE MNOŽIČNE NESREČE

Velike množične nesreče so izjemen izziv za optimalno komunikacijsko rešitev. Za potrebe simulacije načrtovanja prenosnih zmogljivosti smo uporabili vajo množične nesreče Stožice 2016, ki je bila po nam znanih podatkih največja vaja v Sloveniji do sedaj.

Scenarij vaje je bil zgrajen na predpostavki, da je na stadionu Stožice prišlo do terorističnega napada z veliko eksplozijo in naknadnimi terorističnimi akcijami. Vpletenih je bilo 700 statistov, od katerih jih je bilo cca. 350 poškodovanih oziroma mrtvih. Za potrebe simulacije bomo uporabili izmišljene podatke o velikosti intervencijskih ekip in bomo predpostavili, da je bilo na lokaciji 50 rešilnih avtomobilov s 150 člani ekip, 50 gasilskih avtomobilov s 150 člani ekip in še 150 ostalih članov intervencijskih skupin, kot so civilna zaščita in ostali. Varnostnih organov, kot je policija, v tej simulaciji ne bomo upoštevali. Ti organi za svoje delovanje uporabljajo sistem TETRA, bi se pa lahko vključili tudi v omenjeno komunikacijsko omrežje.

Ob tako velikem številu udeležencev so razpoložljivi kanali DMR močno preobremenjeni, kar vpliva na uporabniško izkušnjo in zmanjšuje učinkovitosti. Razpoložljivost omrežja DMR se bo bistveno povečala, saj bo velik del komunikacij nadomeščen s prenosom podatkov preko omrežja 4G. Ta simulacija ni bila izvedena, ocenjujemo pa, da bo optimizacija velika. Prenos medicinskih podatkov preko govorne komunikacije je izjemno neučinkovit.

Za potrebe ocene komunikacijskih potreb v naprednem scenariju, kjer uporabljamo omrežje 4G kot pomemben substitut obstoječih komunikacij na tehnologiji DMR, smo uporabili izkušnje iz poskusne uporabe sistema Program za NMP – PNMP (delovno ime), ki smo ga razvili v zadnjih dveh letih in ki omogoča podatkovno, video konferenčno in video opazovalno funkcionalnost. PNMP je bil poskusno uporabljen na več vajah, med drugim tudi na vaji Stožice 2016.

Ocena podatkovnih kanalov je zgrajena na predpostavki uporabe obstoječe 4G in prihajajoče infrastrukture 5G. Sedanje stanje te infrastrukture v Sloveniji je dobro, rečemo lahko, da je za EU razmere nadpovprečno. Tri primerljiva mobilna omrežja so v veliki meri nadgrajena v tehnologijo LTE in LTE Advanced in predstavljajo dobro osnovo za delovanje. Kapacitete teh sistemov so primerno velike, vendar lahko pričakujemo v izrednih razmerah veliko težav z razpoložljivostjo.

– V primeru potresa ali terorističnega napada bi bile lahko bližnje bazne postaje onesposobljene.
– Lokalni promet bi bistveno narastel in povzročal blokado teh postaj.
– Zaradi varnostnih razmer bi bile bazne postaje »ugasnjene«, kot se je zgodilo npr. v Franciji.

Za te primere bo potrebno na nacionalnem nivoju razviti ustrezne ukrepe. Med njih spadajo:

– Nacionalni center za upravljanje s kapacitetami baznih postaj v izrednih razmerah. Obstoječi programski paketi vseh v Sloveniji instaliranih LTE tehnologij že omogočajo vzpostavitev takega centra, ki bi dinamično glede na potrebe omogočal prioritetno komunikacijo za določene uporabnike glede na njihove SIM kartice (Blue Light SIM) in po potrebi selektivno blokiral ostale uporabnike.
– Operaterji bodo pripravili ustrezno število mobilnih baznih postaj, ki jih bodo po potrebi pripeljali na ustrezne lokacije.
– Zgrajeno bo paralelno omrežje LTE za potrebe kritične infrastrukture.

Vsi ukrepi so komplementarni. Prvi in drugi ukrep sta investicijsko relativno vzdržna, zato je možna in nujna kratkoročna realizacija.

A. *Rešitve znotraj sistema NMP*

Poleg zgornjih celovitih ukrepov smo v sklopu scenarija komunikacij za potrebe NMP predvideli še nekaj rešitev, ki so možne znotraj sistema PNMP in sicer:

– Vozila za PNMP pridobijo integrirano opremo za komunikacijo preko 4G in sicer primerne zunanje antene in optimizirane usmerjevalnike. Oprema podpira delovanje na več frekvenčnih področjih 4G in obeh frekvenčnih področjih WiFi. Taka oprema je cenovno ugodna in nujna za večino vozil NMP.
– Nekatera (komandna) vozila pridobijo tudi ustrezno opremo za vzpostavitev satelitske komunikacije in opcijsko opremo za usmerjeno povezovanje na oddaljene bazne postaje 4G. Taka oprema je cenovno dostopna.
– Podatkovne kanale je z ustreznimi nastavitvami usmerjevalnikov v vozilih in izgradnji Mesh WiFi infrastrukture med vozili možno odlično povezati v celoto. Pri tem po potrebi uporabimo tudi mobilne repetitorje WiFi. Uporabniške mobilne naprave imajo na razpolago 4G in WiFi vmesnike in se lahko dobro povežejo v tako infrastrukturo. Ocenjujemo, da je komunikacijska tehnologija za podporo komunikacijam v okviru NMP dozorela za redno uporabo.

B. *Tehnologija 5G*

Tehnologija 5G za zgornji scenarij omogoča nekaj pomembnih izboljšav. V primeru množične nesreče na mestnem področju bo ponudila bistveno povečane kapacitete in omogočila, da bodo video kanali delovali z višjo kakovostjo prenosa.

Pričakujemo, da bodo mobilne postaje 5G primerne za instalacijo v komandna intervencijska vozila in bodo nadomestila uporabo WiFi-kanalov in s tem povečanje kapacitete in robustnosti teh kanalov.

V scenariju, kot so bile Stožice 2016 in ob predpostavki o nerazpoložljivosti lokalnih mobilnih baznih postaj, bi taka infrastruktura prevzela potrebe po nujnih komunikacijah, obdelanih v nadaljevanju.

IV. POTREBNI KOMUNIKACIJSKI KANALI

Na prizorišču vaje smo uporabljali naslednje komunikacijske kanale:

– Prenos podatkov o stanju pacientov oziroma ostalih prisotnih oseb ter stanju oziroma razpoložljivosti medicinskega osebja. Te podatke prenašamo preko sistema PNMP v obliki optimiziranega, komprimiranega in zaščitenega podatkovnega protokola med posameznimi mobilnimi napravami in strežnikom.

  - Za prenos pacientovih podatkov ocenjujemo, da bo izvedenih do cca 50 prenosov proti centru za enega pacienta, kar bi znašalo cca 50 kB prometa.
  - Za opcijski prenos ene fotografije bo potrebnih cca 500 kB prometa proti centru.
  - Za prenos potrebnih informacij od centra nazaj proti mobilnim napravam, preko katerega bodo izvajane lokalne koordinacije, pričakujemo, da bo 10-kratnik prenosa navzgor.
- Video sistemi:
  - Za potrebe videokonferenčnih povezav z najnižjo uporabno hitrostjo pričakujemo v primeru velike nesreče hkratno uporabo 10 kanalov s hitrostjo 500 kb/s.
  - Za potrebe prenosa video opazovanja pričakujemo vzpostavitev 10 kamer in prenos v HD kakovosti. V primeru omejitev pasovne širine bi z nizkim številom okvirov lahko delovali s hitrostjo 500 kb/s.
  - Ti video kanali bi v osnovni minimalni verziji zadoščali tako za medicinske kot ostale potrebe (gasilci, civilna zaščita...).

Za prenos podatkov o 700 pacientih znaša torej skupna ocena hitrosti pri predpostavki, da se večina teh transakcij zgodi v prvih dveh urah 700 × 550 kb/s × 11, kar znaša skupaj povprečno prenosno hitrost celotnega sistema cca. 5 Mb/s. Večino seveda pomenijo fotografije, ki so pogosto opcijske in bi se prenašale neprioritetno, kar zagotavlja ustrezna logika PNMP.

V primeru uporabe lokalnega strežnika bi se potrebna minimalna hitrost kanala bistveno zmanjšala in sicer na cca. 5 % te kapacitete oziroma na cca 250 kb/s. Tako nizka kapaciteta je posledica optimizacije vseh elementov sistema PNMP.

Za prenos vseh video kanalov bi potrebovali vsaj 20 × 500 kb/s, kar znaša skupaj 10 Mb/s.

Za potrebe video komunikacije lokalni strežnik ne nudi bistvene optimizacije, saj se večina video komunikacije po pričakovanjih porabi na povezavi med lokacijo nesreče in centralnimi službami, se pa seveda aktivira toliko kanalov, kot jih komunikacijsko omrežje zmore.

Skupna potrebna pasovna širina za podporo tako velikega dogodka se torej giblje med 10 in 20 Mb/s, kar je brez težav dosegljivo tako za 4G kot satelitsko tehnologijo.

V primeru razpoložljive višje kapacitete bi se video kanali, uporabljeni v preizkusnem sistemu PNMP zaradi uporabe naprednih adaptivnih protokolov, v nekaj korakih samodejno pohitrili do cca:

- 2 Mb/s za videokonferenčni kanal s kvaliteto HD720 ali
- 4 Mb/s za video opazovalni kanal s HD1080 ali celo
- 12 Mb/s za video opazovalni kanal s kvaliteto 4K, kodek H.265 .

Za te kapacitete satelitska povezava verjetno ne bi več zadoščala, je pa razen v redkih primerih dodana vrednost tega povečanja relativno majhna.

V. ARHITEKTURA STREŽNIŠKIH ELEMENTOV

Za potrebe simulacije delovanja omrežja in doseganje ustrezne robustnosti predvidevamo uporabo distribuiranih strežnikov. Taka arhitektura omogoča ustrezno odzivnost v primeru omejenih prenosnih hitrosti ali občasnem izpadu komunikacije s centrom. Arhitektura strežniškega dela je zasnovana na trojni redundanci, kar pomeni, da trije strežniki z ločenimi bazami podatkov in komunikacijskimi vmesniki delujejo v sinhronizaciji. V primeru izpada steče kompleksen algoritem usklajevanja in nadomeščanja. Velik del, nad 90 % lokalne sinhronizacije mobilnih naprav, ne obremenjuje mobilnega omrežja.

Arhitektura je optimizirana za primere množičnih nesreč, saj omogoča, da se po eden ali dva strežnika postavijo v komandna intervencijska vozila in omogočijo lokalno delovanje tudi brez kakršne koli podatkovne povezave s centrom. Po vzpostavitvi povezave s centrom se podatki med strežniki sinhronizirajo po ustreznem robustnem mehanizmu. Ta sinhronizacija je izjemno učinkovita in potrebuje za svoje delovanje zelo nizke prenosne hitrosti. Čimprejšnja vzpostavitev sinhronizacije je nujna, saj zagotavlja podatke nacionalnim centrom za upravljanje in bolnišnicam, kamor bodo transportirani ponesrečenci.

VI. ZAKLJUČKI

Grobe ocene potrebnih prenosnih hitrosti, ki smo jih za potrebe tega članka pripravili in so seveda potrebne dodatne kritične presoje, kažejo na to, da je tehnologija 4G v povezavi z najnovejšimi tehnologijami WiFi in satelitskim omrežjem prvič dovolj dobra rešitev za vzpostavitev nove arhitekture komunikacijskih povezav za potrebe intervencijskih skupin in v njihovem sklopu služb NMP. Izjemna pokritost ruralnih področij, v čemer je Slovenija med vodilnimi v Evropi in je tudi posledica regulatornih zahtev ob podelitvi frekvenčnega spektra, pomembno izboljšuje uporabnost omenjene rešitve.

Izboljšave, ki jih prinašajo tehnologije LTE Advanced, LTE Pro - najnovejše verzije R12, R13 in R14, so izjemnega pomena in jih je nujno, seveda selektivno, implementirati v slovenskem omrežju 4G. Motivacija za tako implementacijo bi bila v veliki meri lahko komercialna, delno pa tudi regulatorna. Omrežje 5G bi te funkcionalne nadgradnje lahko učinkovito uporabilo.

Tehnologija DMR, ki se uvaja v Sloveniji, je komplementarna, jo je pa nujno uvajati hkrati s primerno robustno implementacijo prenosnih zmogljivosti za povezavo baznih postaj DMR. Ostaja dolgoročni zanesljiv sistem za prenos govora in kratkih sporočil, zgrajen na redundančnih zmogljivostih, ki pa bo lahko bistveno bolj razpoložljiv, če prenos in dostop do množice ostalih podatkov izvedemo digitalno namesto preko povezav, namenjenih prenosu govora.

Tehnologija 5G bo lahko predstavljala pomembno povečanje prenosnih hitrosti in eventualno nadomestila vlogo povezav WiFi na nivoju uporabniških naprav. S tem bi se robustnost bistveno povečala.

Izjemen izziv predstavlja uporaba tehnologije, namenjene IoT. Predvidevamo, da bodo v naslednjih letih na razpolago ustrezne senzorske naprave, ki jih bo možno nadeti pacientom in s tem znotraj prizorišča nesreče spremljati njihovo lokacijo in nekatere njihove življenjske znake. Sistem, ki ga snujemo, je primeren za integracijo takih senzorjev, ki bodo zasnovani na tehnologijah 4G, 4G+ ali 5G. Domet take uporabe presega okvir tega članka.

LITERATURA

[1] Safety First Reinvesting the Digital Dividend in Safeguarding Citizens
[2] Leading the path towards 5G with LTE Advanced Pro
[3] 10 ways LTE Advanced Pro will rede ne mobile networks

ZAHVALE

Zahvaljujemo se vsem, ki so s svojim entuzijazmom, strokovnostjo in vztrajnostjo pripomogli k vzpostavitvi poizkusnega sistema PNMP, predvsem pa Mitji Mohorju, dr. med. in vodstvu Osnovnega zdravstva Gorenjske, ki imajo izjemen posluh za napredek v luči izboljšane možnosti za preživetje žrtev nesreč z uporabo najmodernejše tehnologije.

Franc Dolenc je diplomiral na Fakulteti za elektrotehniko v Ljubljani. V tedanji Iskri Telematiki je zasnoval novo generacijo telekomunikacijskega sistema SI2000, ki je postal eden od izvozno najuspešnejših slovenskih visokotehnoloških izdelkov. Po ustanovitvi podjetja Iskratel je postal direktor za produkte in rešitve. V tej vlogi je povezoval strateško načrtovanje produktne strategije, produktni marketing z vodenjem razvoja v podjetju, ki je skupaj z zunanjimi razvojnimi centri in intenzivnim sodelovanjem z akademsko sfero postalo uspešen regionalni visokotehnološki izvoznik in zaposlovalo blizu 500 vrhunskih inženirjev. Za svoje delo je prejel prestižno Puhovo priznanje. Leta 2009 je ustanovil lastno podjetje Medianteractive, ki se ukvarja z načrtovanjem in razvojem vrhunskih interaktivnih multimedijskih in mobilnih rešitev za sodelovanje in komunikacijo v podjetniških in javnih okoljih.

Varnostna razsežja interneta stvari (IoT)

Uroš Svete, Klemen Kovačič, Fakulteta za družbene vede Univerze v Ljubljani, Katedra za obramboslovje

Povzetek — Informacijsko komunikacijske tehnologije nezadržno spreminjajo naše vsakdanje življenje in že dolgo niso več zgolj delovni pripomoček ali še manj t.i. zabavna tehnologija, temveč postajajo delovno/življenjsko okolje, v katerega so posameznik, družbeni podsistemi in družba v celoti neločljivo integrirani. Internet stvari je brez dvoma tista ločnica, ki je dokončno spojila nekoč dva razmeroma ločena prostora in infrastrukturi, fizično in kibernetsko. In če smo se v obdobju interneta prve in druge generacije še nekako tolažili, da je mogoče preprečiti neposredno varnostno grožnjo, izhajajočo iz kibernetskega prostora, je internet stvari te meje dokončno presekal. Upoštevajoč, da je del interneta stvari implementiran neposredno v človeško telo, pa del interneta postaja neposredno tudi človek. Slednji je tudi v strateškem razumevanju prostora domena, ki postaja vse bolj ključna. V prispevku smo zato izhajajoč iz sodobnih varnostnih teorij in njihovih konceptov, kot je sekuritizacija, preučili varnostna razsežja interneta stvari, pri tem pa se posebej posvetili vzrokom, posledicam in tudi rešitvam omenjenega problema. Pri tem se je še enkrat več izkazalo, da internet v osnovi ni bil zasnovan, da bi bil varen, pač pa trdoživ in nadgradljiv, kar mu je dalo neslutene gospodarske, politične, strateške in varnostne dimenzije.

Ključne besede — internet stvari, varnost, obveščevalne službe, nacionalna varnost, zasebnost

Abstract — Information and communication technology has inexorably changed our every day's life and mightn't have for a long been merely perceived in a way of pure working professional tools or only part of so-called entertainment technology. In opposite it is getting deeply involved in a work / life environment whereby individuals, social subsystems and entire society have become inseparably integrated. Therefore our special attention in the article has been paid to the Internet of Things and its security aspects where without any doubt red thin line was finally crossed and two relatively separate domains and infrastructures, physical and cyber, have been merged into one. And if we have been able in the era of first and second generation of the Internet somehow to prevent direct security threat arising from cyberspace, by the Internet of Things these limits have finally been cut down. Due to the fact the Internet of Things devices could be implemented directly in the human body, mankind is becoming directly a part of the technology. And that's one of the main reasons Internet (of Things) evolves crucial to strategic sphere/domain.

In this article, we are therefore applying the latest security theories and their concepts, such as securitization, for examining IoT security aspects, while specifically focusing on the causes, consequences and solutions to the problem. This has once again proved that the Internet is basically not designed to be safe, but tough, and upgradeable, giving him a huge economic, political, strategic and security dimensions.

Keywords — internet of things, security, intelligence, privacy, national security

I. UVOD

Informacijsko komunikacijske tehnologije nezadržno spreminjajo naše vsakdanje življenje in že dolgo niso več zgolj delovni pripomoček ali še manj t.i. zabavna tehnologija, temveč postajajo delovno/življenjsko okolje, v katerega so posameznik, družbeni podsistemi in družba v celoti neločljivo integrirani. Nesporno dejstvo je, da je predvsem v tehnološko razvitem svetu informacijsko komunikacijska tehnologija vseprisotna in je postala ne samo tehnična, temveč tudi družbena realnost, v kateri živimo. Različne informacijsko komunikacijske tehnologije tako določajo upravne, poslovne, razvojne, varnostne ter druge družbene procese. Želja in privlačnost hitrejšega razvoja pa je družbo pripeljala do točke, ko slednja ni več nosilec razvoja temveč vedno bolj postaja odvisna spremenljivka, ki se razvija in oblikuje glede na razvoj ter tehnične dosežke na področju tehnologije. Sočasno pa prihaja do pojavov, ki predstavljajo tendence k dvojnemu življenju posameznika in družbe, ki danes brez težav, oziroma pogosto celo preveč enostavno prehaja med svojo realno in virtualno oz. oplemeniteno realnostjo. Ravno omenjeno dejstvo pa vse bolj v ospredje postavlja tudi družbene ter etične/filozofske oz. siceršnje družboslovne vidike preučevanja tehnologije (Tripathy, Dutta in Tazivazvino 2016), zato nekateri vizionarji in fiziki kot sta npr. Elon Musk[1] in Stephen Hawking[2] svarijo, da se razvoju tehnologije ne bomo mogli upreti, edino rešitev pa vidita v oblikovanju "svetovne vlade" oz. mehanizma podobnega Organizaciji združenih narodov, ki seveda ne bi bil ujet v pasti blokad omenjene edine v drugi svetovni vojni zasnovane globalne varnostne asociacije. Tovrstni razvoj torej nujno predpostavlja zastavitev nekaterih ključnih družbenih vprašanj vezanih na prihodnjo družbeno, politično in ekonomsko ureditev, prav tako pa bo potrebno na novo določiti, kako v takšni družbi zagotavljati uravnotežen gmotni in duhovni razvoj, kar je ena temeljnih funkcij varnostne teorije in njene operacionalizacije v obliki varnostnih politik in instrumentov. "Napredne" tehnologije omogočajo namreč absolutno udobje/ugodje življenja posameznika na račun možnosti absolutnega nadzora nad svojim okoljem, v bližnji prihodnosti tudi nad svojim telesom. Bailey (2016) v izjemno zanimivi analizi, zakaj in kako nas tehnologija zapeljuje, ugotavlja, da se navkljub vse številnejšim opozorilom o zlorabah vse več uporabnikov odloča za vstop v "neznan svet". In to iz dveh popolnoma različnih razlogov. Prva skupina se ne zaveda pasti in tveganja, ki ga prinaša nova, nepreizkušena in varnostno tvegana tehnologija, druga skupina pa ne želi zamuditi vlaka, je izjemno nepotrpežljiva ter vedno želi biti trend setter.

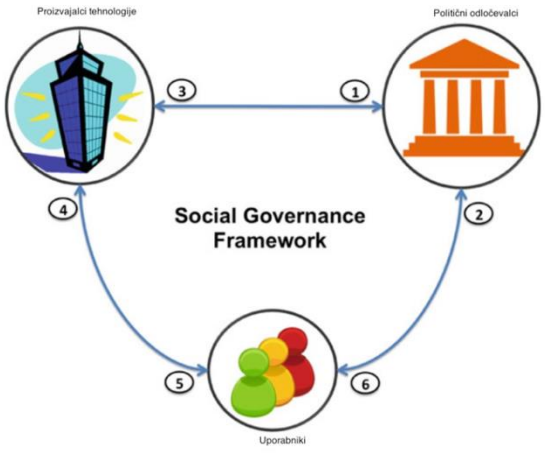
Smilansky (2016) zato opozarja na potrebo po uravnoteženosti med ugodnostmi za uporabnike (tako posameznike kot podjetja) in varnostnimi zagotovili. Pri tem je revolucija "interneta stvari" na žalost precej drugačna v

[1] "Deep artificial intelligence, or artificial general intelligence, where you can have artificial intelligence that is much smarter than the smartest human on Earth, this is a dangerous situation".

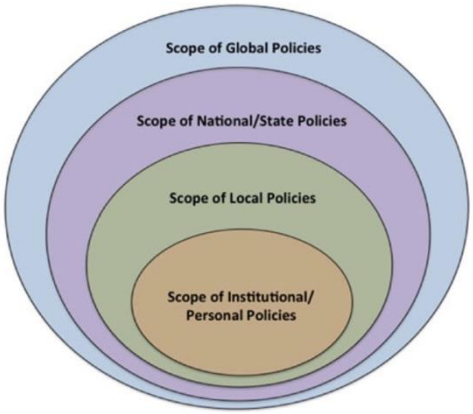
[2] Without a 'world government' technology will destroy us (Stephen Hawking) (http://www.independent.co.uk/life-style/gadgets-and-tech/news/stephen-hawking-world-government-stop-technology-destroy-humankind-th-a7618021.html)

primerjavi z ostalimi revolucijami, kot so npr. socialna omrežja, ki so v zgodnjih fazah razvoja omogočala podjetjem "umik iz uporabe" oz. je bilo mogoče nadzorovati, katere podatke se bo objavljalo in na kakšen način. Potencialno hekiranje varnostnih kamer, avtomobilov, hišnih vrat pa ima takojšnje in neposredne učinke na varnost posameznika, podjetja, ključne infrastrukture in v končni posledici družbe v celoti (Ghani in ostali 2014).

Med naprednimi informacijsko-komunikacijskimi tehnologijami, ki imajo gotovo enega izmed najboljših razvojnih potencialov, je torej brez dvoma t.i. internet stvari, ki poleg računalniških združuje tudi neračunalniške elemente v enotno internetno platformo. Pričakuje se, da bo v naslednjih 5 letih tako povezanih 50 milijard naprav, pri tem pa so ključni dejavniki razvoja na tem področju Electronic Product Code Global (EPCGlobal), Wireless Highway Addressable Remote Transducer (WirelessHART), ZigBee, Near Field Communication (NFC), IPv6 over Low power Wireless Personal Area Network (6LoWPAN), in Developers' Alliance for Standards Harmonization (Roy in Manoj 2016, 449). Čeprav je termin internet stvari (Internet of things oz. IoT) prvi uporabil Kevin Ashton že leta 1999, pa šele danes lahko vidimo, kako silni revolucionarni potencial ima, po drugi strani pa bodo tehnološki preboji zahtevali tako povečano učinkovitost računalniških zmogljivosti, varne brezžične komunikacije, podaljšanje delovanja baterij oz. virov energije, kot razvoj aplikacij in nenazadnje integracijo v obstoječa omrežja ter (industrijske) produkte. Obenem pa se bo od uporabnikov zahtevalo, da "omogočijo vstop" tovrstne tehnologije v svoja tako profesionalna kot zasebna življenja. V končni fazi pa se bo morala tehničnim rešitvam poleg uporabnikov prilagoditi tudi zakonodaja, ki je zaenkrat še velika ovira, po svojem bistvu pa tudi vedno konzervativnejši družben element. Danes se zdi, da družbe na področju interneta stvari nimajo celovite in osredotočene politike ter so zato razpete med tehnološke inovacije, pritiske na potrošnike in vse številčnejše zlorabe, ki dodatno zapletajo varnost v informacijski družbi. Zato Bailey (2016, 1054) predlaga, da bi morali politični odločevalci sprejeti bolj paternalistično zakonodajo, s katero bi prisilili proizvajalce tehnologije, da več pozornosti namenijo varnosti. Misra in drugi (2016, 55) pa izpostavijo ključen trikotnik med političnimi odločevalci, proizvajalci in uporabniki tehnologije (glej sliko 1) na vseobsežni ravni, od posameznika do globalne skupnosti.



Slika 1: Okvir družbenega vladovanja v primeru interneta stvari (Misra, Maheswaran in Hashmi, 2016, 55)



Slika 2: Ravni politik, pomembnih za regulacijo interneta stvari (Misra, Maheswaran in Hashmi, 2016, 56)

V kolikor so bila daljinsko vodena vrata pred dobrim desetletjem za povprečnega državljana višek tehnike, danes daljinsko vodene naprave, povezane z različnimi krmilnimi sistemi, predstavljajo relativno vsakodneven pojav, Plačevanje storitev s pomočjo mobilnega telefona, nadzor okoljskih parametrov (temperatura, vlažnost, osvetlitev) v bivanjskih prostorih na podlagi prednastavljenih zahtev in upravljanih s pomočjo centralnega krmilnega sistema ter možnostjo upravljanja na daljavo preko internetne povezave niso več fikcija hollywoodske filmske industrije, temveč zgolj vprašanje finančne zmožnosti posameznika in njegovega interesa pri uporabi različnih tehničnih rešitev. Internet stvari, pametne naprave in druge sorodne tehnologije pa imajo za osnovo lastnega delovanja zgolj eno skupno značilnost – nadzor oziroma možnost upravljanja na daljavo, bistveno skrajševanje odločevalskega cikla ter možnost napovedovanja. Ob tem pa nujno trčimo na možnost zlorabe tovrstnih tehnologij v namene, ki niso več stvar zagotavljanja udobnega življenja posameznika in skupnosti, temveč se izrodijo v svoje nasprotje v interesu kapitala in politične moči, ko vladajoče (tehnološke) skupine začnejo uporabljati tovrstne tehnologije za "daljinsko upravljanje" družbe in njenih posameznikov za potrebe zagotavljanja lastnega privilegiranega položaja. Uporaba informacijskih tehnologij in vključujoč internet stvari na eni strani, ki seveda omogoča ekonomski napredek pri razvoju posamezniku prijaznejših delovnih mest v smislu izogibanja izpostavljenosti nevarnemu delovnemu okolju, vendar pa na drugi strani iste tehnologije omogočajo bistveno učinkovitejši nadzor delodajalca nad delavci in njihovim ravnanjem, da ne omenjamo pasti izginjanja številnih poklicev in delovnih mest ter zahteve po prilagajanju, ki so za vse številnejše posameznike glavni vir stresa. To z vidika delovnega procesa niti ni sporno, dokler ne začne posegati v pravico do zasebnosti in posameznikove integritete. Na drugi strani pa internet stvari s svojo nadzorstveno funkcijo omogoča uravnavanje različnih parametrov naravno-družbenega kompleksa na način, da omogoča večjo stopnjo trajnosti, saj zagotavlja možnost uravnavane porabe nekaterih ključnih naravnih virov na optimalnejši način, kot je na primer manjša poraba goriva na račun pametnega uravnavanja ogrevanja, pametni transport (npr. Car sharing, Uber, samovozeča vozila in ostale implementacije IKT v avtomobile), lažjo izrabo alternativnih virov na račun možnosti lažjega izmenjavanja virov, urejeno delovanje bivanjskega okolja glede na

zaznavanje prisotnosti posameznika – avtomatsko prižiganje in ugašanje luči, televizije na zaznavanje prisotnosti in drugi energijsko varčevalni ukrepi. Namen naše razprave vsekakor ni kakršnekoli poskus nepotrebne sekuritizacije interneta stvari, pač pa zgolj ponovno izpostaviti, da nobena tehnologija, ki je bila razvita v človeški zgodovini, ni sama po sebi dobra ali slaba, vsaka uporaba je torej odvisna od narave človekove narave in da mora biti vsaka tehnologija družbeno kontekstualizirana. In tej bomo morali v bližnji prihodnosti posvetiti vse več pozornosti.

II. SEKURİTİZACİJA İNTERNETA STVARİ

K širšemu razumevanju varnosti je gotovo prispevala tudi sekuritizacija, kot eden pomembnejših analitičnih instrumentov**,** ki jo v varnostno teorijo vpelje Kopenhagenska šola. Sekuritizacija je namreč proces, v katerem se viri ogrožanja oz. ranljivosti varnostno problematizirajo (sekuritizirajo) ter vzpostavijo mehanizmi učinkovitega in aktivnega odgovora nanje. Njen glavni cilj je analitična razlaga, zakaj politične elite v odločevalskem procesu določene družbene procese in dogodke obravnavajo kot (nacionalnovarnostne) grožnje ter v tem okviru vzpostavijo specifične odgovore nanje, ki so lahko tudi v nasprotju s tradicionalnimi normami in pravili (Grayson, 2003). Koncept sekuritizacije je zato neločljivo povezan s širjenjem varnostne razprave, tako v smislu referenčnih objektov varnosti kot mehanizmov in instrumentov za njihovo zagotavljanje. Po drugi strani pa se ravno na področju kibernetske varnosti vse več avtorjev sprašuje ali ni diskurz v pretirani pozornosti posvečeni varnostnim dimenzijam uporabe informacijsko-komunikacijske tehnologije ter kot protiutež razvijajo koncept inflacije groženj oz. prekomerne sekuritizacije (Brito in Watkins 2011)[3]. Čeprav se bomo v nadaljevanju posvetili konkretnim empiričnim primerom, kako lahko internet stvari obravnavamo kot grožnjo tako informacijski, posameznikovi kot nacionalni varnosti in se zavedamo sekuritizacijske dileme, bomo v začetku analize pozornost posvetili tudi kratkemu pregledu literature, ki obravnava varnostne implikacije interneta stvari. Burt (2016) tako opozarja, da je z izjemnim naraščanjem števila naprav, vključenih v internet, naraslo tudi varnostno zanimanje predvsem za njihove zlorabe, precej manj pa so po njegovem mnenju za varnost zainteresirani tako proizvajalci, ki v tem vidijo dodatni in nepotrebni strošek, kot uporabniki, ki se bojijo zapletenosti uporabe. Tak odnos po mnenju avtorja lahko vodi v apokalipso z neslutenimi posledicami. Kot bomo prikazali v nadaljevanju prispevka, kot veliko grožnjo interneta stvari percipirajo predvsem obveščevalne službe, ki se bojijo, da bi po eni strani kriminalci in teroristi lažje prikrili svoje delovanje v kibernetskem prostoru, po drugi strani pa bi poleg nedržavnih tudi državni akterji lahko izkoristili internet stvari za nadzorovanje, zasledovanje, pridobivanje geolokacijskih podatkov, organiziranje delovanja ter rekrutiranje novih podpornikov. Še posebej pa je zaskrbljujoče vse večje zaupanje sistemom umetne inteligence (Artificial intelligence AI), oplemenitene (augmented) in navidezne resničnosti (virtual reality).

Zato Scardilli (2014) predlaga naslednje varnostne ukrepe:

- uporabo močnih gesel, redno posodabljanje protivirusnih in drugih zaščitnih programov;
- izvedbo pregleda naprav, ki so potencialno ranljive na napade (vse, ki so povezane v internet, četudi nimajo zaslona ali tipkovnice);
- preveriti, ali je požarni zid vklopljen in pravilno konfiguriran;
- po nakupu naprave takoj onemogočiti daljinski nadzor nad njo in spremeniti privzeto geslo;
- na proizvajalčevi spletni strani sneti najnovejšo programsko opremo;
- razmišljaj kot heker - naredi analizo groženj od koder lahko le-te pridejo;
- preden objavite osebne podatke na spletu, ugotovite, kaj bo prejemnik z njimi počel in kako jih bo zaščitil;
- online objaviti le najnujnejše informacije;
- prodajalci varnostnih rešitev naj napravijo enostavne produkte, ki bodo prilagojeni načinom, kako se uporabniki vedejo;
- pomembna je varnostna higiena in procesi, na kakšen način se torej varnostni produkti distribuirajo do uporabnikov.

Zelo pomembno ugotovitev problematičnosti interneta stvari v varnostnem smislu pa lahko najdemo tudi v članku, ki so ga napisali Li, Tryfonas in Li (2016). V njem izpostavljajo ekosistemsko odprtost interneta stvari, ki je pogoj, da se vanj vključi čim več uporabnikov s čim več napravami. Zato je po njihovem mnenju internet stvari pravokoten na ostala raziskovalna področja. Ravno njegova izjemna raznolikost pa je hkrati tudi razlog ranljivosti v smislu dostopnosti, storitvene integritete, varnosti in zasebnosti. Prav tako pa je internet stvari, še posebej na spodnji plasti t.i. senzorike, zmogljivostno zelo podhranjen, saj omejena računska zmogljivost ter energetske zagotovitve onemogočata dobro varnostno zagotovitev. Na srednji plasti (omrežja) pa je internet stvari odvisen od komunikacij, ki omogočajo prestrezanje ter DDoS napade. Zato se mora najvišja raven (aplikacij) pokazati kot sposobna rešiti vse varnostne probleme, kar pa je v številnih primerih, ki jih bomo obravnavali v nadaljevanju, praktično nemogoče.

III. EMPİRİČNİ PRİMERİ VARNOSTNİH İMPLİKACİJ İNTERNETA STVARİ: OD GROŽENJ İNFORMACİJSKİ DO GROŽENJ NACİONALNİ VARNOSTİ

A. Informacijska in osebna varnost

Uporabniki od kupljenih stvari pričakujemo, da bo upravljanje z njimi enostavno in da bodo delovale brez problema, ko jih enkrat vklopimo in omrežimo. S tem posamezniki kot kupci izkazujemo zaupanje do samih izdelovalcev strojne in programske opreme, ki je na neki napravi nameščena. Navsezadnje jim zaupamo praktično vse, kar imamo, od bančnih kartic do osebnih fotografij, avtomobilov itd; to zaupanje pa kot kupci in uporabniki gojimo brez zadostnega zavedanja, da lahko zgolj z uporabo v internet povezane stvari pride do grožnje tako posamezniku in njegovi zasebnosti kot tudi do grožnje družbi, organizacijam, državi in njihovim informacijskim sistemom.

[3] Tudi na področju interneta stvari se v članku 'Don't Believe the Car Hacking Hype' (2015) strokovnjak za avtomobilizem Doug Newcomb sprašuje o smiselnostmi pretiranih zgodb o nevarnosti hekiranja avtomobilov in pri tem navede podatek, da je razen hekanja v raziskovalne in publicistične namene poznan samo en primer tovrstnega napada na avto.

Od interneta stvari pričakujemo, da nam bosta njihova uporaba in medpovezljivost omogočila lažje življenje, enostavnejše izvajanje vsakodnevnih aktivnosti in da nam bo obenem zagotovljeno nemoteno in varno delovanje samih sistemov kot takšnih.

Povezovanje stvari v zasebna omrežja in medmrežje omogoča njihovo preprostejšo uporabo, hkrati pa odpira vrata novim grožnjam, ki izhajajo iz kibernetskega prostora. Tam delujejo kriminalne skupine, teroristične organizacije, hektivisti in navsezadnje tudi države preko nacionalnovarnostnih struktur[4]. Vsi ti akterji iščejo nove načine doseganja svojih interesov v kibernetskem prostoru. Ker omogoča internet stvari razširitev tradicionalnih informacijskih dejavnosti pridobivanja informacij, sredstev, podpornikov in politične ali ideološke moči, predstavlja tudi primeren cilj.

Internet stvari je relativno mlada tehnologija, ki se srečuje z varnostnimi problemi. Proizvajalci teh tehnologij poskušajo uporabiti že obstoječo tehnologijo in jo združiti s stvarmi na način, da bo njihova uporaba lažja. Zaradi integracij, ki se dogajajo, se ponovno pojavijo sistemske ranljivosti ali pa nastanejo nove, ki so lahko izrabljene za izvedbo napada. Vse omrežene naprave, tudi naprave interneta stvari, je danes ob uporabi iskalnikov odprtih TCP/UDP vrat in programov za ugotavljanje operacijskih sistemov mogoče odkriti. Nekateri iskalniki naprav so dostopni prek spletnih strani, kot je Shodan (Shodan 2017) ali prek specializiranih programov, kot na primer NMAP (NMAP 2017) in omogočajo odkrivanje naprav interneta stvari, procesov, ki na njih potekajo, in njihovih ranljivosti. Ti programi omogočajo napadalcem, da v kibernetskem prostoru odkrijejo takšne naprave in pridobijo dovolj informacij, da jih izrabijo. Po podatkih Gartnerjevega raziskovalnega in informacijskega centra je danes le ena od desetih naprav interneta stvari ustrezno zaščitena (Gartner 2017), kar še dodatno olajša delo napadalcev, ko skušajo pridobiti dostop do teh naprav in z njimi upravljati.

Te ranljivosti in šibka zaščita so pričele postajati širši problem s pojavom prvih javno dostopnih ali nejavnih izrab ranljivosti (exploitov), kasneje pa s pojavom prvih IoT-botnetov. IoT-botneti ali botneti naprav interneta stvari so omrežja okuženih naprav IoT in napadalčevih poveljniških naprav, ki so namenjeni za izvajanje napada za zavrnitev storitev, pošiljanja nezaželene pošte, iskanja novih naprav in širjenja okužb ter nadzora nad okuženimi napravami, vse to brez vedenja uporabnikov naprav (Fisher 2013; Kaspersky 2017).

Prvi IoT-botneti so se začeli pojavljati leta 2014, ko je število okuženih naprav interneta stvari obsegalo od samo 100 do kar 75-tisoč naprav. Nezaščitenost ali šibka zaščita naprav IOT omogoča napadalcem, da se povežejo in jih izrabijo kot dostopno točko za izvedbo napada s posrednikom (MITM) za zbiranje informacij o preostalih napravah na omrežju, pošiljanje nezaželene e-pošte ali uporabo za izvedbo napada za zavrnitev storitve (DDOS) (Arbor Network 2017).

Zlonamerna programska oprema in tržišče z botneti se je od leta 2014 pričelo pospešeno razvijati, saj napadalcem vdor v naprave interneta stvari ne predstavlja možnosti dodatnega zaslužka, omogoča pa jim izgradnjo velikih omrežij ugrabljenih naprav. Razvoj in uporaba te zlonamerne programske opreme je privedla do izoblikovanja zloglasnega »Mirai«-botneta, ki je zajemal med 72 in 120 tisoč ugrabljenih naprav za izvedbo napada za zavrnitev storitve DDOS (Krebs 2016a).

Mirai-botnet je postal budnica za informacijske varnostne strokovnjake, saj je uspel v več napadih onemogočiti delovanje večjega števila spletnih mest in strežnikov. Napad, ki je povzročil največ škode, je bil usmerjen proti korporaciji Dyn in njeni informacijski infrastrukturi. Tarča napada so bili strežniki Dyn DNS, ki so odgovorni za domene spletnih mest in določajo informacije o njih. Z uspešno izvedenim napadom za zavrnitev storitev (DDOS) so napadalci z Mirai-botnetom generirali do 1,2 terabitov na sekundo, kar je onemogočilo uporabnikom, da se povežejo do željenih spletnih mest (Loshin 2016).

Mirai-botnet je bil namensko sestavljen izključno iz naprav interneta stvari, ki so imeli odprte povezave na splet ter šibka ali privzeta gesla. Ta gesla so hekerji ali njihovi botneti napadli z ugibanjem oziroma napadom s silo (brute force attack). Napadalci so uporabljali 68 parov privzetih gesel, ki so jim omogočila dostop do naprav. Najbolj pogoste naprave, uporabljene v napadu, so bile CCTV IP kamere, digitalni videorekorderji, brezžični usmerjevalniki, tiskalniki in druge, podobno neprimerno zaščitene naprave. Napadalec je ob vdoru v napravo tudi preprečil lastniku spreminjanje nastavitev in je tako nad napravo lahko prevzel popoln nadzor (Krebs 2016a; Krebs 2016b).

Uspešnost takšnih napadov lahko onemogoči delovanje spleta. Ravno zaradi tega je potrebno veliko bolj aktivno pristopiti k oblikovanju varnostnih sistemov za vse naprave, ki so povezane na splet. Mirai-botnet je bil v času svojega delovanja eden večjih botnetov, vendar kljub vsemu ne največji. Problem nastane, ko se javno objavi zlonamerna programska oprema in ko postanejo dostopna tudi sama navodila za izoblikovanje lastnega botneta, kar se je v primeru te zlonamerne programske opreme zgodilo. Tako samo znanje o oblikovanju IoT-botneta ni bilo več v le rokah njegovih avtorjev. Ti so znanje z objavo na internetu predali naprej, kjer ga je lahko našel (in uporabil) praktično vsakdo, ki se je za to zanimal. Seveda se je najbolj razširilo med ljudmi, ki so imeli željo izoblikovati lastna orodja za povzročanje varnostnih incidentov in kibernetskih napadov ter so posedovali sredstva za ohranjanje takšnih botnetov pri življenju (Cimpanu 2016).

Objavljanje zlonamerne programske opreme Mirai pa je povzročilo tudi oblikovanje drugih botnetov in nastanka novih variacij botneta. V času pisanja tega prispevka je bilo aktivnih vsaj 14 Mirai-botnetov, ki si jih je mogoče tudi izposoditi za izvedbo napada za zavrnitev storitev. Cena Mirai-botneta za 100,000 ugrabljenih pametnih naprav je odvisna od ponudnika, vendar se giblje med 7,500 in 10,000 dolarji za nekajdnevni napad (Cimpanu 2016; Condliffe 2016).

Nove oblike napadov na naprave interneta stvari lahko uporabljajo spremenjeno zlonamerno programsko opremo Mirai, ki nosi dodaten ukaz, ta pa popolnoma onemogoči pametno napravo in izvede napad trajne zavrnitve storitev (PDOS). Bricker-bot, kot so ga poimenovali strokovnjaki, ob vdoru v napravo interneta stvari zasede celoten pomnilnik in spreminja podatke na trdih diskih. Ob tem napad istočasno

[4] Mnoge med njimi vse bolj odkrito priznavajo, da organizirajo namenske strukture za delovanje v kibernetskem prostoru, ena zadnjih je bila tako Nemčija (http://www.dw.com/en/german-army-launches-new-cyber-command/a-38246517), Velika Britanija pa je bila ena prvih držav, ki je priznala tudi razvoj ofenzivnih zmogljivosti (https://www.ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de).

izbriše tudi programsko opremo in s tem onemogoči delovanje samih naprav interneta stvari (Radware 2017). Vendar zlonamerna programska oprema Mirai in njene variacije niso edini botneti, ki napadajo naprave interneta stvari. Poleg te obstaja še veliko drugih zlonamernih programskih oprem in botnetov, ki poskušajo pridobiti na moči z izgradnjo večjega omrežja ugrabljenih naprav, kot so Qbot, Leetbotnet, Amneisa in njihove druge variacije, vendar obstajajo tudi izjeme, ki poskušajo preprečiti vdor napadalcem s tem, da pridobijo dostop do naprave in na njej odpravijo ranljivost, primer takšnega botneta pa sta Hajime in Wifatch (Goodin 2017).

Napadalci ne poskušajo izrabiti naprav interneta stvari le za oblikovanje armad okuženih naprav, ki lahko opravljajo napade zavrnitev storitev, ampak vse več poskušajo izrabiti predvsem varnostne luknje, ki jih te naprave oblikujejo (All things considered 2016). Vse več napadalcev poskuša z dostopom do šibko zaščitene ali nezaščitene pametne naprave pridobiti dostop do notranjih sistemov, saj naprave interneta stvari v večini primerov ne omogočajo uporabe resnejših varnostnih mehanizmov za njihovo zaščito (Savage 2016). Čeprav se v nekaterih primerih pojavljajo naprave, ki uporabljajo vgrajene varnostne mehanizme, se v njih pojavljajo druge ranljivosti. Protokoli in podatkovne povezave, ki jih uporabljajo nekatere naprave interneta stvari, potekajo po zavarovanih in šifriranih povezavah (kot je ZigBee), vendar lahko vsaka nova naprava, ki se poveže v omrežje pametnih stvari, pridobi nešifriran ključ od preostalih naprav, da lahko prične s šifrirano komunikacijo (InfoSec Institute 2015).

V primeru, da je nova povezana naprava interneta stvari okužena z zlonamerno programsko opremo, se lahko ta prične širiti prek šifrirane podatkovne povezave in omogoči napadalcu, da izrablja in upravlja naprave, kot je bilo prikazano s Philipsovimi pametnimi žarnicami (Ronnen et al. 2016; Pauli 2016). To predstavlja dodatno nevarnost za naše domove in druga okolja, v katerih so naprave interneta stvari vgrajene, saj lahko v primeru takšnega napada omogočijo tudi fizičen vdor in posledično škodo (Palmer 2016). Primer takšnega napada je bil že izveden in lahko pričakujemo, da bodo na podoben način napadalci poskušali vplivati na naprave interneta stvari tudi v prihodnje, predvsem zaradi njihove šibke zaščite ter vse večje popularnosti tako imenovanih »pametnih stvari«.

Strokovnjaki na področju informacijske varnosti opozarjajo, da se število povezanih naprav interneta stvari vsakodnevno povečuje. In ravno zaradi njihovega vse večjega števila lahko pričakujemo tudi vse več kibernetskih napadov, ki bodo izvedenih na te naprave in iz njih. Po podatkih Gartnerjevega raziskovalnega in informacijskega centra, naj bi bilo do leta 2020 25-odstotkov vseh kibernetskih incidentov povezanih z vdorom v napravo interneta stvari ali uporabe naprav interneta stvari za izvajanje napada za zavrnitev storitev (Gartner 2017).

B. Internet stvari in obveščevalna dejavnost

Tako kibernetski kriminalci kot tudi organizacije za obveščevalno dejavnost iščejo nove načine pridobivanja informacij. Kibernetski prostor predstavlja odlično okolje, kjer uporabniki vsakodnevno objavimo velike količine bolj ali manj prosto dostopnih podatkov. S pojavom in pričetkom uporabe naprav interneta stvari pa smo omogočili širjenje kibernetskega prostora v vse stvari, ki jih danes uporabljamo. Po podatkih Gartnerjevega raziskovalnega in informacijskega centra je danes aktivnih 6,8 milijard naprav interneta stvari. Nekateri strokovnjaki pa napovedujejo, da bo to število zraslo do 20 (Gartner 2017) ali celo 75 milijard (Danova 2013) do leta 2020. Zaradi enostavne uporabe in vse nižjih cen postajajo te naprave zelo popularne in jih vgrajujemo v lastne domove in druge objekte. Internet stvari je zaradi svojih sposobnosti in velikega števila naprav povezanih na splet primerna tarča za obveščevalne organizacije in službe, saj lahko z njimi pridobijo vpogled v naše življenjsko okolje, posegajo v zasebnost ali zbirajo informacije o našem delu in življenju.

Internet stvari in njegove naprave so povezane na splet 24 ur na dan in 7 dni na teden, pri čemer jih uporabniki ne izklapljamo, saj jih razumemo kot varne in se nam aktivne zdijo veliko bolj uporabne. Kamere, luči, ključavnice in tudi kompleksnejši pametni sistemi, kot so avtomobili, industrijska tehnologija in razni senzorji imajo povezavo na splet, obenem pa razpolagajo z informacijami, kot so geolokacija, podatkovna povezava, slikovno in glasovno gradivo ter industrijski in drugi podatki, ki so lahko za obveščevalne organizacije izjemnega pomena.

Obveščevalne organizacije lahko razdelimo na dva tipa: prve organizacije so v službi držav, druge pa so civilne, z državo nepovezane, namenjene zbiranju informacij o svojih konkurentih na tržišču, ki poskušajo svoji matični organizaciji zagotoviti konkurenčno ali drugačno prednost pred ostalimi. Zato lahko razumemo obveščevalno dejavnost iz zornega kota nacionalne varnosti in varovanja tajnih podatkov, na drugi strani pa kot korporativno varnost in zaščito organizacijskih tajnih podatkov. V današnjem svetu se področja delovanja obveščevalnih organizacij vse bolj povezujejo, saj informacije z enega področja hitro potujejo v druga. Ekonomske, politične, vojaške in druge informacije imajo veliko vrednost v današnjem času in obveščevalne, tako komercialne kot državne organizacije, poskušajo z njimi trgovati ali z njihovo pomočjo pridobiti prednost pred nasprotniki.

Korporativna varnost se prične z zaščito pred konkurenti na tržišču, kjer ti želijo pridobiti dostop do informacij organizacije, ki bi jim lahko predstavljale prednost v delovanju na trgu in boju za profit. Velike organizacije razpolagajo s fizičnimi, pravnimi in informacijskimi varnostnimi sistemi, da se zaščitijo pred zunanjimi akterji ogrožanja. Ti varnostni sistemi so lahko oblikovani večstopenjsko in odlično opravljajo delo zaščite informacijske infrastrukture, organizacije ali posameznika, vendar lahko posameznik to varnost drastično zmanjša s priklopom naprav interneta stvari, ki so slabo zaščitene ali sploh niso (Savage 2016). Po podatkih analize Pwnie Express (2017) 66-odstotkov informacijskih strokovnjakov ne ve, kaj vse uslužbenci na delovnem mestu priklopijo na omrežja in kolikšno varnostno tveganje te naprave predstavljajo. Varnostne luknje, ki s tem nastanejo, lahko povzročijo odtekanje občutljivih informacij, ki lahko posledično povzročijo finančno in škodo na ugledu organizacije, ter izgubo konkurenčne prednosti pred ostalimi. Nevarnost, ki jo nezaščitene naprave interneta stvari predstavljajo, niso več fiktivne. Po podatkih Pwnie Express (2017) analize (*The internet of evil things*), se je 16-odstotkov informacijskih varnostnih strokovnjakov že srečalo z vdori in napadi s posrednikom skozi IoT, 22-odstotkov pa se je na delovnem

mestu srečalo z izsiljevalskimi virusi, ki so onemogočili delovanje naprav interneta stvari (Pwnie Express 2017).

Varnost posameznika in družbe se zagotavlja skozi državne sisteme, ki so namenjeni za zmanjševanje tveganja in implementacijo varnostnih sistemov za preprečitev groženj in napadov. Informacijska varnost delovanja državnih sistemov je ena od bolj ogroženih dimenzij, zaradi pojava državno sponzoriranih ali državnih skupin in organizacij, ki se ukvarjajo le s tem. Njihovo delo je pridobivanje informacij o državah, problemih, s katerimi se srečujejo, ter njihovimi interesi in strategijami. Sofistikacija njihovega delovanja presega vse civilne hekerske in kibernetske kriminalne skupine, kar že samo po sebi predstavlja nevarnosti za informacijsko infrastrukturo države. Ob tem se pojavi vprašanje, kako varne so naprave interneta stvari pred napadi tujih obveščevalnih organizacij in kako jih je mogoče bolje zaščititi in s tem onemogočiti dostopnost do občutljivih podatkov napadalcem.

Obveščevalne organizacije Združenih držav Amerike so prve odkrito izrazile zanimanje za naprave interneta stvari, saj so v njih prepoznali orodje za opravljanje obveščevalne dejavnosti. Njihov optimizem temelji na podobnih sistemih medpovezanih naprav, ki so že bili uporabljeni pred razcvetom komercialnih naprav interneta stvari. Ti kompleksni sistemi medpovezanih naprav so bili namenjeni za uporabo v oboroženih silah in obveščevalnih organizacijah, saj so omogočali hiter način prenašanja informacij in razumevanja bojišča za namene poveljevanja in kontrole oboroženih sil (Wind 2015). Hiter prenos informacij, specializacija za civilno uporabo, miniaturizacija ter želja po enostavni uporabniški izkušnji, pa je omogočilo širitev le-te v naše domove.

Širitev omreženih naprav v naš vsakdan je v obveščevalnih organizacijah povzročila zanimanje za njihovo izrabo za olajšano opravljanje lastnih nalog. Leta 2012 je v svojem govoru na srečanju korporacije In-Q-Tel takratni direktor ameriške Centralne obveščevalne agencije CIA general David Petraeus izpostavil probleme interneta stvari, saj lahko povzročijo nove grožnje nacionalni varnosti in posamezniku, obenem pa predstavljajo odlična orodja za pridobivanje informacij o ljudeh, skupinah in stvareh, njihovi lokaciji, identifikaciji in nadzoru (Ackerman 2012). Direktor ameriške Obrambne obveščevalne agencije DIA James R. Clapper je v svojem poročanju senatu Združenih držav, štiri leta kasneje (2016), predstavil problematiko interneta stvari in njihovo vse hitrejše širjenje v vse ravni našega življenja. Poudaril je, da naprave interneta stvari omogočajo večjo učinkovitost, varčnost, enostavno uporabniško izkušnjo in ekonomsko rast. Ampak ob tem se pojavljajo tudi grožnje, povezane z novo tehnologijo, ki lahko ogroža zasebnost, integriteto podatkov in informacij ter kontinuiteto storitev. Po njegovem mnenju bodo v prihodnje obveščevalne organizacije skušale uporabiti naprave interneta stvari za identificiranje, nadzorovanje, spremljanje lokacije, rekrutiranje lastnikov teh naprav ter pridobivanje dostopa do omrežij ali uporabnikovih podatkov (Clapper 2016).

Napadalci in vse bolj tudi obveščevalne organizacije iščejo in ciljajo na sisteme z najšibkejšo obrambo za pridobivanje dostopa do širših sistemov, kar naredi internet stvari za še toliko bolj primerno tarčo. Tehnologija interneta stvari je lahko izrabljena za poseganje v zasebnost državnih odločevalcev ali zbiranje informacij o političnih strateških načrtih in njihovih sredstvih doseganja. Vsaka nova ranljivost lahko omogoči napadalcem, ki imajo znanja, motivacijo in sredstva, kot jih imajo obveščevalne organizacije, veliko enostavnejšo delo dostopanja do teh informacij.

Obveščevalne organizacije bodo poskušale pridobiti dostop do različnih naprav interneta stvari z namenom pridobivanja informacij o njenih uporabnikih, kar močno posega v posameznikovo zasebnost. Vendar samo profiliranje uporabnikov ni toliko v interesu obveščevalnih organizacij, razen če te razpolagajo z občutljivimi informacijami. Ti uporabniki največkrat zajemajo politične ali ekonomske odločevalce in druge interesne osebe, ki imajo dostop do občutljivih informacij, obenem pa bodo obveščevalne organizacije poskušale ohranjati dostop do informacijskih in drugih sistemov, ki jih ti uporabljajo.

Državne organizacije svoje delovanje prenašajo na splet, ker ta omogoča hitro informiranje širše javnosti kot tudi opravljanje storitev tako za uporabnike kot tudi za lastne potrebe. Različni senzorji, ki so namenjeni spremljanju stanja na terenu, so sestavni del interneta stvari, saj so namenjeni povezovanju sistemov na terenu s kontrolnimi centri in pravočasnemu obveščanju o stanju infrastrukture, območij in zraka. Napadalci in obveščevalne organizacije lahko zato veliko lažje dostopajo do informacij svojih tarč iz katerekoli točke na spletu ter svetu in lahko te podatke izrabljajo za analizo delovanja državnih organizacij in stanja na terenu. S sledenjem, vdori in prestrezanjem informacij lahko bolj učinkovito izoblikujejo lastne odgovore in strategije na delovanje in obnašanje države, tako doma kot v mednarodni skupnosti.

Internet stvari omogoča vsem obveščevalnim akterjem v današnjem svetu, da pravočasno in bolj učinkovito priredijo svoje delovanje na podlagi zbranih informacij. Zato je pomembno omeniti, da se obveščevalna dejavnost izvaja tudi znotraj držav za namene uspešnega preganjanja kriminala in terorizma. Državni organi pregona poskušajo z obveščevalno dejavnostjo zbrati dovolj informacij o kaznivih dejanjih posameznikov ali skupin, da tem preprečijo delovanje, jih nadzorujejo ali kazensko preganjajo za zagotavljanje širše varnosti družbe, države in mednarodne skupnosti. S tem lahko internet stvari omogoča odlično orodje za organe pregona, vendar le, če te delujejo v skladu z zakoni in usmeritvami, ki so določene, in ne posegajo v posameznikovo zasebnost.

Kot primer izrabe interneta stvari lahko omenimo objave orodij Centralne obveščevalne agencije ZDA, ki jih je izvedel Wikileaks v svojem poročilu, imenovanem Vault 7, 7. marca 2017. V njem so opisana orodja, ki jih je izoblikovala CIA z namenom izvajanja obveščevalne dejavnosti in so bila usmerjena proti uporabnikom naprav interneta stvari, kot so pametni televizorji in telefoni ter kamere IP CCTV, ki so omogočala nezaznavno zajemanje glasovnih in video posnetkov (Wikileaks 2017). Poznavanje in oblikovanje zlonamernih programskih oprem in izrab ranljivosti sistemov ter neporočanje le-teh proizvajalcem naprav interneta stvari močno zmanjša varnost sistemov na tržišču. Vsakršna zaznana in nesporočena ranljivost je lahko odkrita tudi s strani drugih obveščevalnih ali kibernetskih kriminalnih skupin, ki jo lahko ravno tako izrabijo. S tem se zasebnost in digitalna varnost uporabnika in vseh njegovih omreženih sistemov drastično zmanjša, zaščita pred izrabami pa ne more biti razvita, saj ostaja nepoznana. Centralna obveščevalna agencija (CIA) ZDA ni edina obveščevalna organizacija, ki je prepoznala možnost uporabe pametnih naprav in interneta

stvari za izvajanje svoje obveščevalne dejavnosti, saj so bile podobne objave tajnih podatkov v preteklosti povezane tudi z drugimi organizacijami iz različnih držav.

Izoblikovanje interneta stvari in medpovezljivih naprav je mogoče uporabiti za doseganje strateških ciljev, ti pa zajemajo pridobivanje informacij ali sabotiranje projektov, ki bi lahko bili uporabljeni za pridobivanje oborožitvenih sistemov, ti pa lahko povzročijo veliko škodo. Nadzorovanje in spremljanje poteka dela, delavcev in opreme predstavlja možnost za obveščevalne organizacije, da sledijo dogajanju in zbirajo informacije skozi sisteme interneta stvari. Integracija naprav interneta stvari v širše sisteme industrijskih kontrolnikov, ki lahko ob najmanjših spremembah privedejo do fizične škode na sistemih ali povzročijo nesreče, ima lahko širše varnostne implikacije za ljudi ali okolje ter zato ostaja primerna tarča za obveščevalne organizacije. Za primer tega bi lahko navedli napad z zlonamerno programsko opremo Stuxnet (Zetter 2014). Omreženi sistemi morajo biti zavarovani za nemoteno in nespremenjeno delovanje, vendar je mogoče te skozi sofisticirane napade spremeniti ali jih tudi onesposobiti, kot se to dogaja v primeru avtomatizirane zlonamerne programske opreme Bricker-bota.

Internet stvari postaja in bo v prihodnosti postal še bolj zanimiv za obveščevalne organizacije zaradi naših preferenc in uporabe tehnologije, ki jo vnašamo v naše domove. Zaslediti je mogoče vse več govora o pametnih domovih in mestih, kjer bi bila vsa tehnologija povezana med seboj. Potrebe po električni energiji in neomejenem pretoku informacij med napravami bi bile ogromne, kar bi lahko povzročilo nove grožnje. Vsaka povezana naprava bi komunicirala z drugimi in imela možnost vplivanja na celotno omrežje, pri čemer bodo lahko napadalci lažje vplivali na delovanje mest in same infrastrukture. Možnost vplivanja na delovanja celotnih mest in njihovih infrastruktur pa bo pritegnila tudi pozornost obveščevalnih organizacij, ki bodo želele zaščititi lastno infrastrukturo in poskušale vplivati na tujo.

Tako kot obveščevalne organizacije tudi celotni državni nacionalno-varnostni sistemi prepoznavajo pomembnost informacijske in kibernetske dimenzije. S pojavom koncepta hibridne vojne in več-domenske bitke je prišlo do spremembe v razumevanju, kako voditi vojne. Trenutne strategije skupnega delovanja različnih vej oboroženih sil in drugih za obrambo pomembnih organizacij bo v prihodnosti zamenjal sistem medsebojno povezanih zmogljivosti različnih akterjev, ki zajemajo tudi informacijske strokovnjake za izvajanje aktivnosti v kibernetskem prostoru ali na elektromagnetnem spektru. Kompleksna integracija informacijskih obveščevalnih organizacij in specializiranih informacijsko-obveščevalnih vojaških enot v delovanje v konfliktu bo omogočila razširitev bojevanja iz tradicionalnih dimenzij (zrak, kopno, morja, vesolje) v nova okolja, kot je kibernetski prostor. (Reilly 2016). Potreba po integraciji informacijskih enot izhaja iz razumevanja informacijskega in kibernetskega okolja kot okolja, ki omogoča uporabo tehnologije, informacij in povezav kot orožja za izvajanje napadov in zbiranje informacij o njegovih uporabnikih.

Vojaške in obveščevalne enote ter organizacije, ki se ukvarjajo z delovanjem v kibernetskem prostoru, so bile v preteklosti razumljene kot podporne organizacije in namenjene zagotavljanj delovanja podpornih sistemov ter zagotavljanja varnosti pred nasprotnikovimi informacijskimi operacijami. Z vse večjo integracijo v nove načine bojevanja so te enote in organizacije pridobile tudi ofenzivne sposobnosti in naloge izvajanja kibernetskih in informacijskih operacij, ki bi lahko omogočile pridobivanje prednosti pred nasprotniki in izrabo teh prednosti tudi v drugih dimenzijah bojevanja. Poleg nalog izvajanja obrambe pred informacijskimi operacijami so pridobile tudi naloge ofenzivnega delovanja in izvajanja aktivnosti proti sovražnim oboroženim silam v konfliktu ali za informiranje civilistov, ujetih na območju bojevanja.

Namen novih konceptov bojevanja je združitev vseh državnih organizacij v obrambno-varnostnem sistemu za namene pridobivanja prednosti, povečevanja učinkovitosti in varčnosti na terenu (Army Capabilities Integration Center 2017). Informacijska dimenzija delovanja organizacij nacionalnovarnostnega sistema postaja zato skozi nove koncepte in grožnje vedno bolj potrebna in dejavna. Pojav novih konceptov vodenja oboroženega spopada in vojn bo zato imel še večje varnostne implikacije na uporabnike novih tehnologij, še posebej na uporabnike naprav interneta stvari, saj bodo omogočile izvajalcem takšnega bojevanja dodatno možnost napada v naše domove ali vplivanja na nas skozi te naprave s informacijskimi ali psihološkimi operacijami. Primer takšnega delovanja je Irak, kjer Združene države Amerike s koalicijo podpirajo operacije iraških vladnih sil proti Islamski državi. Vladnim borcem na terenu pomagajo z informiranjem o podatkih, zajetih s signalnimi in satelitskimi sistemi, z izvajanjem elektronskega bojevanja in blokiranjem signalov, izvajanjem kibernetskih aktivnosti in hekerske dejavnosti ter izvajanjem ciljane propagande (Freedberg 2017). Borci teroristične skupine Islamske države so znani po tem, da poskušajo izrabiti naprave interneta stvari, kot so brezpilotni letalni sistemi (Warrick 2017), pametne naprave in telefonija VoIP (Taylor 2016) ter veliko drugih za pridobivanje prednosti na terenu. Uporabnost novega pristopa omogoča državam boljše delovanje in učinkovitejši boj proti terorističnim organizacijam, obenem pa omogoča povečanje učinkovitosti in predstavlja orodje za iskanje prednosti v vojni z bolje tehnološko opremljenimi nasprotniki in sovražnimi državami. Internet stvari bo pripeljal do možnosti implementacije tega koncepta, saj bo potreben za hitro širjenje informacij, vendar bo obenem postal tudi tarča za doseganje ciljev.

Večja specializacija obveščevalnih organizacij, oboroženih sil in kibernetskih kriminalcev bo zato povzročila potrebo po oblikovanju boljših varnostnih in obrambnih mehanizmov naprav interneta stvari, obenem pa zahtevala od uporabnikov, da se zavedamo obstoja različnih vrst groženj v kibernetskem okolju in da razumemo, kako lahko kot posamezniki pripomoremo k oblikovanju varnejšega kibernetskega okolja in informacijske infrastrukture.

IV. ZAKLJUČEK

İnternet stvari je brez dvoma tista ločnica, ki je dokončno spojila nekoč dva razmeroma ločena prostora in infrastrukturi, fizično in kibernetsko. İn če smo se v obdobju interneta prve in druge generacije še nekako tolažili, da je mogoče preprečiti neposredno varnostno grožnjo, izhajajočo iz kibernetskega prostora, je internet stvari te meje dokončno presekal. Upoštevajoč, da je del interneta stvari implementiran neposredno v človeško telo (kot so npr. srčni vzpodbujevalniki), pa del interneta postaja neposredno tudi človek. Slednji je tudi v strateškem razumevanju prostora

domena, ki postaja vse bolj ključna. V prispevku smo zato izhajajoč iz sodobnih varnostnih teorij in njihovih konceptov, kot je sekuritizacija, preučili varnostna razsežja interneta stvari, pri tem pa se posebej posvetili vzrokom, posledicam in tudi rešitvam omenjenega problema. Pri tem se je še enkrat več izkazalo, da internet v osnovi ni bil zasnovan, da bi bil varen, pač pa trdoživ in nadgradljiv, kar mu je dalo neslutene gospodarske, politične, strateške in varnostne dimenzije. Internet je tako povsem spremenil sodobno mednarodno skupnost, tako da so nekatere države celo ustanovile posebna diplomatska predstavništva za tehnološko ključna podjetja[5], Voditelji slednjih se na državniških srečanjih sestajajo s predsedniki vlad in državnimi suvereni. Države vse bolj javno priznavajo, da ustanavljajo posebna poveljstva za kibernetske operacije na ravni zvrsti, kot so kopno, zrak, morje in vesolje. In obveščevalne službe (tako državne kot zasebne) so vse bolj odvisne od informacij, pridobljenih na osnovi informacijsko-komunikacijske tehnologije. Ob vsej prednosti, zlasti odločevalski, logistični in ekonomski, pa bo največjo pozornost potrebno posvetiti ravno posamezniku, ki je daleč najbolj ranljiv deležnik kibernetskega prostora. Ustavna določila zahodnih demokracij, ki stoletja varujejo svobodo izražanja, zasebnost in človekove pravice, so na preizkušnji podobno kot med obema svetovnima vojnama, ko so jih ogrožali naraščajoči totalitarizmi. Danes se vse bolj zdi, da je preteči totalitarizem tehnologija sama in nekateri, v članku že omenjeni futurologi, opozarjajo na morebitne dramatične in kataklizmične posledice. In čeprav se je zloraba interneta stvari začela zaradi nepredvidljive človekove narave, lahko ob misli na točko singularnosti (https://en.wikipedia.org/wiki/Technological_singularity) pomislimo tudi na scenarij, ko bo samoučeča tehnologija mimo volje njenih lastnikov in razvijalcev pridobila popoln nadzor nad našim življenjem. Če je tak scenarij znanstvena fantastika, pa so neizmerne baze podatkov, ki so jih o uporabnikih pridobila (na bolj ali manj legalen način) socialna omrežja in tisti podatki, ki jih različne službe lahko pridobijo preko interneta stvari, realnost, ki jo lahko percipiramo kot ogrožujočo ali pa kot neizogibno realnost. Vstopamo torej v čas popolne transparentnosti, kar za nekatere pomeni faza popolne demokracije in celo (ponovni) konec zgodovine, za druge pa obdobje totalnega medsebojnega nadzora, pri čemer se KGB, Stasi in Gestapo zdijo le nedolžni primeri. Naš namen ni, postaviti se na katerokoli stran, pač pa opozoriti na nujnost povezovanja različnih znanstvenih disciplin in njihove odgovornosti za razvoj družbe. Zato bo potrebno v veliki meri redefinirati tudi digitalno dividendo, ki ne bo več ločila tistih, ki imajo dostop in tistih, ki ga nimajo, pač pa one, ki razumejo in tiste, ki ne.

LITERATURA

[1] 'Don't Believe the Car Hacking Hype' 2015, *PC Magazine*, pp. 43-45, Academic Search Premier, EBSCO*host*, viewed 19 April 2017

[2] Ackerman, S 2012, *CIA Chief: We will spy on you through your dishwasher*. Available from: https://www.wired.com/2012/03/petraeus-tv-remote/. [24 April 2017].

[3] All Things Considered 2016, *An Experiment Shows How Quickly The Internet Of Things Can Be Hacked*. Available from: http://www.npr.org/sections/alltechconsidered/2016/11/01/500253637/an-experiment-shows-how-quickly-the-internet-of-things-can-be-hacked. [24 April 2017].

[4] Andrea, I., Chrysostomou, C. and Hadjichristofi, G., 2015, July. Internet of Things: Security vulnerabilities and challenges. In *Computers and Communication (ISCC), 2015 IEEE Symposium on* (pp. 180-187). IEEE.

[5] Arbor Network 2017, *IoT BOTNETS & DDoS ATTACKS: WHAT YOU NEED TO KNOW*. Available from: https://www.arbornetworks.com/iot-botnets-ddos-attacks-what-you-need-to-know. [24 April 2017].

[6] Army Capabilities Integration Center 2017, Multi-Domain Battle: Combined Arms fort he 21st Century. Available from: http://www.arcic.army.mil/App_Documents/Multi_Domain_Battle.pdf. [24 April 2017].

[7] Bailey, MW 2016, 'Seduction by Technology: Why Consumers Opt Out of Privacy by Buying into the Internet of Things', *Texas Law Review*, 94, 5, pp. 1023-1054, Academic Search Premier, EBSCO*host*, viewed 19 April 2017.

[8] Brito, J. in Watkins, T., 2011. Loving the cyber bomb-the dangers of threat inflation in cybersecurity Policy. *Harv. Nat'l Sec. J.*, *3*, pp. 39-84.

[9] Burt, J 2016, 'IoT Could Be Used by Spies, U.S. Intelligence Chief Says', *Eweek*, p. 1, Academic Search Premier, EBSCO*host*, viewed 19 April 2017.

[10] Cimpanu, C 2016, *You Can Now Rent A Mirai Botnet of 400,000 Bots*. Available from: https://www.bleepingcomputer.com/news/security/you-can-now-rent-a-mirai-botnet-of-400-000-bots/. [24 April 2017].

[11] Clapper, JR 2016, *Worldwide Threat Assessment of the US Intelligence Community*, US Senate Select Committee on Intelligence. Available from: https://www.intelligence.senate.gov/sites/default/files/wwt2016.pdf. [24 April 2017].

[12] Condliffe, J 2016, *IoT Botnets Are Growing - and Up for Hire*. Avalable from: https://www.technologyreview.com/s/602994/iot-botnets-are-growing-and-up-for-hire/. [24 April 2017].

[13] Danova, T 2013, Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020. Available from: http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10. [24 April 2017].

[14] Fisher, D 2013, What is a Botnet? Available from: https://blog.kaspersky.com/botnet/1742/. [24 April 2017].

[15] Freedberg, SJ 2017, Iraq: Prooving Ground for Multi-Domain Battle. Available from: http://breakingdefense.com/2017/04/iraq-proving-ground-for-multi-domain-battle/. [24 April 2017].

[16] Gartner 2017, *The thing is not really the thing*. Available from: http://view.ceros.com/gartner/iot/p/1. [24 April 2017].

[17] Ghani, H., Khelil, A., Suri, N., Csertán, G., Gönczy, L., Urbanics, G. and Clarke, J., 2014. Assessing the security of internet-connected critical infrastructures. *Security and Communication Networks*, *7*(12), pp.2713-2725.

[18] Goodin, D 2017, *BrickerBot, the permanent denial-of-service botnet, is back with a vengeance*. Available from: https://arstechnica.com/security/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/. [24 April 2017].

[19] Grayson, K., 2003. Securitization and the boomerang debate: A rejoinder to Liotta and Smith-Windsor. *Security Dialogue*, 34(3), pp. 337-343.

[20] InfoSec Institute 2015, *Hacking ZigBee Networks*. Available from: http://resources.infosecinstitute.com/hacking-zigbee-networks/. [24 April 2017].

[21] InfoSec Institute 2017, *The Rise of the IoT Botnet: Beyond the Mirai Bot*. Available at: http://resources.infosecinstitute.com/rise-iot-botnet-beyond-mirai-bot/#gref. [24 April 2017].

[22] Kaspersky 2017, What is a Botnet? Available from: https://usa.kaspersky.com/resource-center/threats/botnet-attacks. [24 April 2017].

[23] Krebs, B 2016a, *Hacked Cameras, DVRs Powered todays Massive Internet Outage*. Available from: https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/. [24 April 2017].

[24] Krebs, B 2016b, *Who makes the IoT Things Under Attack*. Available from: https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/. [24 April 2017].

[25] Li, S., Tryfonas, T. and Li, H., 2016. The internet of things: a security point of view. *Internet Research*, *26*(2), pp.337-359.

[26] Loshin, P 2016, *Details emerging on Dyn DNS DDoS attack, Mirai IoT botnet*. Avalable from: http://searchsecurity.techtarget.com/news/450401962/Details-emerging-on-Dyn-DNS-DDoS-attack-Mirai-IoT-botnet. [24 April 2017].

[27] MalwareTech 2016, *Mapping Mirai: A Botnet Case Study*. Available from: https://www.malwaretech.com/2016/10/mapping-mirai-a-botnet-case-study.html. [24 April 2017].

[5] http://fortune.com/2017/02/06/denmark-ambassador-apple-google/

[28] Mavromoustakis, C.X., Mastorakis, G. and Batalla, J.M., 2016. Internet of Things (IoT) in 5G Mobile Technologies. *Modeling and Optimization in Science and Technologies. Springer International Publishing*, *56*, p.93.
[29] Misra, S., Maheswaran, M. and Hashmi, S., 2016. Security Challenges and Approaches in Internet of Things. *SpringerBriefs in electrical and computer engineering (*.
[30] NMAP 2017, *NMAP home page*. Available from: https://nmap.org/. [24 April 2017].
[31] Palmer, D 2016, *IoT devices can be hacked in minutes, warn researchers*. Available from: http://www.zdnet.com/article/iot-devices-can-be-hacked-in-minuteswarn-researchers. [24 April 2017].
[32] Pauli, D 2016, *IoT worm can hack Philips Hue lightbulbs, spread across cities*. Available from: https://www.theregister.co.uk/2016/11/10/iot_worm_can_hack_philips_hue_lightbulbs_spread_across_cities/. [24 April 2017].
[33] Pwnie Express 2017, *Internet of Evil Things*. Available from: https://www.pwnieexpress.com/2017-internet-of-evil-things-report. [24 April 2017].
[34] Radware 2017, *»Brickerbot« Results In PDoS Attack*. Available from: https://security.radware.com/ddos-threats-attacks/brickerbot-pdos-permanent-denial-of-service/. [24 April 2017].
[35] Reilly, JM 2016, »Multidomain Operations«. Air and Space Power Journal. Available from: http://www.au.af.mil/au/afri/aspj/digital/pdf/articles/2016-Spring/V-Reilly.pdf. [24 April 2017].
[36] Ronen, E, O'Flynn, C, Shamir, A & Weingarten, A, *IoT Goes Nuclear: Creating a ZigBee Chain Reaction*. Available from: http://iotworm.eyalro.net. [24 April 2017].
[37] Roy, S. and Manoj, B.S., 2016. IoT enablers and their security and privacy issues. In *Internet of Things (IoT) in 5G Mobile Technologies* (pp. 449-482). Springer International Publishing.
[38] Savage, M 2016, *Attackers Exploit Weak IoT Security*. Available from: http://www.darkreading.com/threat-intelligence/attackers-exploit-weak-iot-security/d/d-id/1327159. [24 April 2017].
[39] Scardilli, B 2014, 'Securing the Internet of Things. (Cover story)', *Information Today*, 31, 5, pp. 1-36, Academic Search Premier, EBSCO*host*, viewed 19 April 2017.
[40] Shodan 2017, *Shodan home page*. Available from: https://www.shodan.io/. [24 April 2017].
[41] Smilansky, O 2016, 'Security IN THE internet of Things Era', *CRM Magazine*, 20, 9, pp. 30-33, Academic Search Premier, EBSCO*host*, viewed 19 April 2017
[42] Taylor, H 2016, Islamic State's favourite technologies outlined by studies. Available from: http://www.cnbc.com/2016/07/22/islamic-states-favorite-technologies-outlined-by-study.html. [24 April 2017].
[43] Tripathy, B.K., Dutta, D. and Tazivazvino, C., 2016. On the Research and Development of Social Internet of Things. In *Internet of Things (IoT) in 5G Mobile Technologies* (pp. 153-173). Springer International Publishing
[44] Warrick, J 2017, Use of weaponized drones by ISIS spurs terrorism fears. Available from: https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html?. [24 April 2017].
[45] WikiLeaks 2017, *Vault 7: CIA Hacking Tools Revealed*. Available from: https://wikileaks.org/ciav7p1/. [24 April 2017].
[46] Wind 2015, The Internet of Things for The Intelligence Community. Available from: http://events.windriver.com/wrcd01/wrcm/2016/08/WP-IoT-the-internet-of-things-for-the-intelligence-community.pdf. [24 April 2017].
[47] Zetter, K 2014, *An unprecedented look at Stuxnet, the world's first digital weapon*. Available from: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. [24 April 2017].

Dr. **Uroš Svete** je izredni profesor na Katedri za obramboslovje Fakultete za družbene vede Univerze v Ljubljani. Raziskovalno in pedagoško se ukvarja z varnostnimi implikacijami informacijsko komunikacijske tehnologije, razvojem obrambne in vojaške tehnologije ter preučevanjem sodobnih konfliktov. V mednarodnem prostoru je izvršni sekretar raziskovalnega odbora Oborožene sile in preučevanje konfliktov v okviru Svetovne sociološke asociacije (ISA).

Klemen Kovačič je študent podiplomskega študija na Fakulteti za družbene vede, smer Obramboslovje. Področja njegovega raziskovalnega zanimanja so informacijska tehnologija, z njo povezane grožnje in varnostni aspekti uporabe brezpilotnih letalnih sistemov.

Unlocking Wideband 5G

Mirko Ivančič, Amiteh, Slovenija

Abstract — While the frequency of "mmWave" systems can vary from 10 to more than 100 GHz, there are aspects of system design and the impact of hardware limitations that are common. A combination of high frequency and wide bandwidth require close attention to broadband noise, phase noise, linearity, frequency response and power dissipation. The use of directional antennas introduces another dimension to the problem of maintaining an effective link, since beam steering is required. This presentation discusses these issues and some solutions using a number of examples from 802.11ad and OFDM signals.

Keywords — mmWave, frequency, 802.11ad, OFDM, measurement challenges, interference, spectrum

I. INTRODUCTİON

The need to go to mm-wave is mainly related to the fact that the frequencies used for communication and information transmission till now are crowded and prone to interference. So there is a need to look for uncharted area to be able to guarantee a certain level of service.

Why are our operators shifting to mmWave? Before examining this question in more detail, let's review some of the emerging industry drivers.

II. IN THE WİRELESS WORLD

In the wireless arena we have:

– massive growth in data demand; fixed, nomadic & mobile. mmWave will play an important role in addressing this need.
– huge growth in the number of connected devices with the coming of the Internet of Things and finally
– an explosion in the diversity of wireless applications such as gesture control & augmented reality.

Consumers expect all of these to be addressed while maintaining exceptional network performance in terms of data throughput and performance in a crowd. All of this should be maintained while they move around. This is driving evolution from 4G to 5G.

Starting with 5G, the tremendous growth in mobile broadband traffic relies on access to sufficient radio frequency spectrum for high data throughput. We all know, that the sub-6 GHz cellular bands are extremely crowded and extremely fragmented. Therefore, in order to meet the expected 5G throughput, high frequency bands in the millimeter wave (mmWave) range will be adopted due to availability of large amounts of contiguous spectrum allowing for high data rates. 5G is considering frequency ranges up to 100 GHz to address this need. In terms of bandwidth, there are applications at 500 MHz (3.5 GHz for DPD work), 2 GHz, 5 GHz with emerging applications going even wider. Even though these frequency blocks in Table 1are just approximate, mmWave bands provide up to 10× more contiguous bandwidth than current cellular bands.

III. DESİGN AND MEASUREMENT CHALLENGES AT MİLİMETER WAVES

At high frequencies such as mmWave, the large spectrum blocks allowed for wide transmission bandwidths which can meet the high data rate demand in dense areas. Due to the properties at high frequencies (atmospheric absorption as a function of frequency), as we move to higher frequencies, transmission range gets shorter. We talk about close-range communication (100 meters or so) rather than kilometers. The fact that it is close-range communication, mmWave also allows for very efficient frequency reuse with simultaneously operating networks that do not interfere with each other. What this means is smaller cell size i.e. small cells. So mmWave small cells, with highly directional signals, will enable ultra-dense deployment in large cities and very crowded locations, ex. stadiums, for high, guaranteed throughput.

Table 1: Millimeter-wave 5G Frequency bands

Frequency	*OFCOM*	*FCC (Jun 2016)*	*ITU (Oct 2015) For study*
28 (25–27 GHz)		BW 425 MHz × 2	24.25–27.5 GHz
37 GHz		BW 400 MHz × 4	37–40.5 GHz
39 GHz		BW 200 MHz × 7	
40.5–43.5 GHz		FFS	42.5–43.5 GHz
45.5–48.9 GHz			45.5–47G Hz
47.2–50.2 GHz			
50.4–52.6 GHz			
57–66 GHz		59.3 – 71 GHz (extend ISM—unlicensed)	
64–71 GHz	66–71 GHz		66–76 GHz
71–76 GHz			
81–86 GHz			

A. *Issues at mmWave frequencies*

The problem is that engineers now have to design and measure these mmWave wide bandwidth signals. These come with measurement challenges though. The usual vector design and measurement challenges are significantly more difficult to solve. Imperfections that would be inconsequential at a 5 GHz carrier frequency with 20 MHz of modulation bandwidth, could render a 100 GHz carrier with 3.5 GHz wide incomprehensible. Communication designers are used to EVMs of 1 % – 2 %. As we go up in bandwidth and frequency, we also have to deal with higher levels of integrated broadband noise and phase noise respectively, which makes the EVM significantly higher. These are

challenges for both design and test. Small timing errors and gain mismatch between I/Q also all become much larger at mmWave. “Great Service In a Crowd” is one of the visions of 5G.

mmWave is also used for small cell backhaul, line-of-sight (LOS) – using directive antennas to overcome path loss. The available bandwidth is perfect and this is preferable to laying new fiber in complex terrains. There is emerging 92 GHz to 95 GHz small cell point-to-point backhaul ongoing today.

It also happens to be a 86 GHz to 92 GHz passive band used for Earth exploration, Radio Astronomy and Space Research. Designers have to ensure that even though not operating in these protected bands, emissions are below appropriate levels (–105 dBm/Hz in this case).

B. Measurement challenges at mmWave frequencies

The same properties that enable frequency re-use and dense deployment of small cells present design and measurement challenges. At high frequencies path loss is higher, signals get attenuated with distance and so it is very difficult to measure. To exacerbate this, as the signal bandwidth increases, the power gets spread out over a wider range of frequencies. The power spectral density of the signal gets lower and this also presents challenges.

Other than chasing small spurious or distortion products, customers also have to make measurements representing a real world environment. What this means is that relative measurements where both the carrier and the unwanted emissions are measured. This limits the use of a preamplifier to boost sensitivity due to the presence of the carrier. So high sensitivity AND dynamic range is needed.

The advantage in size for deployment comes with difficult design and measurement challenges. There are often very tight mechanical tolerances and connectivity to these devices is difficult with small fragile cables.

The complicated setups that customers have to deal with to make measurements including down-conversion with external mixing makes it challenging to setup and make repeatable measurements.

The spectrum for 5G and wireless breaks into three main areas nowadays:

– The first is below 6 GHz where we will see more the LTE advanced evolution.
– Above 6 GHz the research is focused right now at 28 GHz and 39 GHz. Several modulations are under investigation, the majority of these are OFDM derivative, TDD… They are looking to use them as small cell extension but as well backhaul.
– Above 40 GHz we will look at backhaul and wider spectrum batch. Those are very demanding and in all of these bands the availability of spectrum in all region does vary.

IV. THE IMPORTANCE OF MAKİNG A GOOD CONNECTİON

Cables are what we’ve been using for the majority of measurements for a very long time. There’s much to commend them, in particular the point about knowing where the signal is. The loss for signals at cm wavelengths is probably bearable.

A cable is a particular type of waveguide. Waveguides have been a stalwart for mmWave for decades. Low loss and again knowing where the signal is offset the inconvenience. Flexible plastic waveguides may in the future be a practicable alternative. Probes will become progressively more important for component evaluation.

Radiated tests might be the only thing you can do, because there’s nothing to connect to. That problem isn’t new to some people. At higher frequencies it’ll become more widespread, and we’ll need to take care to get repeatable measurements.

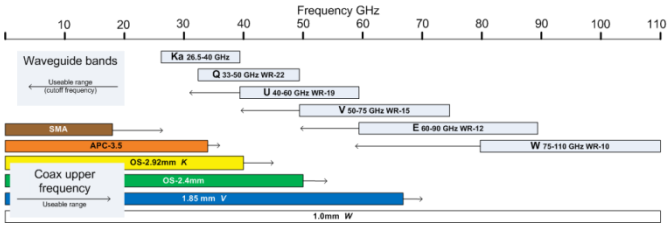


Figure 1: Cables and waveguides

V. ULTRA WİDEBAND MMWAVE IQ MEASUREMENTS

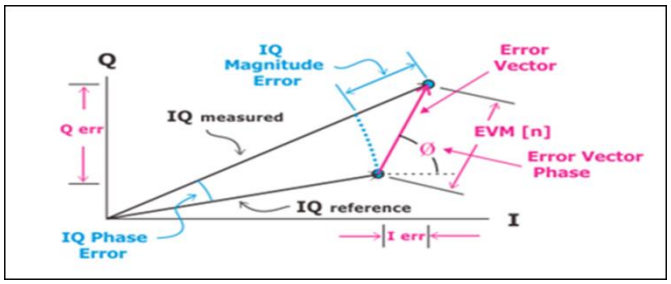


Figure 2: UWB mmWave IQ Measurements

What is EVM? The purpose of EVM is to identify transmitter issues that will affect a receiver conforming to the minimum requirements of a specification.

EVM is the normalized ratio of the difference between two vectors: IQ measured signal and IQ reference. While EVM usually involves a calculation of the reference from the signal being measured, it doesn’t have to. The reference can come from a second measurement channel, or a data file representing the wanted signal.

Required EVM depends on the modulation. Figure 3 shows EVM for some modulations. For the link to work, EVM should be at the limits shown. For the components test required level would be 10 dB better than the systema as a whole.

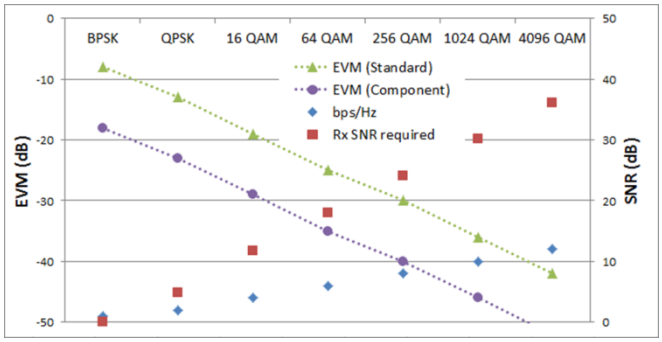


Figure 3: EVM for some modulations

Here are two examples of the measured QAM64 signal at 83.5 GHz:

– 1.6 GSym/s, 2 GHz BW (Figure 4),
– 4.0 GSym/s, 4.8 GHz BW (Figure 5).

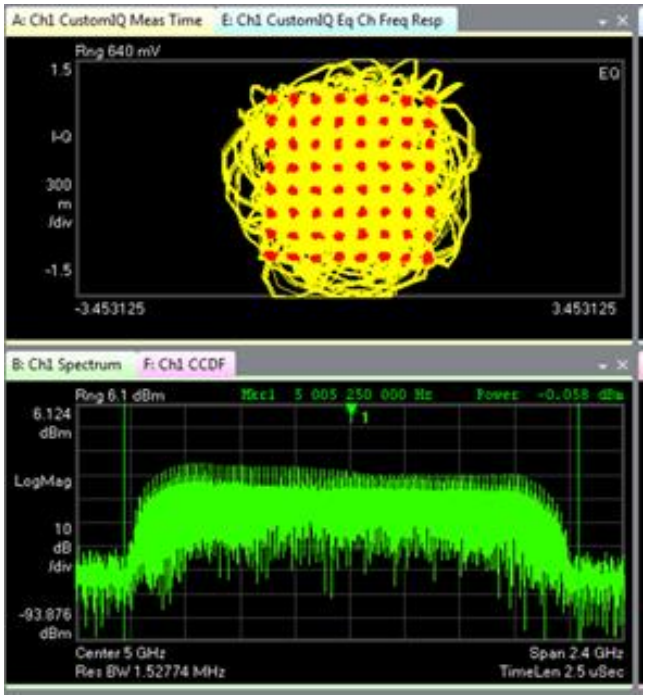


Figure 4: QAM64 signal at 83.5 GHz - 1.6 GSym/s, 2 GHz BW

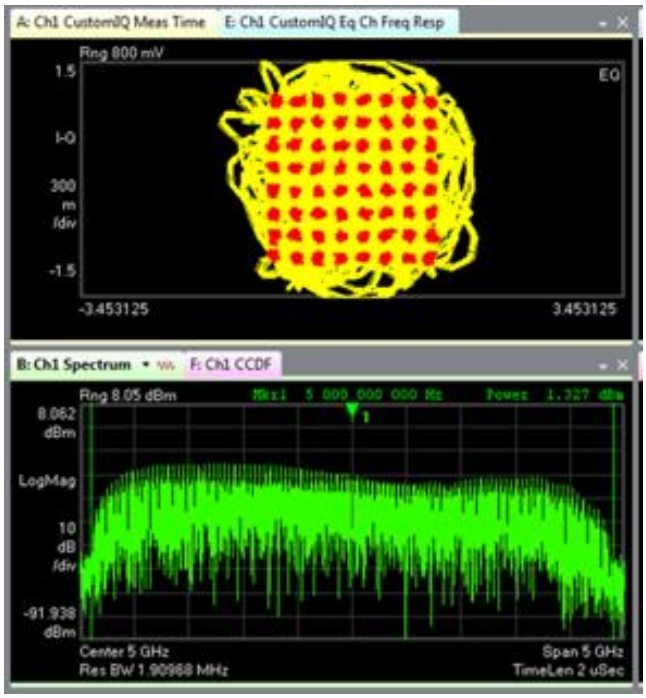


Figure 5: QAM64 signal at 83.5 GHz - 4.0 GSym/s, 4.8 GHz BW

Figure 6 shows a typical measuring system for aforementioned measurements.

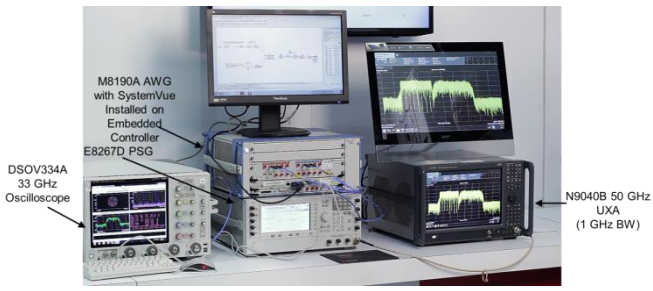


Figure 6: Typical measuring system for UWB mmWaves

VI. CONCLUSION

So with that, here is a summary of some of the common measurement challenges we have outlined previously:

– small dimensions and complex test setups,
– challenging ultra wideband mmWave IQ measurements,
– small signal strength.

We recognize that these measurements aren't easy. We have been partnering with key customers and in a moment we will introduce a breakthrough solution that will dramatically simplify design and measurement at mmWave and over wide bandwidths for our customers as they continue to innovate.

Figure 7: Common measurement challenges

LITERATURE

[1] Keysight Technologies, Coaxial Connectors, Adapters and Connectors, http://literature.cdn.keysight.com/litweb/pdf/5992-0118EN.pdf

Mirko Ivančič je diplomiral leta 1978 na ljubljanski Fakulteti za elektrotehniko, smer telekomunikacije in se zaposlil v podjetju Iskra Elektrozveze, kjer je vodil oddelek merilne tehnologije. Leta 1984 se je kot inženir za podporo tehničnih računalnikov zaposlil v Hermesu, v sektorju zastopstva za Hewlett-Packard. Od 1986 do 1992 je bil odgovoren za prodajo testno-merilne opreme za področje Hrvaške, nato je postal vodja servisa in leta 1993 član uprave Hermes Plus, d. d. in direktor podpore za vse HP-jeve izdelke za področje Slovenije, Hrvaške, Makedonije in delno Slovaške. Leta 1996 je postal direktor merilne skupine za prodajo in podporo elektronske, medicinske in kemijsko-analitske merilne opreme. Leta 1997 je zapustil Hermes in po letu dni dela v podjetju Spes postal direktor Venture, podjetja za razvoj, proizvodnjo in trženje plovil. Leta 2002 se je pridružil Avektisu, takratnemu slovenskemu zastopniku podjetja Agilent Technologies (bivši HP), kot vodja prodaje elektronske merilne opreme. Od leta 2010, ko je Agilentov partner za Slovenijo postal Amiteh d.o.o., pa dela pod okriljem tega podjetja.

5G – infrastruktura za napredne storitve javne varnosti, zaščite reševanja in pomoči

Boštjan Tavčar, Uprava Republike Slovenije za zaščito in reševanje

Povzetek — V članku je orisana vizija razvoja omrežij 5G, novih storitev in njihove primernosti za uporabo na področju javne varnosti, zaščite reševanja in pomoči - PPDR. Priložnosti, da Slovenija postane ena od referenčnih držav za razvoj tehnologije 5G ne smemo zamuditi.

Ključne besede — 5G, PPDR, Massive MIMO, majhna zakasnitev

Abstract — Article describes the vision of 5G networks development, new services and their use in the field of the Public Protection and Disaster Relief – PPDR. Opportunity for Slovenia to become reference country for development of 5G technologies should not be missed.

Keywords — 5G, PPDR, Massive MIMO, low latency

I. UVOD

V letošnjem letu lahko pričakujemo začetek izgradnje enotnega digitalnega radijskega omrežja državnih organov Republike Slovenije. Omrežje bo temeljilo na dveh medsebojno komplementarnih tehnologijah DMR in TETRA ter bo prek povezovalnega člena povezano v celoto. Neizbežno se končuje obdobje samostojnih namenskih radijskih omrežij posameznih državnih organov, kot tudi obdobje razvoja ločenih namenskih in javnih tehnoloških rešitev. Ob tem se odpirajo številna nova vprašanja, zlasti vprašanje kako zagotoviti ustrezno pokritost terena in ob tem omogočiti učinkovit prenos podatkov. O tem sem pisal v lanskoletnem članku: »LTE – tehnologija pametnih omrežij na področju zaščite in reševanja«. Tehnologija 5G je v marsičem še v fazi ideje, ki v nekaterih zamislih pomeni nove možnosti, ne zgolj komuniciranja, temveč tudi samodejnega pridobivanja koristnih informacij in samodejnega vodenja procesov. V nadaljevanju bom poskušal orisati priložnosti tehnologije 5G na področju varstva pred naravnimi in drugimi nesrečami ter odgovoriti na nekatera vprašanja, čeravno se bojim, da je slednjih veliko več, kot je danes razpoložljivih odgovorov.

Tehnologija 5G naj bi zagotavljala:

– velike hitrosti prenosa podatkov med 1 in 10 Gb/s,
– zakasnitve manjše od 1 ms,
– kratke odzivne čase,
– dobro spektralno učinkovitost,
– visoko kapaciteto sistema,
– boljše razmerje med hitrostjo prenosa podatkov na sredini in na robu celic,
– dobro energijsko učinkovitost sistemov in terminalov,
– boljšo zanesljivost in razpoložljivost v izrednih razmerah,
– samodejno organizacijo omrežij,
– boljšo programsko nadgradljivost opreme,
– in drugo.

Poleg naštetega, naj bi bile v omrežjih 5G omogočene ne zgolj neposredne komunikacije med uporabniškimi terminali temveč tudi med napravami. Terminali in naprave naj bi delovale po principu kognitivnega radija, ki se bo sproti prilagajal komunikacijskemu kanalu z namenom njegove optimalne izkoriščenosti, ob hkratni optimizaciji za to potrebnega frekvenčnega prostora in porabe energije.

Uporaba frekvenčnih področij od 10 do 300 GHz obeta velike hitrosti prenosa podatkov, ob hkratni razbremenitvi nižjih frekvenčnih pasov, katerih prednost je boljše razširjanje radijskih valov in s tem večji domet, kar je pomembno na ruralnih območjih, še zlasti za potrebe služb za javno varnost ter zaščito in reševanje (PPDR). Po drugi strani bodo višji frekvenčni pasovi zelo primerni za komunikacije v zaprtih prostorih in območjih kjer bo veliko število ljudi, kot so na primer območja za evakuacijo ob naravnih nesrečah prizadetih ljudi.

II. 5G – PRILOŽNOSTI

Druga generacija namenskih sistemov radijskih zvez DMR in TETRA je omogočila digitalizacijo in s tem boljšo kakovost govora, ni pa izpolnila obljub po učinkovitem in hitrem prenosu podatkov. Nadgradnja standarda, TETRA2, je sicer obljubljala višje bruto hitrost prenosa podatkov, tja do 115 kbit/s, vendar je zaradi uporabe 64-QAM modulacije zahtevala višji nivo signala na sprejemniku, –91 dBm in zato večje število baznih postaj.

Tehnologija LTE rešuje problem učinkovitega in hitrega prenosa podatkov tudi za potrebe javne varnosti ter zaščite in reševanja. Kljub temu so odprta še številna, ne zgolj strokovno tehnična vprašanja, na katere sem opozoril v članku: »LTE – tehnologija pametnih omrežij na področju zaščite in reševanja«, ki je bil predstavljen na 32. delavnici Vitel.

Tehnologija 5G ni zgolj nadgradnja tehnologije LTE, v smislu še višjih hitrost prenosa podatkov in odprave posameznih pomankljivosti. Je tehnologija, ki obljublja, da bo omogočila nove storitve. Še vse preveč razširjeno mišljenje, da so telekomunikacije zgolj podpora obstoječim procesom in temelj za informatizacijo le teh, je hudo zmotno in škodljivo, saj zavira razvoj. Tehnologijo 5G je nujno potrebo razumeti tudi kot priložnost za spremembe načina razmišljanja in organizacije služb na področju javne varnosti ter zaščite reševanja in pomoči. Za udejanjenje sprememb je nujno, da so na pozicijah odločevalcev tudi strokovnjaki s področja telekomunikacij, ker le ti pravilno razumejo tehnologije, kot so naštete v nadaljevanju.

Massive MIMO je tehnologija, ki uporablja za prenos signala zelo veliko število anten. Ključno pri njej je, da ima vsak kanal ločeno prostorsko karakteristiko, to pomeni, da se signali iz oddajnih do sprejemnih anten razširjajo po čim več različnih poteh. Tak primer so komunikacije znotraj objektov

in komunikacije v mestih, manj pa komunikacije na prostem na podeželju.

Tehnologija za zagotavljanje boljše pokritosti na robu celic s ponavljalniki signala bo zagotovila boljše razmerje med hitrostjo prenosa podatkov na sredini in robu celice ter s tem boljšo kakovost storitev. Ponavljalnike bo s pridom mogoče uporabiti tudi pri večjih naravnih in drugih nesrečah na območjih s slabšo pokritostjo z radijskim signalom.

Majhne zakasnitve pri prenosu podatkov so ključne za časovno kritične storitve. Nekatere od teh storitev so: upravljanje brezpilotnih zrakoplovov – dronov v notranjosti stavb, storitve tele-medicine, neposredne komunikacije med vozili ob sprožitvi klica eCall, določanje lokacije gasilcev in drugih reševalcev v notranjosti stavb ter drugo.

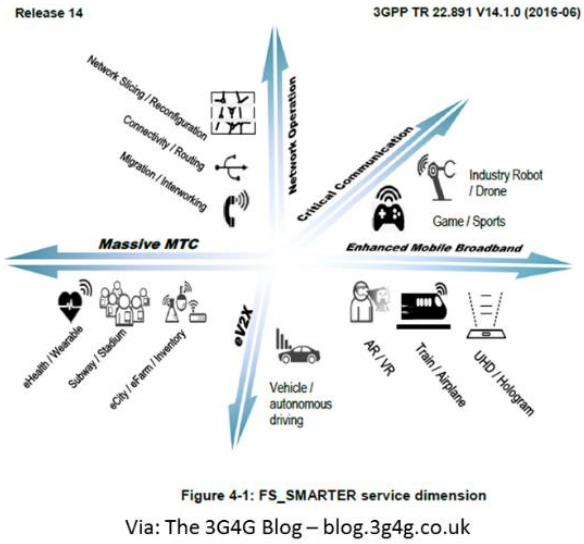
Uporaba milimetrskih valov oziroma kanalov v frekvenčnih pasovih do 300 GHz bo zagotavljala večje pasovne širine in s tem prenos večjih količin podatkov. Omogočala bo tudi ponavljanje frekvenc na krajših razdaljah, zaradi manjšega dosega radijskih valov pri teh frekvencah. V primeru velikih naravnih in drugih nesreč bo na območjih za evakuacijo ljudi, območjih za sprejem in pripravo reševalnih enot, območjih štabov, torej povsod tam, kjer bo velika koncentracija ljudi, mogoče zagotoviti dobre in razpoložljive komunikacijske storitve.

Omrežja 5G bodo zelo verjetno heterogena omrežja, sestavljena iz različnih tipov omrežij za različne namene: omrežij za mobilno telefonijo, omrežij za prenos velikih količin podatkov, med drugim tudi za HDTV, omrežij z minimalnimi zakasnitvami prenosa podatkov za časovno kritične storitve, omrežij za povezovanje senzorjev z majhno porabo energije in drugo.

S sistemom DMR lahko zagotovimo ustrezno pokritost Slovenije s 52 baznimi postajami. Na podlagi primerjalnih izračunov dometa baznih postaj DMR, TETRA in LTE lahko ocenimo, da bi za primerljivo pokritost potrebovali 274 baznih postaj TETRA in 531 baznih postaj LTE na frekvenčnem pasu 400 MHz oziroma 927 na frekvenčnem pasu 700 MHz [1]. Omrežja 5G bo sestavljalo še večje število še bolj na gosto posejanih baznih postaj, še zlasti pri uporabi višjih frekvenčnih območij. Pri tem je poraba energije pomembna iz dveh vidikov, ekonomskega in nacionalno varnostnega. V primeru velikih naravnih in drugih nesreč, kot je bil primer ujme z žledom v začetku leta 2014, pride do izpada električne energije na prizadetih območjih, ki so lahko velikosti posameznih regij. Delovanje telekomunikacijskih sistemov je v takšnih pogojih mogoče zagotoviti zgolj z napajanjem prek agregatov, zato je pomembno, da je njihova poraba električne energije čim manjša. Tehnologija 5G naj bi bila energijsko bolj učinkovita od tehnologije LTE, še vedno pa ne tako učinkovita, kot je na primer tehnologija DMR, ki pa po funkcionalnosti sploh ni primerljiva s tehnologijama LTE in 5G.

III. 5G – SLOVENIJA KOT REFERENČNA DRŽAVA

Evropska zveza v akcijskem načrtu 5G za Evropo [2] poziva države članice, da razmislijo o uporabi bodoče infrastrukture 5G tudi za izboljšanje zmogljivosti in storitev na področju javne varnosti ter varstva pred naravnimi in drugimi nesrečami. Pri tem spodbujajo države, da razvoj in uporabo omrežij 5G za te namene vključijo v svoje nacionalne načrte razvoja telekomunikacij. Pobuda je zanimiva, saj prihaja v času, ko tehnologija 4G – LTE z različico standarda 14, ki je napovedan za junij 2017, šele pričenja svojo pot na področju namenskih komunikacijskih sistemov za javno varnost ter zaščito in reševanje. Različica standarda 14 med drugim predvideva storitve za javno varnost ter zaščito in reševanje: Dodatek za oddajanje multimedijskih vsebin za potrebe javne varnosti, s katerim bodo, na primer, policisti na terenu na svojih radijskih postajah v živo spremljali video prenos dogajanja na javnih prireditvah. Predvidene so tudi storitve za boljše lociranje klica, storitve prek WLAN, možnost uporabniškega zaznavanja in preprečevanja lažnih klicev, robustnejši protokol za vzpostavitev govornih klicev prek VoLTE in drugo. Predvidene so storitve za komunikacijo vozil z okolico – storitve V2X, izboljšane TV video storitve, optimizirana naj bi bila poraba energije pri posameznih storitvah, zmanjšane naj bi bile zakasnitve, pri prenosu v frekvenčnem pasu 41 (TDD LTE) naj bi bila predvidena višja oddajna moč (26dBm +/-2dB, Power Class 2) in drugo. Komercialno zanimivo opremo lahko pričakujemo okoli leta 2020, ko naj bi bila vzpostavljena pilotska omrežja 5G. V bistvu gre po eni strani za evolucijo LTE v 5G na nivoju radijskega dostopa, po drugi strani pa za razširitev radijskega dostopa na nova frekvenčna območja vse tja do 100 GHz. Pobuda za vzpostavitev pilotskih omrežij 5G je zanimiva tudi s finančnega stališča, saj bo Evropska zveza z jasnim namenom, ne da zgolj ujame vlak razvoja na področju tehnologij 5G, temveč da postane vodilna na tem področju, omogočila dostop do finančnih sredstev za pilotska 5G omrežja. Na državah članicah je, da sprejmejo izziv.



Slika 1: LTE – standard različica 14 [3]

Z namenom, da proučijo možnosti kandidiranja Slovenije kot ene od referenčnih držav za testiranje tehnologije 5G, so se v preteklih mesecih dvakrat sestali predstavniki Ministrstev za javno upravo, obrambo, notranje zadeve, Agencije za komunikacijska omrežja in storitve, Fakultete za elektrotehniko in podjetij Telekoma Slovenije, Ericsson in Iskratel. Osebno sem se udeležil sestankov v vlogi predstavnika za področje varstva pred naravnimi in drugimi nesrečami, kot neodvisnega podsistema nacionalne varnosti. Na začetku smo naredili pregled aktivnosti v katere so vključeni akterji iz Slovenije in bi bile lahko povezane s tehnologijo 5G. Naj navedem samo tiste, pri katerih

sodelujejo tudi predstavniki Uprave Republike Slovenije za zaščito in reševanje. To so projekti I-Heero, NEXES in Enotno digitalno radijsko omrežje državnih organov Republike Slovenije – omrežje DMR. Pri projektu I-Heero se ukvarjamo z razvojem naslednje generacije sistema eCall, novih storitev, ki bodo zahtevale višje hitrosti prenosa podatkov, majhne zakasnitve in drugo, kot tudi razširitvijo storitev sistema eCall za tovorna in enosledna vozila. Predlog, da bi eCall naprave v vozilih ob nesreči poleg klica na številko 112 pošiljale opozorilo tudi eCall napravam v sosednjih vozilih, je ključen za preprečevanje verižnih nesreč. Predlog je uresničljiv v omrežjih 5G, ki bodo poleg majhne zakasnitve prenosa podatkov omogočala tudi neposredne komunikacije med napravami. Pri projektu NEXES proučujemo možnosti uporabe mobilnih in fiksnih podatkovnih omrežij za prenos klicev v sili. Nekaj več o projektu je zajeto v nadaljevanju. Omrežje DMR bo poleg omrežja TETRA sestavljalo enotno govorno digitalno radijsko omrežje državnih organov Republike Slovenije. Prvotno načrtovano povezavo obeh omrežij je smiselno razširiti še na povezavo z omrežjem Slovenskih železnic GSM-R prek in z javnim omrežjem LTE/5G.

Dogovorili smo se, da bomo v pilotskem omrežju 5G preizkušali možnosti povezav baznih postaj TETRA in DMR prek omrežja 5G, možnosti hitrega prenosa podatkov v frekvenčnem pasu okoli 6 GHz,pPrenos podatkov v omrežju z majhnimi zakasnitvami za upravljanje dronov in uporabo protokolov za medsebojno komunikacijo naprav IoT. Za vsakega od predvidenih testiranj bomo pripravili različne scenarije, predvsem s področja javne varnosti ter zaščite in reševanja.

Odločitev Slovenije, da kandidira za eno od referenčnih držav za testiranje tehnologijo 5G, je strateškega pomena. Ne zgolj geografske danosti, ki so kot nalašč za vzpostavitev dobrega testnega referenčnega okolja, temveč tudi pripravljenost vseh deležnikov, tako tujih in domačih podjetij, nacionalnega operaterja, raziskovalnih inštitucij kot tudi državnih inštitucij s področja javne varnosti ter zaščite in reševanja, so dobra garancija za uspeh, od katerega bodo koristi vsestranske.

IV. STORITVE KLICA V SILI 112 NASLEDNJE GENERACIJE V OMREŽJIH 5G

Storitve klica v sili na 112 so vedno sledile razvoju telekomunikacijskih in informacijskih tehnologij. K prvotnim govornim klicem smo najprej začeli dodajati podatke, kot sta številka in lokacija kličočega. Temu je sledila možnost pošiljanja besedilnih klicev v obliki SMS-sporočil. Zapletlo se je pri video klicih, saj mobilni telefoni kljub možnosti video klicev v omrežjih 3G le teh niso bili sposobni pošiljati na številko 112, zaradi drugačnega procesiranja klica v sili v samem telefonu. Vse našteto predstavlja prvo generacijo storitev klica v sili, pri kateri potuje klic prek ustaljenih govornih in besedilnih komunikacijskih storitev.

Leta 2008 je bila v Sloveniji predstavljena aplikacija za besedilne klice v sili WAP112. Aplikacija, ki je delovala na protokolu WAP je kot prva uporabljala podatkovno omrežje za prenos klica v sili. Pri razvoju aplikacije sem sledil trem osnovnim zamislim, to je da mora biti neodvisna od operaterjev mobilne telefonije, da mora delovati na odprtih podatkovnih protokolih in da mora delovati na vseh telefonskih aparatih, ki podpirajo omenjene protokole. V bistvu je šlo za popolnoma novo in inovativno zamisel, omogočanja klicev v sili, predvsem za gluhe in naglušne. Aplikacijo WAP112, ki v malo spremenjeni obliki - v tem času smo iz protokola WAP prešli na protokol http - deluje še danes in za katero smo leta 2009 dobili mednarodno nagrado združenja EENA, lahko brez pretiravanja smatramo za prvo aplikacijo storitev klica v sili 112 naslednje generacije.

Razvoj naslednje generacije klica v sili je dobil nov zagon leta za tem, z evropskim projektom NEXES. Ideja projekta je izboljšati medsebojno povezljivost služb, ki sprejemajo klice v sili na 112 in omogočiti sprejem klicev iz različnih namenskih ali spletnih aplikacij prek ali s pomočjo enotnega omrežja IP. EENA predlaga v ta namen vzpostavitev vseevropskega mobilnega omrežja za namenske aplikacije za klic v sili, imenovanega PEMEA. Pogoji za takšno omrežje so zadosti visoka stopnja zanesljivosti, razpoložljivosti in varnosti delovanja. Glede slednje je še vedno odprto vprašanje, ali zagotavljanja ustrezno varovanje osebnih podatkov, zaradi česar se osebno zavzemam, da se morajo klici na 112 vzpostavljali neposredno med klicateljem in pristojno službo za sprejem klicev v sili na 112, kjerkoli po Evropi oziroma v vseh tistih državah, ki se bodo vključile v omrežje PEMEA.

Slika 2: Zasnova WAP112

Mobilna omrežja LTE in 5G so pogoj za uspešno vzpostavitev in uspešen razvoj storitev klica v sili 112 naslednje generacije. V začetku meseca marca tega leta je v Sofiji potekalo testiranje povezljivosti storitev govornega klica v sili naslednje generacije z uporabo storitve VoLTE prek omrežja LTE/IMS. Ugotovljeno je bilo, da sta bila prenos in zaznava podatka, da gre za klic v sili uspešna, da pa je za kakovost storitve v prvi vrsti odgovorna bazna postaja – eNodeB, medtem ko je za podatke o točni lokaciji kličočega odgovoren terminal. Podatki o lokaciji so se uspešno prenesli prek omrežja PEMEA. Možnost uporabe omrežij LTE za prenos naslednje generacije storitev klica v sili je bila prikazana tudi na delavnici projekta NEXES, ki jo je v začetku meseca aprila gostila Fakulteta za elektrotehniko Univerze v Ljubljani. V okviru delavnice je na koncu potekala tudi razprava o tehničnih in organizacijskih vidikih razvoja storitev klica v sili 112, v okviru katere so bile izpostavljene tudi potrebe, ki jih bo mogoče uresničiti šele v omrežjih 5G. Ena od takšnih je možnost točnega lociranja klica v večstanovanjskih blokih, kar dandanes predstavlja skoraj nerešljiv problem. V omrežjih 5G bo pridobitev lokacije klica iz posameznega stanovanja mogoča predvsem z uporabo podatkov iz dela omrežja, ki bo skrbelo za medsebojno komuniciranje naprav IoT.

V. 5G IN INFORMACIJSKA DRUŽBA

Zasnova informacijske družbe, kot jo je že leta 1933 predstavil ekonomist Fritz Machlup, temelji na povezanosti oziroma soodvisnosti med produkcijo in znanjem. Zamisel poznana tudi pod pojmom »industrija znanja« predstavlja prehod iz na materialnih dobrinah temelječe ekonomije na ekonomijo temelječo na znanju. Z razvojem informacijskih tehnologij in še zlasti povezovanjem le teh v vse bolj enovito in vseobsežno informacijsko omrežje, je v teoriji informacijske družbe začela dobivati pomembno mesto zamisel družbe omrežij. Nasprotniki te zamisli sicer trdijo, da se zgolj ustvarja vtis, da smo s povezovanjem in dostopnostjo do informacij vstopili v novo obliko družbe, vendar pri tem pozabljajo, da takšno povezovanje kot dostopnost do informacij omogočata drugačne medsebojne odnose in drugačno, lahko tudi bolj celovito razumevanje informacij. Pustimo ob strani možnost manipuliranja z informacijami in razširjanja dezinformacij. Dejstvo je da informacijske tehnologije ne zgolj »informatizirajo« obstoječe družbene odnose in procese, temveč ustvarjajo nove in s tem nove oblike družbe. Digitalna transformacija je torej proces prehoda iz današnje v bodočo informacijsko družbo, z uporabo sodobnih informacijsko komunikacijskih tehnologij. Zamisel informacijske družbe tudi ni več vezana zgolj na produkcijo v njeni prvotni obliki, temveč tudi na storitve, tako materialne kot nematerialne. Podsistem nacionalne varnosti varstva pred naravnimi in drugimi nesrečami med drugim opravlja storitve zaščite in reševanja ljudi, živali in okolja in ga je zato nedvomno potrebno obravnavati kot del »produkcijskega« okolja, saj s svojo dejavnostjo prispeva k bruto družbenemu prihodku. Njegove storitve morajo nujno slediti zamislim informacijske družbe, saj le na ta način lahko zagotovimo nadaljnjo povečevanje učinkovitosti sistema. Pri tem moram ponovno poudariti, da ne gre zgolj za informatizacijo dosedanjih procesov, temveč za ustvarjanje novih. To srednjeročno pomeni tudi spreminjanje ustaljenih zasnov in doktrin zaščite in reševanja. To spreminjanje pa bo uspešno le v tesni povezavi in upoštevanju stroke s področja informatike in komunikacij. Pred tem se moramo nujno znebiti še preveč ukoreninjenega mišljenja, da so službe s področja informatike in komunikacij zgolj podporne službe! Nujno je tudi spoznanje, da je za spremembe ključnega pomena podpora okolja, ki mora biti spodbujena s konstruktivnimi in na strokovnih temeljih utemeljenimi političnimi odločitvami.

Omrežja 5G bodo omrežja informacijske družbe, zato je njihove storitve že danes potrebno obravnavati v smislu zgoraj zapisanih misli. Že danes je potrebno bodoče uporabnike pripravljati na storitve, ki jih bodo omogočala in jih spodbujati, da izhajajoč iz poznavanja teh storitev začnejo spreminjati svoje načine delovanja. Prav tako jih je potrebno spodbujati, da v duhu informacijske družbe razvijajo nove zasnove svojega delovanja in z njimi spodbujajo nadaljnji razvoj oziroma smer razvoja informacijskih in komunikacijskih tehnologij. Ena od nalog v okviru vzpostavitve referenčnega omrežja 5G bo izdelava čim več scenarijev možne uporabe novih storitev. Enega od takšnih vzorčnih scenarijev »Opis gašenja požara v garažnem objektu« je predstavljen v nadaljevanju.

»Prek aplikacije za klic v sili na številko 112 pokliče občan in pove da se iz garaže ob stadionu, na katerem je večji glasbeni dogodek, vali dim. Operater v centru za obveščanje ga prosi, da mu pošlje HD fotografijo garaže, za tem pa da vključi kamero in snema dogajanja v okolici garaže. Posnetek se prek aplikacije na telefonu in omrežja 5G prenaša neposredno v center za obveščanje. Na podlagi pridobljenih podatkov, še zlasti točne lokacije dogodka in ocene stanja, operater aktivira gasilce in reševalce ter o požaru obvesti policijo. Ko gasilci prispejo na kraj dogodka vodja intervencije ugotovi, da je protipožarni sistem na objektu v okvari ali pa je poškodovan zaradi požara. Zaradi velike količine dima ni znana točna lokacija požara v garaži. Vodja intervencije se odloči, da bo z dronom poskušal preiskati garažo in poiskati žarišče požara. Zaradi izpada dela omrežja 5G v garaži upravljanje drona ni mogoče. Vodja intervencije se odloči da bo v garažo poslal dve ekipi gasilcev, po tem ko preveri da v garaži še vedno deluje omrežje 5G, namenjeno IoT napravam. Zaradi varnosti morajo biti gasilci opremljeni s senzorji za merjenje življenjskih funkcij, senzorjem padca in tipko za klic v sili. Vodja intervencije tako lahko ves čas prek omrežja 5G spremlja gasilce pri njihovem delu in jih opozarja na morebitne nevarnosti. Ko se gasilci prebijejo do mesta požara, ga poskušajo omejiti, hkrati pa okoli požara postavijo temperaturne senzorje, tako da lahko vodja intervencije prek omrežja 5G sproti spremlja stanje v njegovi okolici. Druga ekipa gasilcev poskrbi za zavarovanje, s čimer omogoči prihod ostalih ekip in začetek gašenja. Ko je požar pogašen, gasilci s termovizijskimi kamerami preverijo stanje v garaži. Ker na določenih mestih obstaja nevarnost ponovnega vžiga, se vodja intervencije odloči za postavitev dveh termovizijskih kamer za spremljanje stanja prek noči. Video signal obeh kamer se do vodje intervencije prenaša prek zunanjega omrežja 5G. Intervencija se zaključi zjutraj naslednjega dne.«

VI. ZAKLJUČNA MISEL

V Sloveniji zmoremo soustvarjati tehnologije 5G, ki so ene ključnih za digitalno transformacijo za prehod v informacijsko družbo. Ob tem se moramo zavedati, da moramo pri tem sodelovati vsi, ne zgolj strokovnjaki s področja informacijskih in komunikacijskih tehnologij. Za uspešnost takšnega projekta je nujna tudi podpora okolja, ki mora biti spodbujena s konstruktivnimi političnimi odločitvami.

LITERATURA

[1] Boštjan Tavčar, LTE – tehnologija pametnih omrežij na področju zaščite in reševanja, VITEL, 2016
[2] NEXES, http://nexes.eu/the-nexes-concept/
[3] LET, http://www.3gpp.org/release-14
[4] Informacijska družba, https://sl.wikipedia.org/wiki/Informacijska_dru%C5%BEba
[5] Qualcomm, Leading the world to 5G: Cellular Vehicle-t-Everiythibg (C-V2X) technologies, June 2016
[6] European Commission, 5G for Europe: An Action Plan, 2016
[7] Hossian KhaLEGHI Bizaki, Towards 5G Wireless Networks, 2016, ISBN-10: 953-51-2834-5
[8] Erik Dahlman, Stefan Parkvall, Johan Skold, 4G, LTE-Advanced Pro and The Road to 5G, 2016, ISBN: 978-0-12-804575-6
[9] Dugie Standeford, Martin Sims, Dr. Jonathan Watson, The 4G/5G spectrum guide 2016, 2016

Boštjan Tavčar je diplomiral na Fakulteti za elektrotehniko v Ljubljani na univerzitetni smeri telekomunikacije. Od leta 1994 je zaposlen na Ministrstvu za obrambo, na Upravi Republike Slovenije za zaščito in reševanje, v zadnjih letih kot vodja Centra za obveščanje Republike Slovenije. Skrbi za uveljavitev in razvoj informacijskih in komunikacijskih sistemov in enotne evropske številke za klic v sili 112. Je avtor aplikacije za klic v sili za gluhe in naglušne WAP112, ki je bila predhodnica storitev klica v sili naslednje generacije in za katero je Uprava RS za zaščito in reševanje v letu 2009 prejela mednarodno nagrado Evropskega združenja za klic v sili EENA. Je pobudnik vzpostavitve sistema eCall v Sloveniji, aktivno pa je sodeloval tudi pri njegovem razvoju. V preteklosti je sodeloval pri različnih evropskih projektih, U2010, MONET, ABSOLUTE, HeERO in drugih. Danes sodeluje pri projektih i-HeERO in NEXES. Bil je tudi član medresorskih skupin za uvedbo enotnega digitalnega radijskega omrežja državnih organov Republike Slovenije. Boštjan Tavčar je predavatelj na Višji strokovni šoli za telekomunikacije, Šolskega centra za pošto ekonomijo in telekomunikacije v Ljubljani. Je avtor več strokovnih člankov s področja telekomunikacij, informatike in varstva pred naravnimi in drugimi nesrečami ter soavtor knjige »Gradniki telekomunikacijskih sistemov 1«.

Podporniki

Sponzors

Ericsson

Iskratel

Telekom Slovenije

AKOS

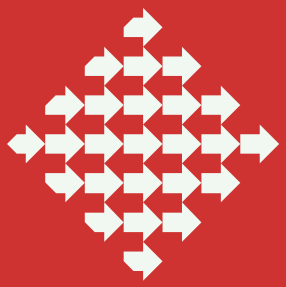
Amiteh

Univerza v Mariboru, FERI

strokovni

Univerza v Ljubljani, FE

strokovni



Slovensko društvo za elektronske komunikacije

Elektrotehniška zveza Slovenije