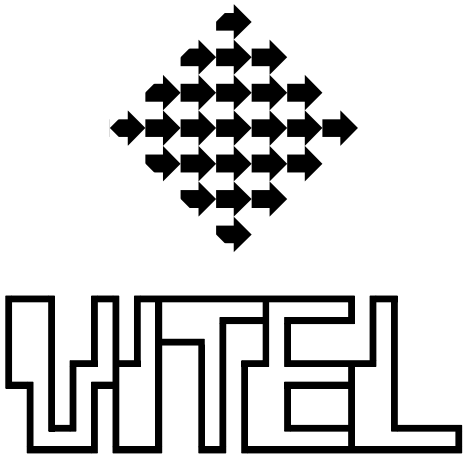
ELEKTROTEHNIŠKA ZVEZA SLOVENIJE
SLOVENSKO DRUŠTVO ZA ELEKTRONSKE KOMUNIKACIJE



Petindvajseta delavnica o telekomunikacijah

INTERNET STVARI

ZBORNIK REFERATOV

12. in 13. maj 2011 **Brdo pri Kranju, Slovenija**

Stegne 7
1521 Ljubljana, Slovenija

Organizira:

Elektrotehniška zveza Slovenije
http://www.ezs-zveza.si
Slovensko društvo za elektronske komunikacije
http://www.sikom.si

Pokrovitelj:

IEEE Communications Society

Uredili: Nikolaj Simič, Pavel Meše, Boštjan Vlaovič, Ana Robnik, Alojz Hudobivnik
Priprava za tisk: Tatjana Strahija, Laboratorij za telekomunikacije, UL FE
Oblikovanje naslovnice: Filip Samo Balan in Aleksander Vreže
Izdajatelj: Elektrotehniška zveza Slovenije
Tisk: Borut Verhovec s. p., Ljubljana
Število izvodov: 150

ISSN 1581–6737

Kazalo

Kazalo iii

Zgodovina dosedanjih delavnic VITEL in mednarodnih simpozijev VITEL (International Telecommunications Symposium) v

Uvodna beseda vi

Programsko-organizacijski odbor delavnice vii

Programski odbor dogodkov VITEL vii

Četrtek, 12. maj 2011

Smart Grids: A Transformation Journey . . . 2
Thierry Pollet
Internet stvari - izzivi in priložnosti . . . 6
Mihael Mohorčič
Odprta komunikacijska platforma IoT . . . 11
Andrej Kos, Urban Sedlar, Klemen Peternel, Mojca Volk, Janez Sterle, Luka Zebec, Tomaž Vidonja, Janez Bešter
Internet stvari: Spodbujanje ali regulacija? . . . 16
Urban Kunc
Internet stvari in vgrajena zasebnost . . . 24
Andrej Tomšič
Vloga IK tehnologij pri uvajanju konceptov pametnih omrežij . . . 27
Andrej Souvent, Tomaž Pfajfar, Igor Papič
Uporaba prilagajanja odjema in razpršene proizvodnje električne energije . . . 32
Gregor Černe, Zoran Marinšek, Mitja Bizjak
Infrastruktura za implementacijo pametnih omrežij - Zaključki projekta SUPERMEN . . . 37
Janez Šmid
Upravljanje storitev jedrnega omrežja . . . 43
Goran Uršič, Uroš Juvan, Janez Jurjevec
Postavitev senzorskega omrežja na infrastrukturi javne razsvetljave . . . 47
Miha Smolnikar, Carolina Fortuna, Matevž Vučnik, Marko Mihelin, Mihael Mohorčič
Optimalno upravljanje električnih porabnikov v inteligentnem domu . . . 53
Mark Umberger, Iztok Humar

Petek, 13. maj 2011

Building the Internet of Things . . . 58
Jari Arkko
Uporabnost omrežij Metro Wi-Fi za Internet stvari . . . 62
Rudolf Sušnik, Jure Sodja
Uporaba vsestranskega senzorskega vozlišča za podporo okoljskim aplikacijam . . . 67
Kemal Ališ, Marko Kastelic, Denis Škrabl, Miha Smolnikar, Tomaž Javornik, Mihael Mohorčič
Approaches to sustainable telcos: global action and local intelligence . . . 73
Fedor Gabrovšek, Simeon Lisec, Radovan Sernec
Integracija mobilnih in brezžičnih senzorskih omrežij . . . 77
Marko Pesko, Luka Vidmar, Mitja Štular

Predlog uvedbe davčno zanesljivih fiskalnih blagajn 81
Domen Baškovec
Internet stvari in mobilna omrežja 85
Primož Jenko, Iztok Saje
Security and Data Protection in the Internet of Things 90
Petr Pavlu
Low-Latency in Wireless Communications 93
Philipp Svoboda, Navid Nikaein, Raymond Knopp, Antonio Maria Cipriano, Srdjan Krco, Igor Tomić, Markus Laner, Eric Larsson, Yi Wu, Manuel Garcia Fuertes, Janie Baños, Nenad Željković, Djordje Marović, Divna Vučković
RFID tehnologija v IoT projektih 100
Andrej Planina
Vpliv telemedicine na življenje ljudi in na razvoj Slovenije kot EU regije - projekt eBIOMED 103
Uroš Stanič, Jana Stanič
Lokacijske storitve, RFID senzorji za uporabo v bolnišničnih okoljih 108
Matevž Mesojednik, Uroš Slak
Povezan dom postaja resničnost za ljudi in stvari 113
Slobodan Bodnaruk, Mitja Golja, Ana Robnik, Gregor Smolej
Interakcija s fizičnimi objekti v namene upravljanja komunikacijskih storitev 118
Darko Bodnaruk, Klemen Peternel, Urban Sedlar

Seznam avtorjev **122**

Zgodovina dosedanjih delavnic VITEL

— DELAVNICA o telekomunikacijah (1 ; 1993 ; Brdo pri Kranju): *ISDN omrežja in storitve v Sloveniji*
— DELAVNICA o telekomunikacijah (2 ; 1994 ; Brdo pri Kranju): *Mobilne in brezvrvične telekomunikacije*
— DELAVNICA o telekomunikacijah (3 ; 1995 ; Brdo pri Kranju): *Podatkovna omrežja in storitve v Sloveniji*
— DELAVNICA o telekomunikacijah (4 ; 1995 ; Brdo pri Kranju): *Načrtovanje, upravljanje in vzdrževanje komunikacijskih omrežij*
— DELAVNICA o telekomunikacijah (5 ; 1997 ; Brdo pri Kranju): *Varnost in zaščita v telekomunikacijskih omrežjih*
— DELAVNICA o telekomunikacijah (6 ; 1997 ; Brdo pri Kranju): *Zbliževanje fiksnih in mobilnih omrežij ter storitev*
— DELAVNICA o telekomunikacijah (7 ; 1998 ; Brdo pri Kranju): *Telekomunikacije in sprejetje Slovenije v Evropsko unijo*
— DELAVNICA o telekomunikacijah (8 ; 1999 ; Brdo pri Kranju): *Omrežja IP, internet, intranet, ekstranet*
— DELAVNICA o telekomunikacijah (9 ; 1999 ; Brdo pri Kranju): *Upravljanje omrežij in storitev*
— DELAVNICA o telekomunikacijah (10 ; 2000 ; Brdo pri Kranju): *Mobilnost v telekomunikacijah*
— DELAVNICA o telekomunikacijah (11 ; 2001 ; Brdo pri Kranju): *Dostop do telekomunikacijskih storitev*
— DELAVNICA o telekomunikacijah (12 ; 2002 ; Ljubljana): *Poslovne telekomunikacije*
— DELAVNICA o telekomunikacijah (13 ; 2002 ; Brdo pri Kranju): *Kakovost storitev*
— DELAVNICA o telekomunikacijah (14 ; 2003 ; Brdo pri Kranju): *Varnost v telekomunikacijskih sistemih*
— DELAVNICA o telekomunikacijah (15 ; 2003 ; Brdo pri Kranju): *Mobilni internet*
— DELAVNICA o telekomunikacijah (16 ; 2004 ; Brdo pri Kranju): *Pametne stavbe*
— DELAVNICA o telekomunikacijah (17 ; 2005 ; Brdo pri Kranju): *Telefonija IP (VoIP)*
— DELAVNICA o telekomunikacijah (18 ; 2005 ; Ljubljana): *Storitev trojček = Triple play*
— DELAVNICA o telekomunikacijah (19 ; 2007 ; Brdo pri Kranju): *Brezžični širokopasovni dostop*
— DELAVNICA o telekomunikacijah (20 ; 2007 ; Brdo pri Kranju): *Optična dostopovna omrežja*
— DELAVNICA o telekomunikacijah (21 ; 2008 ; Brdo pri Kranju): *Povsem IP–omrežja*
— DELAVNICA o telekomunikacijah (22 ; 2009 ; Brdo pri Kranju): *Širokopasovna mobilna omrežja*
— DELAVNICA o telekomunikacijah (23 ; 2009 ; Brdo pri Kranju): *Konvergenčne storitve v mobilnih in fiksnih omrežjih*
— DELAVNICA o telekomunikacijah (24 ; 2010 ; Brdo pri Kranju): *Prehod na IPv6*
— DELAVNICA o telekomunikacijah (25 ; 2011 ; Brdo pri Kranju): *Internet stvari*

in mednarodnih simpozijev VITEL (International Telecommunications Symposium)

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

Uvodna beseda

V času globalnih komunikacij, ko je podatkovni promet med napravami že zdavnaj prerasel promet med človeškimi uporabniki, so se pojavile nove tehnologije, ki omogočajo vrsto storitev, ki zahtevajo povezovanje naprav brez posredovanja človeka. Ob trenutnem trendu naraščanja števila naprav, ki se povezujejo v medmrežje, bo podatkovni promet med napravami popolnoma zasenčil promet med ljudmi in temu je treba nujno prilagoditi tudi omrežja, ki povezujejo naprave ter protokole, ki skrbijo za nemoteno povezovanje in prenos podatkov.

Med te storitve sodijo pametna omrežja (Smart Grids) za upravljanje proizvodnje in porabe električne energije, senzorska omrežja, aplikacije na osnovi RFID, e-zdravje, e-promet, pametne hiše, inteligentno urbano okolje in še bi lahko naštevali.

Vse te storitve nam omogočajo boljše in udobnejše pogoje bivanja, po drugi strani pa odpirajo kopico vprašanj, ki jih bomo morali rešiti, preden bodo vse te storitve zaživele v polnem razmahu. Industrija po vsem svetu se ukvarja s pripravo zmogljivih terminalskih in senzorskih naprav, podpornih sistemov za obdelavo ogromne količine podatkov ter komunikacijskih sistemov, ki bodo povezovali raznovrstne naprave v enotno medmrežje. In tako se rojeva internet stvari.

Pametna elektroenergetska omrežja bodo v najkrajšem času prinesla pomembne prihranke in s tem povečala konkurenčnost industrijskih podjetij, hkrati pa zaradi pospešenega uvajanja alternativnih virov energije zmanjšala izpuste toplogrednih plinov, zaradi inteligentnega odjema energije pa znižala vršno porabo ter s tem stroške prenosa energije.

E-zdravje je eno od področij, ki bo najbolj vplivalo na kakovost življenja posameznikov, pri čemer gre pri tem tako za povečevanje možnosti zdravljenja kot tudi učinkovitejšo preventivno zdravstveno dejavnost. Mogoče bo ravno pri e-zdravju sodelovalo največ raznorodnih tehnologij, kot so senzorji za merjenje vrste življenjskih parametrov, merilne in nadzorne naprave, shrambe podatkov, e-identifikacija in podobno. Izmenjava podatkov o bolnikih in njihovih anamnezah je gotovo eno od vprašanj, od katerih je odvisna uspešna realizacija e-zdravja, saj je izmenjava teh podatkov zelo občutljiva zadeva zaradi varovanja osebnih podatkov in zasebnosti.

Tudi e-promet je področje, ki bo dolgoročno prineslo zmanjšanje stroškov prevoza, izgube časa na poti, zmanjšanje izpustov toplogrednih plinov in posredno pripomoglo k optimizaciji industrijske proizvodnje. Prvi koraki so bili narejeni, uvajamo sisteme elektronskega cestninjenja brez zaustavljanja, prihaja pa pametno zaznavanje in upravljanje prometa v povezavi s pametnimi vozili in prometno signalizacijo.

Med bolj pereča vprašanja uvajanja interneta stvari gotovo sodita tudi vprašanje regulacije interneta ter varovanje zasebnosti in zaščita osebnih podatkov. Zato je tem vprašanjem posvečena cela sekcija, poleg tega pa bomo o tej temi posebej govorili tudi na okrogli mizi, ki bo gostila eminentne strokovnjake s področja interneta stvari, zaščite zasebnosti in varovanja podatkov, gradnje omrežij za internet stvari ter uporabnike storitev interneta stvari.

Poglavitni namen delavnice je osvetliti zgoraj omenjena področja, izmenjati pridobljene izkušnje ter spodbuditi širšo slovensko tehnološko in poslovno javnost na področju telekomunikacij in informatike k razpravi in izmenjavi mnenj z namenom povečanja motivacije pri razvoju in napredku tega področja ter oblikovanju ustreznih ter učinkovitih strategij. Zanimivost področja se odraža v številnih iniciativah, združenjih, raziskovalnih aktivnostih in dogodkih, namenjenih razreševanju navedenih izzivov širom sveta.

Nikolaj Simič
Predsednik programskega odbora delavnice

Programsko-organizacijski odbor delavnice

Nikolaj Simič, predsednik
Tom Erjavec
Alojz Hudobivnik
Iztok Humar
Marko Jagodič
Janez Keršmanc
Pavel Meše
Ana Robnik
Boštjan Vlaovič

Programski odbor dogodkov VITEL

Alojz Hudobivnik, predsednik
Andrej Andoljšek
Janez Anžič
Boštjan Batagelj
Janez Bešter
Matjaž Blokar
Marko Bonač
Marjan Bradeško
Zmago Brezočnik
Tom Erjavec
Bogomir Horvat
Iztok Humar
Marko Jagodič
Avgust Jauk
Gorazd Kandus
Andrej Kos
Anton Kos
Ivo Kranjčevič
Miha Krišelj
Savo Leonardis
Pavel Meše
Ana Robnik
Nikolaj Simič
Jaka Sodnik
Rudolf Sušnik
Mitja Štular
Sašo Tomažič
Anton Umek
Boštjan Vlaovič
Aleksander Vreže
Mira Zupančič
Drago Žepič

Četrtek, 12. maj 2011

Smart Grids: A Transformation Journey

Thierry Pollet, Energy - Strategic Industries Division, Alcatel-Lucent

Abstract — The Smart Grid blends the electricity network with a communications network as to ensure guaranteed and safe delivery of energy in an environment that meets the European 20-20-20 guidelines. This paper focuses on the transformation of the transmission and distribution energy network towards a smart grid. It will outline the impact on communications, the services and the operational environment.

Keywords — Smart Grids, IP/MPLS, convergent networks, Service Oriented Architecture

I. The European Grid: Key Data

Since Thomas Edison developed and built the first electricity generating plant in New York City in the 1870s, the grid has become one of the largest systems deployed by mankind. A net installed electrical energy capacity of 800 GW (SI: 2,8 GW) powers the activities of about 500 million Europeans (EU27) (SI: 2.2 million) [1,2]. The annual electricity consumption (Industry, Transport, Households and Services) accumulates to 2.856 TWh (SI: 12,8 TWh). Households contribute to about one third of the energy consumption. The transmission network covered by the ENTSO-E members consists of about 300 000 km of HV lines [3].

II. Electricity Market & Regulation

The European electricity market has fundamentally been reshaped by the Electricity Directive 96/92/EC (1999) on liberalization of the national electricity markets in Europe. This Directive distinguishes the market roles of supply of energy vs. transport and distribution. It stipulates free individual choice of supplier, irrespective the location and that management of the grid remains the responsibility of the TSO whereas suppliers determine the sourcing (production and/or import). In Europe, the DNO and TSO domain are regulated. Non-regulated actors are: energy suppliers, local producers, Balance Responsible Party (BRP), Trader, Balance Supply Party or Ancillary Service Supplier. With smart grid, additional actors are expected to be created such as: ESCO (energy service companies), Distribution Generation Aggregators, Storage Capacity aggregators, Data Clearing House etc.

In January 2007, the European Commission adopted a communication (COM(2007)1) [5] proposing an energy policy for Europe, with the goal to combat climate change and boost the EU's energy security and competitiveness. This set out a new energy path towards a more secure, sustainable and low-carbon economy. The following targets were endorsed:

– reducing greenhouse gas emissions by at least 20 % by 2020 (compared with 1990 levels);
– improving energy efficiency by 20 % by 2020;
– raising the share of renewable energy to 20 % by 2020.

III. Challenges for the Grid

Demand: the European annual average consumption growth between 2010-2015 is expected to be about 1.26 % , whereas the annual peak load is growing even faster [3]. In a traditional business-as-usual scenario, this would require timely investment in new generation capacity. In the context of the European Directive, this is to be addressed by a combination of energy efficiency programs, and introduction of renewable energy sources in combination with low carbon generation capacity [4]. Slovenia is one of the countries where the largest annual average consumption growth is expected. The annual demand of the distribution companies has been rising at a rate of 3 % (1997-2007), and forecast to be around 2.5 % in the coming years [2].

Supply Mix: the electricity sector has a crucial role in cutting carbon emissions. The supply mix (Table 1: Slovenian energy mix) is to evolve to include a higher percentage of low carbon generating energy supply. Renewables (RES) will play an increasingly important role in the energy mix. This comprises hydro, wind, biomass, geothermal and solar energy. This can be achieved through large scale RES but as well with microgeneration: smaller distributed sources of PV and wind. The latter implies that distribution networks are to support bi-directional power flows. The intermittent nature of the RES forces the industry to rethink the power-meets-demand paradigm. In addition, the Japanese earthquake forces a debate on accelerated reduction of the nuclear component in Europe's future energy mix.

Table 1: Slovenian Gross Inland Energy Consumption, per Source of Energy (%) [6]

Year	Oil & petrolum	Gas	Solid fuels	Nuclear	Renewable
2006	40,7	13,3	20,3	18,8	8,6

2009	37,3	11,9	20,4	21,2	12,7

IV. THE REGULATED ENVIRONMENT

A. *Transmission Service Operators*

ENTSO-E[1] represents 41 TSO's from 34 countries. It develops 2-yearly a non-binding community wide 10 year network development plan (TYNDP), aligned with the EU energy policy priorities:

– SOS: Security of Supply
– RES: Tackling climate change and integration of Renewable Energy Sources
– IEM: Economic efficiency and realization of the Internal Energy Market.

In the TYNDP of 2010, TSO's lay out plans to support large scale intermittent resources to be integrated in the transmission network and to support international power flows to maintain system balance. At European level, the plans are geared to support massive renewable integration in the North (wind in remote and possibly off shore areas) and South part of Europe (wind, hydro and solar in the Iberian Peninsula). In addition, East-West and North-South flows in the South-East and Central South Regions are to be supported as to ensure power balancing in the countries involved (e.g. export and transit towards Italy). In Slovenia, the main priorities are:

– the installation of new HV (400 and 220KV voltage level) and connections to support international power transit (Austria, Hungary, Croatia, Italy) since changing and stronger power flows cause growing operational security concerns (transit bottleneck).
– the development of the Slovenian inner grid and their interconnections in order to be able to meet the future requirements, aiming at completing a 400 kV ring.
– phase shifting transformers as to remove the power flow bottleneck at the Slovene-Italian border in supporting increased transit power flows from Slovenia into Italy.

Smart Grids for the TSO take form under:

– support for increased transmission capacity
– enhanced flexibility and controllability of power flows
– close to real time system data
– improved real-time monitoring and controllability of the operational status of the system.
– enhanced flexibility and controllability of power flows, also permitting increased transmission capacity.

Note that Slovenia is currently yearly importing about 20 % of demand energy. Currently, its actual generation capacity falls 20 % short of the winter peak demand.

B. *Distribution Network Operators*

The Distribution Network Operator landscape in Europe is very country specific. Some countries are characterized by a single or few dominating DNO's, whereas in others, the landschape is split between a set of about equal sized DNO's. In some countries there are many DNO's, which can be very different in size depending on the region they serve (Figure 1).

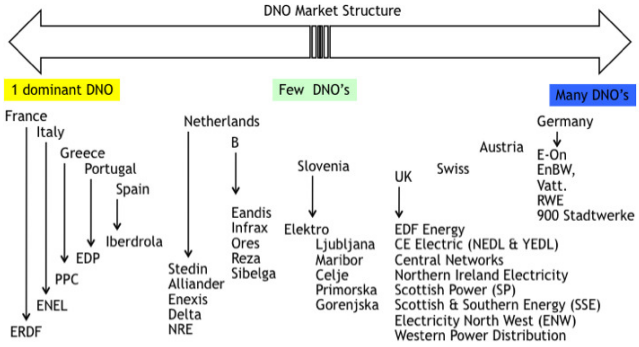


Figure 1: DNO Market Structure

Smart Grids for DNOs means:

– enabling the network to integrate users with new requirements
  – supporting of New types of Loads (E.g. EV, storage) and new sources (DES)
– enhancing efficiency in day-to-day grid operation
  – automated fault identification, isolation and optimal grid reconfiguration after faults
  – enhanced monitoring and control of power flows and voltages.
  – enhanced monitoring of network components down to LV
  – monitoring of network assets
– ensuring network security, system control and quality of supply
  – improved monitoring of safety particularly in public areas during network ops
  – system security assessment and management of remedies, including actions against terrorist attacks and cyber threats
– better planning of future network investment and improved infrastructure life cycle management.
– improved asset management (energy + telco assets)

V. SMART GRIDS: BRIDGING ENERGY AND COMMUNICATION NETWORKS

Figure 2 depicts the Smart Grid Architecture Diagram [7], encompassing the TSO as well as the DNO domain[2]. Robust communications and data

[1] Slovenia belongs to the Continental-South-East Regions.

[2] For reasons of simplicity, this picture does not make strict separation between the administrative domain of the TSO and the

handling will become critical as the variety of new energy applications grows. Figure 3 shows the communication requirements for the various utility applications.

Traditional utility communications use TDM circuit based technologies in support of utility operational services such as SCADA, tele-protection, safety voice, condition monitoring and utility IT services such as office voice and call center.

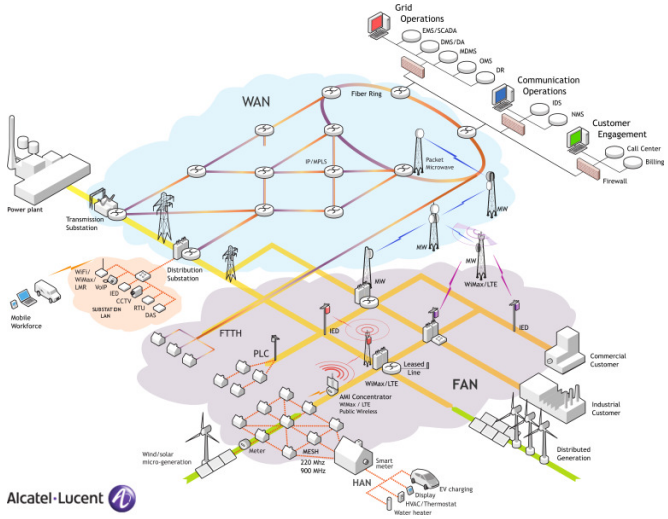


Figure 2: Smart Grid Architecture

Increased operational efficiency, lower costs, increased flexibility, enhanced security are drivers towards a converged communications network. IP/MPLS technology supports both legacy TDM (SDH), and Ethernet-IP services. IP/MPLS offers a modern utility communications infrastructure aimed at:

– satisfying the growing need for IP and Ethernet communications such as eSCADA, VoIP, CCTV, GOOSE, IP mobile radio
– transition from TDM to a mix with growing packet traffic; packet traffic dominating in the future
– allowing access to critical information in real time
– packet-traffic QoS, with dedicated bandwidth for critical traffic as to prioritize mission-critical applications over other traffic
– integrating new applications in the communications network
– security, automation, collaboration
– supporting centralized network management and simplified maintenance

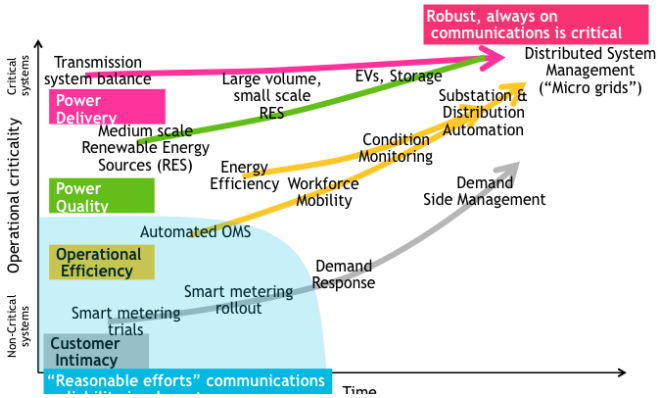


Figure 3: Coms Characteristics for Utility Services

Support of TDM services over IP/MPLS is achieved through CES (circuit emulation service). There are two principle structures available:

– CESoP — Circuit Emulation Service over Packet provides fractional services (nxDS0)
– SAToP — Structure Agnostic TDM over Packet provides unstructured T1/E1 services

It has been proven that even the most stringent utility services in terms of delay such as teleprotection[3] can be supported over IP/MPLS [8].

Extension of a converged communication technology further down the energy network towards the end-points will benefit new applications in the distribution network. This is not restricted to the expected mass roll-out of smart (residential) metering, but as well for distribution automation: fault management, remote monitoring, volt/Var reduction and integration of distributed energy resources into the grid (Figure 4).

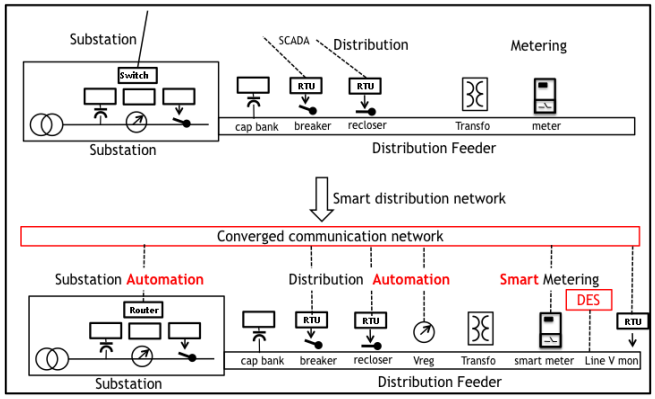


Figure 4: Smart Distribution Networks

Smart Grids communications will enable the utility operations to reach far out in the energy network as to collect information from the field devices. Wheras this massive amount of information may benefit the various utility business domains the current utility applications may not be ready. Traditional applications (EMS,

DNO. In reality, each has an own communications networks and IT environment.

[3] Standards specify delays of 8-12ms for teleprotection (IEEE1646-2004)

OMS, SCADA, Planning) are silos. A challenge is the transformation of the IT environment to adhere to service oriented principles (SOA): the capability of the applications to exchange data through abstract interfaces. Data management refers to the collection, validation, correlation, transformation, structuring and storage of the various data channels collected from the gid. A common information model allows the various applications to access and exchange this data, in support of the smart grid operations.

VI. SUMMARY

IP/MPLS transformation of existing utility communication networks (WAN and Sub-station LAN) is a foundation of the smart utility in support of future smart grid applications that by design will be packet oriented. Legacy (non-IP) services can continue to be supported.

Smart distribution networks will produce large amounts of data that now become available to the operational IT environment. This will create significant value to operations provided that the IT environment will be transformed to adhere to SOA principles.

VII. GLOSSARY

BRP	Balance Responsible Party
DES	Distributed Energy Sources
DNO	Distribution Network Operator
EMS	Energy Management System
ESCO	Energy Service Company
MPLS	Multi-protocol label switching
OMS	Outage Management System
QOS	Quality of Service
RES	Renewable Energy Sources
SCADA	Supervisory Control and Data Acquisition
SOA	Service Oriented Architecture
TSO	Transmission Service Operator
VoIP	Voice over IP

LITERATURE

[1] Eurostat, statistics on population and energy, http://epp.eurostat.ec.europa.eu

[2] Development Strategy of the Electrical Power System of the Republic of Slovenia, Electro-Slovenia, Ljubljana, 2009.

[3] Ten Year Development Plan 2010-2020, ENTSO-e, https://www.entsoe.eu

[4] The National Energy Efficiency Action Plan 2008–2016, Government of Slovenia, 2008.

[5] http://ec.europa.eu/energy/energy_policy/doc/01_energy_policy_for_europe_en.pdf

[6] EU Sustainable Energy Week, Share of renewables in the EU27 energy supply almost doubled between 1999 and 2009, April 2011.

[7] Alcatel-Lucent, Dynamic Communications for maintaining power quality, http://enterprise.alcatel-lucent.com/smartgrid/, 2010.

[8] Alcatel-Lucent, Altalink: Building new high-speed IP communications network linking substations through Alberta, http://enterprise.alcatel-lucent.com/smartgrid/case-study-altaLink.html, 2010.

THIERRY POLLET currently holds the position Smart Grid Solution Architect Lead with Alcatel-Lucent. In coordination with business development he translates market requirements into solution and product requirements. He articulates to utility customer capture leads the value proposition of Alcatel-Lucent in the electricity sector, and works with these accounts towards architectures and solutions to be implemented in their network and IT department (Thierry_Pollet@me.com).

Internet stvari – izzivi in priložnosti

Mihael Mohorčič
Odsek za komunikacijske sisteme, Institut "Jožef Stefan"

Povzetek — Internet stvari predstavlja enega izmed stebrov interneta prihodnosti, ki bo z uporabo standardiziranih komunikacijskih protokolov in omrežne infrastrukture, sposobne samostojne konfiguracije, razširil Internet na heterogene fizične in navidezne stvari, ki nas obdajajo v vsakdanjem življenju. Te stvari bodo komunicirale med seboj ali s končnimi uporabniki in tako z novo dodano vrednostjo v obliki informacije o stvarnem stanju postale aktivne udeleženke procesov na različnih področjih človeškega udejstvovanja. Ta koncept zahteva rešitev številnih izzivov na različnih področjih, hkrati pa odpira priložnosti za vrsto novih storitev, aplikacij in poslovnih modelov. Prispevek podaja pregled področij uporabe Interneta stvari, ki potrjuje njegovo vseprisotnost ter nakazuje priložnosti in pričakovan vpliv na industrijo, okolje in družbo. Nadalje sta na kratko predstavljeni temeljni tehnologiji Interneta stvari, to sta radiofrekvenčna identifikacija ter brezžična senzorska in aktuatorska omrežja, identificirane pa so tudi nekatere druge podporne tehnologije. Prispevek se zaključuje z raziskovalni in razvojni izzivi, ki stojijo na poti širše vpeljave koncepta v vsakdanje življenje, in trenutnimi trendi razvoja.

Ključne besede — Internet stvari, Internet prihodnosti, Splet stvari, senzorska in aktuatorska omrežja

Abstract — The Internet of Things represents one of the four main pillars of the Future Internet. Using standard and interoperable communication protocols and self configurable dynamic network infrastructure, it will extend the Internet to include heterogeneous “smart” physical and virtual “things” that are part of our living environments. These things will communicate to each other as well as with end users. With the added value information about the actual status of things they will play an active role in various procedures in different areas of human activities. This opens an opportunity for a range of new services, applications and even business models, but at the same time poses several challenges requiring further research. In this paper we provide an overview of the application domains which confirms the planned omnipresence of the Internet of Things, reveals its opportunities and the expected impact on the industry, environment and society. The two fundamental technologies of the Internet of Things are briefly presented, the radio-frequency identification and wireless sensor and actuator networks, and some of the supporting technologies are also identified and discussed. The paper concludes with the research and development challenges that hinder broader introduction of the concept in everyday life and with the current development trends.

Keywords — Internet of Things (IoT), Future Internet, Web of Things (WoT), Sensor and Actuator Networks

I. UVOD

Mineva že več kot 10 let od zametka koncepta, ki je danes znan pod imenom Internet of Things, njegov izvor pa pripisujejo raziskovalni sferi, ki se je okrog leta 2000 ukvarjala s prehodom s črtnih kod na tehnologijo RFID [1]. Čeprav je bilo v tem času v razvoj Interneta stvari vloženih mnogo raziskovalnih naporov, pa se resnejši premiki kažejo šele v zadnjem letu ali dveh, ko so se za idejo ogrela podjetja kot sta HP s CeNSE platformo in IBM s konceptom Smarter Planet, in jo začela uporabljati podjetja kot Nike v pametni obutvi Nike+ [2].

Velik pomen za razvoj Interneta stvari ima tudi prihod večnamenskih večsenzorskih naprav kot so pametni telefoni. Ti so tipično opremljeni z GPS sprejemnikom, merilniki pospeška, merilniki osvetlitve in temperature, in lahko poleg merjenja moči radijskega signala spremljajo tudi navade uporabnikov. Pojavljajo pa se že prvi pametni telefoni z vgrajenimi brezžičnimi tehnologijami kot so DASH7, NFC in Bluetooth Low Energy za neposredno povezovanje s "pametnimi stvarmi".

Začetnemu obdobju razvoja Interneta stvari bo v kratkem sledila tudi ekonomija obsega in s tem povezan padec cen in predvidena hitra osvojitev tehnologij. Tako Intel za leto 2015 napoveduje 15 milijard naprav povezanih v splet, Ericsson pa je v svojih napovedih še bolj drzen in za leto 2020 napoveduje kar 50 milijard različnih naprav z dostopom na splet.

Ne glede na točnost omenjenih napovedi je že na prvi pogled jasno:

- da danes prevladujoči internetni protokol IPv4 ne more zadostiti potrebam po priključevanju tolikšnega števila naprav;
- da bodo v kratkem v splet povezane naprave, za katere si tega še danes niti ne predstavljamo; ter
- da bo sčasoma obseg prometa komunikacije med napravami (*angl. machine-to-machine, M2M*) presegel obseg prometa komunikacije med ljudmi (*angl. human-to-human, H2H*) ter med napravami in ljudmi (*angl. machine-to-human, M2H*).

Navedeno nakazuje, da je pri nadaljnjem razvoju in vpeljevanju Interneta stvari pričakovati konsolidacijo na področju tehnologij in protokolov. Strojna oprema, s katero se bodo opremljale stvari oziroma bo v njih

vgrajena, pa se bo morala prilagajati zahtevam področja uporabe in tudi konkretnim aplikacijam.

Namen prispevka je predvsem podati izzive in priložnosti, s katerimi se srečujemo pri razvoju in vpeljevanju koncepta Interneta stvari. V drugem poglavju umestimo koncept Interneta stvari v Internet prihodnosti in ga razmejimo od konceptov spleta stvari in senzorskih omrežij. Tretje poglavje navaja reprezentativna področja uporabe Interneta stvari, četrto poglavje pa podaja kratek opis temeljnih tehnologij in identificira nekatere ključne podporne tehnologije. V petem poglavju so našteti pomembnejši raziskovalni in razvojni izzivi, ki jih je potrebno rešiti pred širšo vpeljavo Interneta stvari, podani pa so tudi trenutni trendi razvoja, prispevek pa zaključuje šesto poglavje z diskusijo o raziskavah in razvoju področja v Evropi in v Sloveniji.

II. UMESTITEV INTERNETA STVARI V INTERNET PRIHODNOSTI

Internet stvari poleg Interneta uporabnikov, Interneta vsebin in Interneta storitev predstavlja enega štirih stebrov Interneta prihodnosti [3].

Z vidika *Interneta uporabnikov* bo moral Internet prihodnosti podpirati interaktivno vključevanje vse večjega števila različnih uporabnikov z različnimi potrebami in pričakovanji. To bo privedlo do kreiranja virtualnih skupnosti ter izmenjave znanj in izkušenj med vključenimi uporabniki, pri čemer bodo pri zbiranju ogromnih količin informacij in znanj pomembno vlogo odigrale semantične tehnologije.

V okviru *Interneta vsebin in znanj* se bodo razvili mehanizmi, ki bodo presegli samo zbiranje in uporabo informacij. Omogočili bodo napredno obdelavo in razširjanje znanja na lokalni in globalni ravni ter ob tem vključevali zavestne intelektualne aktivnosti. Razvite bodo na primer napredne spletne aplikacije in večpredstavnostni iskalniki, ki bodo dajali znanje na voljo tako človeškim uporabnikom kot napravam oziroma stvarem.

Internet stvari lahko opišemo kot dinamično globalno omrežno infrastrukturo, ki bo z uporabo standardnih komunikacijskih protokolov in sposobnostjo samostojne konfiguracije Internetu prihodnosti dodala zmožnost interakcije z realnimi fizičnimi objekti. Vključila jih bo v poslovne, informacijske in družbene procese, ki so del vsakdanjega življenja. Na ta način dobimo tako imenovano pametno okolje, v katerem lahko preko konteksta uporabe določenih stvari aktivno vlogo igrajo tudi ljudje. V tem okolju lahko rečemo, da povezane stvari predstavljajo storitev oziroma so same uporabniki storitev.

Internet prihodnosti bo spremenil tudi način zagotavljanja in izvajanja storitev tako uporabnikom kot povezanim stvarem in napravam. V okviru *Interneta storitev* je poudarek na storitveno orintiranem računalništvu, kontekstualiziranih in proaktivnih storitvah in orkestraciji storitev.

V povezavi z Internetom stvari naletimo na vrsto sorodnih konceptov, ki so lahko celo vsebovani v konceptu Interneta stvari. Predvsem je potrebno ločiti med Internetom stvari, spletom stvari (*angl. Web of Things*, *WoT*), komunikacijo med napravami (M2M) in brezžičnimi senzorskimi omrežji (*angl. Wireless Sensor Network, WSN*).

Pri Internetu stvari gre za funkcionalno, tehnološko in aplikacijsko heterogene stvari in predmete, tipično opremljene s senzorji, aktuatorji, RFID značkami, in podobno. Te stvari so enoznačno prepoznavne, lahko jih lociramo, naslovimo in nadziramo preko Interneta ter so z uporabo ustreznih tehnologij in standardiziranih komunikacijskih protokolov povezane v globalno omrežje. Stvari z enakimi komunikacijskimi zmogljivostmi se lahko z uporabo žične ali brezžične komunikacije povezujejo med seboj in obdelujejo izmenjane podatke v skladu z vnaprej dogovorjenimi pravili. Pri tem bodo pomembno vlogo igrale semantične tehnologije, s pomočjo katerih bomo lahko opisali tudi pristojnosti posameznih stvari. Na podlagi te splošne dostopnosti stvari se bodo razvile nove aplikacije, ki bodo bistveno spremenile dojemanje in upravljanje različnih predmetov in postopkov ter s tem vplivale na kakovost in način življenja.

Za razliko od Interneta stvari, ki omogoča dostopnost in povezovanje naprav in stvari, gre pri spletu stvari za integracijo vgrajenih naprav v splet z uporabo spletnih protokolov in storitev kot so HTML, XML, RSS in drugih, torej za dostopnost podatkov z naprav in stvari. Posebno vlogo v okviru povezanih vgrajenih naprav imajo senzorska omrežja, kjer gre običajno za brezžično povezana prostorsko porazdeljena vozlišča, ki skupno opazujejo oziroma spremljajo določen fizikalni ali kemijski pojav.

III. REPREZENTATIVNA PODROČJA UPORABE

Po napovedih naj bi Internet stvari s svojo vseprisotnostjo v stvareh in predmetih, ki nas obdajajo, izrazito vplival na praktično vsa področja človeškega udejstvovanja. Literatura je polna različnih primerov uporabe, od najbolj vsakdanjih, katerih zametke najdemo v omejenih oblikah že danes, do futurističnih, ki se najbrž še vrsto let ne bodo uresničili.

Glavne domene uporabe Interneta stvari obsegajo industrijo, okolje in družbo. V industrijski domeni gre za uporabo pametnih povezanih stvari v podporo finančnim in komercialnim transakcijam med različnimi organizacijami, torej za aplikacije nadzora in krmiljenja proizvodnje, transporta in logistike,

ponujanja storitev bančnega sektorja in javne uprave, itd.

Domena okolja obsega aktivnosti v zvezi z zaščito, nadzorom in razvojem naravnih virov. Aplikacije segajo od preciznega poljedelstva in reje do upravljanja z energetskimi viri, upravljanja z okoljem, nadzora življenjskih habitatov, ipd.

V družbeni domeni pa je vloga Interneta stvari v razvoju in vključevanju različnih skupnosti, mest in ljudi in obsega predvsem storitve za izboljšanje participacije državljanov in različnih družbenih struktur v javnem življenju.

Primeri področja uporabe v navedenih domenah so [4]:

- nadzorni sistemi in energetska učinkovitost v aeronavtiki,
- nadzorni sistemi v avtomobilski industriji, komunikacija med vozili ter komunikacija z obcestno infrastrukturo,
- podpora pametnim zgradbam (avtomatizacija, samodejno odčitavanje energetskih števcev, brezžični nadzor itd.),
- integracija osebnih telesnih omrežij z medicinsko tehnologijo za varovanje zdravja, nadzor vitalnih znakov, pozicioniranje, določanje lokacije v realnem času, in podobno,
- sistemi za nadzor in podporo mobilnosti in samostojnemu življenju starajoče se populacije,
- poodporni sistemi za prodajo, logistiko in upravljanje z dobavno verigo,
- podpora proizvodnji in upravljanju z življenjskim ciklom produkta,
- sistemi za nadzor okolja in življenjskih habitatov,
- podporni sistemi za poljedelstvo in rejo za povečanje učinkovitosti pridelave in boljšo sledljivost.

Uporaba tehnologij Interneta stvari na naštetih področjih odpira priložnost za nove poslovne koncepte in storitve na podlagi podatkov o fizičnih stvareh v realnem času, vpogled in boljše razumevanje kompleksnih postopkov, učinkovitejše ravnanje v primeru različnih nesreč, nadzor degradacije naravnega okolja, nadzor človeških aktivnosti, izboljšanje učinkovitosti rabe energije in drugo.

IV. TEHNOLOGIJE INTERNETA STVARI

Koncept Interneta stvari sloni na vrsti komplementarnih tehnologij med katerimi pa za temeljne tehnologije, ki povezujeta fizični svet z digitalnim, veljata radiofrekvenčna identfikacija (*angl. Radio-Frequency Identification, RFID*) ter brezžična senzorska in aktuatorska omrežja (*angl. Wireless Sensor and Actuator Networks, WSAN*).

Radiofrekvenčna identifikacija omogoča označevanje stvari in predmetov z elektronsko oznako ter s pomočjo ustreznega čitalca brezžično spremljanje fizičnega stanja, v katerem se označena stvar ali predmet nahaja. Elektronska oznaka je v splošnem sestavljena iz integriranega vezja in antene, lahko pa je opremljena tudi s senzorji ter v primeru aktivnega RFID sistema z baterijami oziroma sklopom za zbiranje energije iz okolja obratovanja. Glede na način napajanja oddajnika torej ločimo med pasivnimi in aktivnimi RFID sistemi, ki se posledično razlikujejo tudi po velikosti, ceni in največjim dometom med oznako in čitalcem. Trenutno so med pomembnejšimi aktivnostmi na področju razvoja RFID sistemov globalna standardizacija, usklajevanje označevanja in interoperabilnost sistemov, na raziskovalnem področju pa miniaturizacija in integracija s specifičnimi senzorji.

Komplementarni RFID oznakam, ki so še vedno v največji meri uporabne za identifikacijo v povezavi z lokacijo označenega predmeta in čitalca, so senzorji in akuatorji. Ti se vgradijo ali namestijo na stvari in predmete ter se uporabljajo za zaznavanje najrazličnejših fizikalnih in kemijskih veličin in pojavov. Miniaturizacija senzorjev in aktuatorjev ter njihova namestitev na elektronska vezja (t.i. platforme) z mikrokrmilniki in komunikacijskimi moduli omogoča zajemanje, procesiranje, hranjenje in pošiljanje izmerjenih veličin neposredno ali preko več vmesnih platform običajno preko prehoda na strežnik s podatkovno bazo. Platforme se razlikujejo po vrsti lastnosti in zmogljivosti, v večini primerov pa se v senzorska in aktuatorska omrežja povezujejo z uporabo brezžičnih komunikacijskih tehnologij. Z namenom zagotavljanja medsebojnega delovanja heterogenih platform se je razvilo več komunikacijskih standardov. Na fizičnem sloju in sloju nadzora dostopa do medija MAC je nedvomno najpomembnejši in najbolj razširjen standard IEEE 802.15.4. Ta služi kot osnova različnim standardom za povezovanje senzorskih in aktuatorskih vozlišč v omrežja kot so ZigBee[1], MiWi[2], WirelessHART[3], 6LoWPAN[4], in drugi. Pri senzorskih in aktuatorskih omrežjih pogosto naletimo še na tehnologijo komunikacije bližnjega polja (*angl. Near Field Communications, NFC*), na različice standarda Bluetooth[5] in tudi na WiFi[6].

Prav veliko število nekompatibilnih komunikacijskih standardov je privedlo do tega, da lahko stvari in predmeti v različnih omrežjih sodelujejo le preko rešitev na aplikacijskem sloju z uporabo

[1] http://www.zigbee.org/
[2] http://www.microchip.com/stellent/idcplg?IdcService=SS_GET_PAGE&nodeId=2113&param=en520414
[3] http://www.hartcomm.org/
[4] http://www.6lowpan.org/
[5] http://www.bluetooth.com/
[6] http://www.wi-fi.org/

spletnih tehnologij kot so SOAP, XML in REST. Te spletne tehnologije že tudi prilagajajo za uporabo na strojni opremi z omejeno procesno in energetsko zmogljivostjo.

Poleg tehnologij RFID ter brezžičnih senzorskih in aktuatorskih omrežij je za koncept Interneta stvari ključnih še več podpornih tehnologij in njihova vertikalna integracija. Med temi velja izpostaviti storitveno orientirano arhitekturo (*angl. Service Oriented Architecture, SOA*), dinamično sestavljanje storitev in omrežij, virtualizacijo, semantične tehnologije, in koncept programske povezovalne platforme (*angl. middleware*), ki povezuje fizično zajemanja podatkov iz okolja z aplikacijami, ki te podatke potrebujejo.

Za vpeljavo Interneta stvari je izrednega pomena tudi prihod večnamenskih naprav z vgrajenimi senzorji kot so pametni telefoni, ki so tipično opremljeni z GPS sprejemnikom, merilniki pospeška, merilniki osvetlitve in temperature, za povezovanje z drugimi napravami pa lahko uporabljajo že vgrajene komunikacijske vmesnike.

V. IZZIVI IN TRENDI RAZVOJA

Kljub pomembnemu napredku na področjih identifikacijskih, senzorskih in aktuatorskih tehnologij je pred širšo vpeljavo koncepta Interneta stvari še vrsta raziskovalnih in razvojnih izzivov, ki jih je potrebno rešiti. Med pomembnejše izzive štejemo [5][6][7]:

- sposobnost integracije heterogenih naprav, tehnologij in storitev,
- brezžično povezljivost v okviru omejitev glede porabe energije, izvedbe antene, uporabe radijskih tehnologij itd.,
- skalabilnost komunikacijskih protokolov na različnih slojih,
- razvoj novega transportnega protokola prilagojenega napravam z omejenimi zmogljivostmi,
- problematika imenovanja, naslavljanja, identifikacije in upravljanja z mobilnostjo,
- zagotavljanje zasebnosti podatkov in zaščite pred nepooblaščenim dostopanjem do stvari in podatkov,
- karakterizacija prometa značilnega za komunikacijo med napravami, določitev zahtev po kakovosti storitev s stališča naprav in shem za njihovo zagotavljanje,
- sposobnost naprav za konfiguriranje, upravljanje in optimizacijo samih sebe v skladu z zavedanjem o svojem kontekstu,
- učinkovito upravljanje z energijo in zbiranje energije iz okolja obratovanja,
- vertikalno integracijo rešitev zgornjih raziskovalnih in razvojnih izzivov.

Navedeni izzivi so medsebojno povezani, nekatere rešitve pa so pogojene tudi s specifičnimi zahtevami področja uporabe. Kljub temu so pri različnih rešitvah vidni nekateri skupni trendi kot so:

- Modularna in odprta zasnova strojne in programske senzorske platforme (npr. Arduino[7], Versatile Sensor Node[8], itd.);
- Odprte platforme s podporo semantičnih tehnologij za zbiranje, napredno obdelavo in dajanje na razpolago velikih količin ustrezno anotiranih podatkov v realnem času iz različnih vrst senzorjev, naprav, omrežij (npr. Pachube[9], Sensor.Network[10] itd.);
- Razvoj koncepta uporabe senzorjev kot storitve (*angl. Sensor-as-a-Service*), ki bo na podlagi souporabe senzorjev omogočal sestavljanje virtualnih priložnostnih senzorskih omrežij na zahtevo posamezne aplikacije;
- Napredni skupki aplikacij (*angl. mash-up*), ki ne bodo temeljili le na podatkih iz različnih povezanih stvari ampak bodo z uporabo napredne obdelave podatkov zajetih na različnih napravah, na različnih lokacijah in ob različnih časovnih trenutkih, ter njihovi obogatitvi z informacijami iz alternativnih virov, postali vir dodatnega znanja in vedenja z možnostjo napovedovanja.

VI. ZAKLJUČEK

Namen tega prispevka je predstaviti koncept Interneta stvari kot enega stebrov Interneta prihodnosti. S tega stališča je podan pregled reprezentativnih področij, na katerih pričakujemo prve primere vpeljave koncepta, predstavljene so ključne tehnologije, ki ga tvorijo, identificirani pa so tudi glavni izzivi in trendi razvoja.

Podobno kot na vrsti drugih področij Evropska skupnost podpira raziskave in razvoj na področju Interneta stvari predvsem preko 7. okvirnega programa. V okviru tega programa so trenutno sofinancirani projekti kot so ASPIRE[11], CASAGRAS2[12], ebbits[13], ELLIOT[14], GRIFS[15], IoT@Work[16], IoT-A[17], IoT-i[18], iSURF[19] in drugi. Ti projekti so tudi povezani v

[7] http://www.arduino.cc/
[8] http://videolectures.net/wsn2010_mihelin_vsn/
[9] http://www.pachube.com/
[10] http://sensor.network.com/
[11] http://www.fp7-aspire.eu/
[12] http://www.iot-casagras.org/
[13] http://www.ebbits-project.eu/news.php
[14] http://demos.txt.it/elliot-project/
[15] http://www.grifs-project.eu/
[16] https://www.iot-at-work.eu/
[17] http://www.iot-a.eu/
[18] http://www.iot-i.eu/
[19] http://www.srdc.com.tr/isurf/

raziskovalni grozd IERC[20] (*European Research Cluster on the Internet of Things*), katerega namen je koordinacija zmogljivosti in aktivnosti na področju Interneta stvari in iskanje širokega konsenza o viziji njegovega uvajanja v Evropi.

Internet stvari je izredno zanimivo področje tudi za Slovenijo, tako za raziskovalne organizacije, saj sloni na znanjih in tehnologijah, ki jih posamezne skupine že obvladujejo, kot za gospodarstvo, saj te tehnologije za pilotsko testiranje in zagon proizvodnje zahtevajo razmeroma nizke finančne vložke. Raziskovalne in razvojne skupine se v aktivnosti na področju Interneta stvari vključujejo tako na evropski ravni (npr. preko posameznih projektov ali pa preko evropskih tehnoloških platform in povezav) kot preko slovenskih povezav in združenj (npr. FI.SI) in domačih projektov (npr. kompetenčni center KC OPCOMM).

Kot je prikazano v prispevku gre pri Internetu stvari za aplikativno naravnano področje, in rešitve vsakega posameznega problema lahko ob ustreznem načrtovanju in integraciji predstavljajo del celotne rešitve. V luči tega se kot najprimernejši način nadaljnjega razvoja in vpeljevanja koncepta kaže postavljanje pilotskih sistemov in njihova integracija z drugimi domačimi in evropskimi pilotskimi sistemi za navzkrižno testiranje rešitev v heterogenih okoljih. Tak pristop po eni strani zagotavlja razvoj odprtega koncepta Interneta stvari s podporo enostavni integraciji različnih tehnologij in rešitev na različnih nivojih, po drugi strani pa tudi participacijo slovenskih raziskovalnih in razvojnih skupin v evropskih projektih, kjer so pilotske postavitve vedno iskane.

ZAHVALA

Avtor se zahvaljuje sodelavcem SensorLaba za mnoge tvorne pogovore o konceptih, tehnologijah in izzivih Interneta stvari, ki so sooblikovali razumevanje področja in se v določeni meri odražajo v pričujočem prispevku.

LITERATURA

[1] SRI Consulting Business Intelligence, Disruptive Technologies APPENDIX F: The Internet of Things, Global Trends, 2025.
[2] R. MacManus, Top 10 Internet of Things Developments of 2010, *ReadWriteWeb*, December 15, 2010, http://www.readwriteweb.com/archives/top_10_internet_of_things_developments_of_2010p2.php
[3] D. Papadimitriou (Ed.), Future Internet, The Cross-ETP Vision Document, Version 1.0, January 8, 2009.
[4] O.Vermesan, M. Harrison, H. Vogt, K. Kalaboukas, M. Tomasella, K. Wouters, S. Gusmeroli, S. Haller, Internet of Things: Strategic Research Roadmap, September 15, 2009.
[5] M. Zorzi, A. Gluhak, S. Lange, A. Bassi, From Today's INTRAnet of Things to a Future INTERnet of Things: A Wireless- and Mobility-Related View, *IEEE Wireless Communications*, December 2010, Vol. 17, No. 6, pp. 44-51.
[6] A. Iera, C. Floerkemeier, J. Mitsugi, G. Morabito, The Internet of Things [Guest Editorial], *IEEE Wireless Communications*, December 2010, Vol. 17, No. 6, pp. 8-9.
[7] L. Atzori, A. Iera, G. Morabito, The Internet of Things: A survey, *Comput. Netw.* 54, 15 (October 2010), pp. 2787-2805.

Mihael Mohorčič je višji znanstveni sodelavec in vodja Odseka za komunikacijske sisteme na Institutu Jožef Stefan. Doktoriral je leta 2002 na Fakulteti za elektrotehniko Univerze v Ljubljani. Leta 2006 je bil na Mednarodni podiplomski šoli Jožefa Stefana izvoljen v naziv docent. Tam je tudi dopolnilno zaposlen in izvaja več predmetov na 2. in 3. stopnji bolonjskega študija. Njegovo raziskovalno delo sodi na področja satelitskih, stratosferskih, brezžičnih, kognitivnih in senzorskih omrežij.

[20] http://www.internet-of-things-research.eu/

Odprta komunikacijska platforma IoT

Andrej Kos[1], Urban Sedlar[1], Klemen Peternel[1], Mojca Volk[1],
Janez Sterle[1], Luka Zebec[1], Tomaž Vidonja[2], Janez Bešter[1]

[1]Univerza v Ljubljani, Fakulteta za elektrotehniko, Laboratorij za telekomunikacije
[2]Kompetenčni center OpComm, Tehnološka mreža ICT

Povzetek — Članek predstavlja zasnovo platforme IoT, ki nosi ime OpComm. Opisuje njeno podatkovno naravnanost skupaj z glavnimi funkcionalnostmi. Pomembna dela platforme sta modul za analitiko in vizualizacijo podatkov ter sloj, ki omogoča povezovanje v zunanji svet preko odprtih vmesnikov. Opisani so tudi nekateri realni scenariji uporabe platforme.

Ključne besede — platforma IoT, OpComm, podatkovno rudarjenje, analitika, vizualizacija, odprti vmesniki

Abstract — This article explains design of the IoT platform, named OpComm. It describes main functionalities with emphasis on data analysis, data visualization and open interfaces. In the last part some usage scenarios are presented.

Keywords — IoT platform, OpComm, data mining, data analysis, data visualization, open interfaces

I. UVOD

Platforma OpComm predstavlja odprto in skalabilno platformo za zajem, shranjevanje, obdelavo in analizo podatkov.

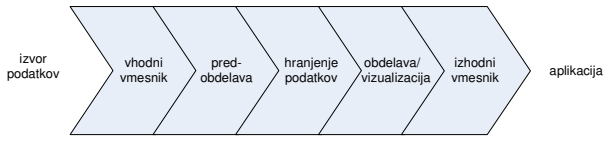
V prispevku je predstavljena funkcionalna zasnova platforme. Dodani so opisi posameznih modulov in navedeni nekateri izbrani scenariji uporabe.

II. PLATFORMA OPCOMM

Poglavitni namen platforme OpComm je agregiranje podatkov iz različnih virov, zagotavljanje varnosti in kontrole dostopa do podatkov in potrebnih virov platforme, ki so potrebni za njihovo obdelavo, ter obogatitev podatkov na osnovi analitskih tehnik in postopkov strojnega učenja.

OpComm predpostavlja uporabo odprtih vmesnikov tako na dohodni kot na izhodni strani, s čimer sta mogoča nadzorovano posredovanje podatkov v platformo ter nadzorovan dostop do surovih in obdelanih podatkov.

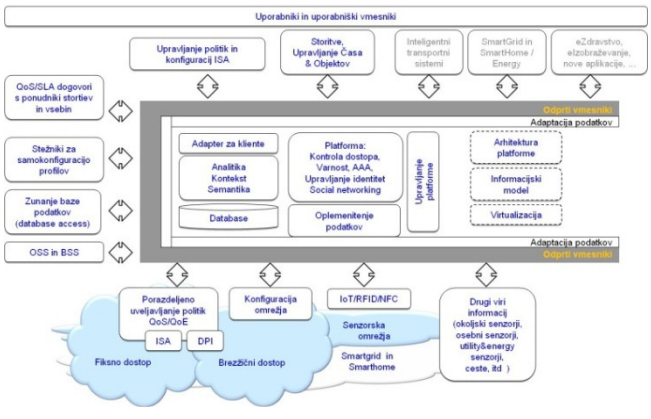
Podatkovna naravnanost platforme omogoča njeno uporabo tako v širokem spektru individualnih scenarijev, kot tudi v naprednih scenarijih, ki temeljijo na zlivanju podatkov različnih domen.



Slika 1: Tok podatkov posameznega scenarija

Ključne funkcije platforme predstavljajo jedro njenega delovanja in omogočajo.

– Sistematiziran zajem podatkov ne glede na vir, frekvenco in obliko; predvideni scenariji, ki so podrobneje predstavljeni v nadaljevanju, služijo za izdelavo podatkovnih modelov; slednje je mogoče širiti z dodajanjem novih scenarijev.
– Predobdelava podatkov, v katero sodijo razpoznava entitet na osnovi vnaprej definirane domenske ontologije, eliminacija duplikatov in anonimizacija podatkov.
– Obdelava in analiza podatkov, ki vključuje bogatenje podatkov, razpoznava konteksta in vzorcev, identifikacija anomalij in razpoznava trendov. Postopki analize temeljijo na različnih tehnikah strojnega učenja in bodo pripravljene v skladu z načrtovanimi scenariji.
– Vizualizacija podatkov, ki vključuje vizualizacijo KPI posameznih predvidenih scenarijev ter delovanja same platforme (nadzorne plošče).
– Realno-časovno obveščanje na osnovi procesiranja dogodkov v sklopu dogodkovno-krmiljene arhitekture, kjer so izvori dogodkov bodisi zunanji (preko ustreznih vmesnikov) ali notranji (gradniki same platforme).



Slika 2: Izhodiščna shema arhitekture platforme

A. *Analitika in vizualizacija*

Del zmogljivosti platforme OpComm bo namenjen analizi in vizualizaciji podatkov z namenom opazovanja, analiziranja, interpretacije, predstavitve in potencialno tudi izvoza obdelanih podatkov v tista okolja in rešitve, ki bodo za svoje delovanje uporabljale storitve platforme OpComm.

Postopki obdelave in analize bodo izvedeni nad podatki po opravljeni predobdelavi. Del modulov analitike bo integriranih v sklopu platforme OpComm (t.i. »*leightwight*« analitika), kompleksnejši postopki analize in obogatitve pa bodo izvedeni s pomočjo zunanjih namenskih modulov in sistemov (npr. napredni sistem za podatkovno rudarjenje).

Poleg tega bodo podprte tudi funkcionalnosti za osnovno in napredno vizualizacijo podatkov, ki bo služila za predstavitev surovih in obdelanih podatkov ter osnovo za izvedbo postopkov vizuelne analitike.

V modulih za analitiko in vizualizacijo v okviru platforme OpComm bodo vključene različne uveljavljene in inovativne tehnike podatkovne analize, kot npr. ontologije, postopki strojnega učenja, podatkovno rudarjenje, statistična obdelava podatkov, semantična razpoznava konteksta in vzorcev, vizuelna analitična orodja ipd. Poleg tega bodo podprte zmogljivosti za po-uporabo in vključevanje izbora uveljavljenih samostojnih odprtokodnih orodij, kot npr. okolje Matlab [1] za naprednejšo analizo podatkov, ter orodji igraph [2] in Graphviz [3], javanski API in knjižnice JUNG [4] in okolje Pajek [5] za različne oblike vizualizacije in reprezentacije podatkov.

Skladno z univerzalno zasnovo platforme OpComm bo tudi temeljno delovanje analitičnih modulov zasnovano splošno, pri čemer pa bodo postopki obdelave in prikaza podatkov domensko-specifični in prilagojeni konkretnim uporabniškim scenarijem. Za vsak identificiran scenarij bodo natančno opredeljene zahteve ter specificirani postopki podatkovne analize in vizualizacije z izbranim naborom orodij in tehnik za definiran nabor KPI (sestavljeni iz surovih in obdelanih podatkov). Poleg tega bodo za izbrane scenarije po potrebi opredeljeni tudi postopki priprave in izvoza obdelanih podatkov v druga okolja in rešitve, kar bo omogočilo nadgradnjo inteligence zagotovljenih storitev (npr. definicija in izvoz podatkov o omrežnih performancah v sisteme za krmiljenje dostopa in delo s politikami, priprava informacij o komunikacijskem kontekstu za krmiljenje naprednih storitev prisotnosti, ipd.).

Poleg zagotavljanja opisanih postopkov in storitev bodo moduli za analizo in vizualizacijo v okviru platforme OpComm vključeni tudi v funkcije za nadzor internega delovanja platforme (nadzorna plošča).

B. *Odprti vmesniki*

Odprti vmesniki predstavljajo stik platforme z zunanjimi omrežji. Preko njih različni viri platformi, kot centralnemu agregatorju, posredujejo svoje podatke. Takšnih virov je lahko mnogo, zato je pomembno, da so vmesniki performančno zmogljivi in dopuščajo visoko pretočnost z minimalno stopnjo režije. Zaradi različnih scenarijev uporabe mora biti zagotovljena ustrezna razširljivost ter interoperabilnost v smislu podpore množici programskih jezikov.

Platforma sprejema podatke s strani več tipov odjemalcev, pri čemer imajo nekateri večjo, drugi pa manjšo razpoložljivo procesorsko moč. Posledično implementira dve vrsti vmesnikov, ki dopuščata različne nivoje abstrakcije. To so visokonivojski vmesniki spletnih storitev (angl. Web Services), ki se danes uporabljajo v večini obstoječih platform in pa t.i. lightweight senzorski vmesniki [6, 7].

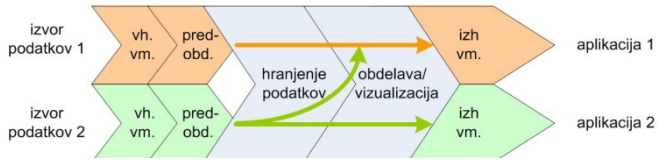
Prvi običajno za prenos podatkov uporabljajo protokol za prenos hiperteksta HTTP (angl. Hyper Text Transfer Protocol), ki deluje po principu zahteva-odziv. Protokol je preprost in je v praksi pogosta izbira za prenos informacij v različnih namenskih sistemih. Hkrati prestavlja enega od temeljnih gradnikov svetovnega spleta. Najbolj pogosta vmesnika spletnih storitev, ki za svoje delovanje uporabljata omenjeni protokol, sta SOAP (Simple Object Access Protocol) [8] in REST (Representational State Transfer) [9].

Senzorski vmesniki so v primerjavi s prej omenjenimi predvsem protokolno »lažji«, saj se prenos podatkov velikokrat dogaja že na transportnem nivoju ISO/OSI modela. Režije je manj, slednjo pa največkrat predstavlja preprosta ovojnica. Senzorji običajno ne razpolagajo z veliko procesorsko močjo, zato je uporaba visokonivojskih protokolnih skladov posledično nemogoča. To je tudi glavni razlog, da platforma ločuje med obema tipoma odprtih vmesnikov.

III. PODROČJA IN SCENARIJI UPORABE

Namen platforme je podpora vrsti uporabniških scenarijev, ki se v prvi vrsti poslužujejo posameznih funkcionalnosti platforme na neodvisen način (uporaba generičnih funkcionalnosti za podporo podatkovno intenzivnim scenarijem), kot prikazuje Slika 1, hkrati pa predstavljajo možnost za soodvisno uporabo in zlivanje podatkov med posameznimi vertikalami (Slika 3). To predstavlja možnost za veliko dodano vrednost in obogatitev podatkov s preseganjem meja tradicionalno zaprtih informacijskih sistemov.

Platforma je uporabna za številne dogodkovno odvisne scenarije: e-cestninjenje, Internet of Things (IoT), Smart Grids, Smart Traffic, Smart City, Real-time Fraud Detection, Denial of Service (DoS) ipd.



Slika 3: Zlivanje podatkov dveh vertikal

V nadaljevanju predstavljamo štiri scenarije uporabe, ki služijo kot vodilo pri snovanju platforme in slednjo izkoriščajo tako na neodvisen način (izdelava podatkovno-krmiljenih aplikacij), kot na soodvisen način z uporabo zlivanja podatkov.

A. *Pametni dostop*

V sodobnih komunikacijskih sistemih je komunikacijska veriga tipično sestavljena iz več med seboj tehnološko, konceptualno in performančno raznolikih segmentov v omrežju (kombinacije omrežnih protokolov IPv4/IPv6 in MPLS v jedru, raznolike fiksne in mobilne dostopovne tehnologije, ipd.). Pri tem je uporabnikom na voljo pester nabor multimedijsko bogatih in med seboj zlitih storitev (govorne storitve, pretočni video, podatkovne storitve, ipd.), do katerih lahko dostopajo preko izbranih dostopovnih omrežij in pri tem uporabljajo poljubno terminalno opremo. Takšna kompleksnost komunikacijske verige posledično zahteva dinamično upravljanje delovanja dostopovnih omrežij, ki skrbi za ustrezne kapacitete in kakovost, poleg tega pa tudi napredno in inteligentno zagotavljanje storitev in delo z uporabnikovimi profili in pravicami.

Za vzpostavitev opisanih zmogljivosti krmiljenja dostopa in zagotavljanja storitev je v omrežju potrebno zagotoviti ustrezne inteligentne funkcije, ki bodo na voljo v okviru platforme OpComm.

Platforma bo preko dohodnih vmesnikov zbirala in agregirala podatke o uporabniku, storitvah, omrežju in omrežnih gradnikih (podatke lahko prejema od merilnih agentov, integriranih nadzornih funkcij v omrežnih elementih, iz lokalnih podatkovnih baz, ipd.), poleg tega pa bodo v podatkovni bazi na voljo tudi drugi podatki, ki tvorijo komunikacijski kontekst in lahko predstavljajo dodano vrednost za potrebe izvajanja inteligentnega krmiljenja dostopa (npr. podatki o učinkih izbrane terminalne opreme na kakovost storitve z vidika končnega uporabnika ali podatki o uporabnikovih nastavitvah dosegljivosti v storitvi prisotnosti). Nad zbranimi podatki bo platforma s pomočjo modulov za analizo in vizualizacijo izvedla demonsko-specifično analizo in interpretacijo. Rezultat teh postopkov bodo določene vrednosti izhodnih KPI, definiranih za dani scenarij, ki jih bo platforma preko izhodnih vmesnikov izvozila v ustrezne elemente komunikacijskega omrežja (npr. strežnik politik ali AAA nadzornik). Primeri možnih scenarijev, v katerih opisano zlivanje in interpretacija razširjenega nabora podatkov o komunikaciji prinaša pomembno dodano vrednost, so:

- napredno prilagajanje prioritet storitev glede na informacije o prisotnosti uporabnika,
- dinamično krmiljenje porabe pasovne širine v ozkopasovnem dostopovnem omrežju na osnovi podatkov o razpoložljivih kapacitetah, potratnosti storitve in njene prioritete ter QoE informacijah za danega uporabnika,
- nadzor delovanja omrežja in napredna diagnostika na osnovi tehnik prometne analize in semantične razpoznave vzorcev.

B. *Upravljanje z osnovnimi sredstvi*

Platforma bo pridobivala in shranjevala podatke s strani posameznih stvari oz. osnovnih sredstev skozi njihovo celotno življenjsko dobo. Omenjena osnovna sredstva delimo na tista z lastno inteligenco (»*smart*«) ali pa na pasivne stvari (»*non-smart*«). Prve imajo zmožnost, da same komunicirajo s platformo in pošiljajo podatke o stanju, lokaciji in ambientu v katerem se nahajajo. Druge so popolnoma brez lastne inteligence in za komunikacijo s platformo potrebujejo ustrezno podporno tehnologijo. Običajno so takšni objekti opremljeni z uporabo ustreznih identifikacijskih tehnologij, kot so črtna koda, radijska frekvenčna identifikacija (RFID) ipd. Za pošiljanje podatkov na platformo je posledično potrebno uporabiti ustrezno napravo, ki podpira izbrano identifikacijsko tehnologijo in podatek o predmetu posreduje platformi.

Obstoječa sredstva je v nekaterih smiselnih scenarijih možno opremiti tudi z zmogljivimi senzorji, ki v realnem času posredujejo informacijo o tem v kakšnem stanju sredstvo je (temperatura in vlažnost okolice, osvetljenost, tresljaji, lokacija itd.). Na ta način gradimo obsežna senzorsko omrežje, ki je vir številnih koristnih informacij.

Platforma bo podatke o osnovnih sredstvih hranila, hkrati pa omogoča izvedbo poglobljene analize. Na ta način bo možno hitro ugotoviti v kakšnem stanju je posamezen objekt, oziroma ali ambientalni parametri ustrezajo zahtevanim. Na podlagi analize bo upravitelj osnovnih sredstev lahko sprožil ustrezne akcije (npr. izpolnil delovne naloge) ali pa raziskal morebitne odvisnosti med posameznimi parametri.

C. *Analiza karakteristik IPv6 storitev v internetu*

Protokol IPv6 predstavlja logično nadgradnjo in razširitev protokola IPv4 in prinaša večji naslovni prostor, širšo podporo varnostnim mehanizmom ter odpira možnosti za globalno oddajanje več prejemnikom (angl. multicast). Že nekaj let poteka intenzivna migracija internetnih omrežij in storitev na IPv6, vendar so karakteristike že nadgrajenih sistemov na globalni skali relativno slabo nadzorovane, prav tako pa niso poznane praktične (angl. real-world)

implikacije in vplivi uvedbe IPv6 na karakteristike posameznih storitev.

V okviru opisanega scenarija bo platforma OpComm služila za sprejem in hranjenje podatkov porazdeljenih programskih modulov za izvajanje nabora večprotokolnih testov, s čimer bo mogoča primerjava karakteristik IPv4 in IPv6.

Kot tipične testne vzorce lahko uporabimo t.i. *dualstack* storitve, ki so dostopne po obeh protokolih, kar omogoča primerjavo karakteristik iz različnih točk omrežja.

Programski moduli zbrane podatke preko dohodnih vmesnikov posredujejo platformi OpComm, ki skrbi za njihovo varno shranjevanje, obdelavo in analizo, ter ustreznim aplikacijam zagotavlja dostop do surovih in obdelanih podatkov. Aplikacija lahko podatke uporabi za izdelavo naprednih poročil s pregledom karakteristik IPv6 storitev v skoraj-realnem času, dodatno pa omogoča identifikacijo storitev in segmentov omrežja, ki izkazujejo anomalije in jih je potrebno posledično spremljati z natančnejšo granulacijo.

D. *Presence*

Platforma OpComm bo sposobna pridobivati in shranjevati podatke o prisotnosti s strani različnih virov. Na podatkih bo izvajala analizo, obenem pa bodo ti podatki prek odprtih vmesnikov platforme na voljo zunanjim storitvam, ki bodo lahko delovale v odvisnosti od stanja prisotnosti.

V splošnem nam viri dajejo dve vrsti informacij.

- Komunikacijske informacije (posredovane s strani komunikacijskih naprav, storitev, aplikacij) podajajo trenutno komunikacijsko stanje (nekdo npr. »chat-a«, telefonira ...), priporočen tip komunikacije (izbran s strani uporabnika), profil zvonjenja na mobilnem terminalu itd.
- Razširjene informacije (posredovane s strani ostalih - tudi ne-komunikacijskih - naprav, storitev in aplikacij) omogočajo vpogled v širši uporabniški kontekst. To so predvsem informacije o lokaciji, trenutni aktivnosti (sestanek, malica, dopust ...), hitrosti, ambientu (okoliški hrup), zadnjih aktivnostih znotraj spletnih aplikacij (npr. čas zadnjega poslanega FB sporočila), samo-poročanje itd.

Interpretacija podatkov s strani storitev je lahko odvisna tudi od konteksta uporabnika (npr. podatek, da lahko uporabnik trenutno sprejema klice na mobilniku, ima različen pomen, glede na to, ali je za računalnikom v službi, se nahaja doma, ali pa se vozi po avtocesti s hitrostjo 130 km/h). Platforma OpComm bo storitvam, prek uporabe analitike, omogočala tudi informacije o kontekstu uporabnika.

Storitve, ki bodo strnjeno informacijo o prisotnosti, s strani platforme, uporabljale (krmiljenje komunikacij, beleženje časa in aktivnosti), bodo imele tudi možnost posredovanja določenih povratnih informacij, s čimer lahko prepreči večkratno ponavljanje slabih odločitev logike platforme.

IV. ZAKLJUČEK

Prispevek opisuje odprto inteligentno IoT platformo OpComm. Slednja omogoča fleksibilno večnivojsko shranjevanje podatkov v odvisnosti od zahtev posameznega scenarija (glede na količino in tip podatkov). Platforma se z zunanjim svetom povezuje preko odprtih vmesnikov, ki jih delimo na visokonivojske (abstraktne) in t.i. lightweight senzorske vmesnike.

Ena izmed ključnih funkcionalnosti platforme je tudi horizontalno povezovanje posameznih vertikal, kar omogoča obogatitev podatkov na osnovi podatkov iz drugih domen. Posledično se pojavljajo novi scenariji uporabe in zlivanja obstoječih podatkov.

Platforma v svoji arhitekturni zasnovi omogoča enostavno in jasno vključitev novih domenskih scenarijev. Na podlagi slednjih lahko prek odprtih vmesnikov razvijalci predstavljajo in razvijajo nove inovativne storitve.

LITERATURA

[1] Matlab, dostopno na http://www.mathworks.com/products/matlab/
[2] igraph, dostopno na http://igraph.sourceforge.net/
[3] Graphviz, dostopno na http://graphviz.org/
[4] Java Universal Network/Graph (JUNG) Framework, dostopno na http://jung.sourceforge.net/
[5] Pajek, dostopno na http://pajek.imfm.si/doku.php?id=pajek
[6] MQTT For Sensor Networks (MQTT-S), Protocol Specification Version 1.1
[7] MQ Telemetry Transport, dostopno na http://mqtt.org/
[8] SOAP, dostopno na http://en.wikipedia.org/wiki/SOAP
[9] REST, dostopno na http://en.wikipedia.org/wiki/REST

Andrej Kos (andrej.kos@fe.uni-lj.si) je diplomiral leta 1996 na Fakulteti za elektrotehniko, Univerze v Ljubljani in doktoriral leta 2003. Trenutno je zaposlen kot docent na Fakulteti za elektrotehniko. Trenutno se ukvarja z raziskavami na področju širokopasovnih paketnih omrežij in inteligentnih storitvev naslednje generacije.

Urban Sedlar (urban.sedlar@fe.uni-lj.si) je diplomiral leta 2004 na Fakulteti za elektrotehniko, Univerze v Ljubljani in doktoriral leta 2010. Zaposlen je v laboratoriju za telekomunikacije (LTFE) na Fakulteti za elektrotehniko, kjer se ukvarja se z raziskavami na področju internetnih sistemov in storitev.

Klemen Peternel (klemen.peternel@fe.uni-lj.si) je diplomiral leta 2007 na Fakulteti za elektrotehniko Univerze v Ljubljani s področja telekomunikacij. V Laboratoriju za telekomunikacije opravlja razvojno-raziskovalno delo na področju načrtovanja in razvoja telekomunikacijskih sistemov in storitev naslednje generacije. Sodeluje tudi pri pripravi in izvedbi

izobraževanj s področja telekomunikacij in programskega jezika Java.

Mojca Volk (mojca.volk@fe.uni-lj.si) je diplomirala leta 2004 in doktorirala leta 2010 na Fakulteti za elektrotehniko, Univerza v Ljubljani. Trenutno je zaposlena v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko, kjer se ukvarja z raziskavami na področju širokopasovnih omrežij naslednje generacije in tehnologijami za analizo, modeliranje in vizualizacijo ter zagotavljanje kontekstualnih storitev in kakovosti komunikacije v sodobnih multimedijskih storitvenih okoljih.

Janez Sterle (janez.sterle@fe.uni-lj.si) je diplomiral leta 2003 na Fakulteti za elektrotehniko Univerze v Ljubljani s področja telekomunikacij. Od leta 2002 dela v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko. Njegovo raziskovalno in pedagoško delo je usmerjeno v preučevanje in razvoj omrežnih sistemov in storitev naslednje generacije. Področja katerim se trenutno najbolj posveča so večprotokolna komutacija na osnovi label, internetni protokol naslednje generacije, varnost v internetnih omrežjih ter razvoj in uvajanje novih integriranih storitev v fiksna in brezžična dostopovna omrežja.

Luka Zebec (luka.zebec@fe.uni-lj.si) je diplomiral leta 2000 in magistriral leta 2003 na Fakulteti za elektrotehniko Univerze v Ljubljani, oboje s področja telekomunikacij. Od leta 1999 dela kot raziskovalec v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko. Njegovo pedagoško, raziskovalno in razvojno delo je povezano z raziskovanjem, načrtovanjem in razvojem konvergenčnih internetnih aplikacij ter telekomunikacijskih sistemov in storitev naslednje generacije. Sodeluje pri pripravi in izvedbi izobraževalnih seminarjev in delavnic ter na izobraževalnih prireditvah kot avtor strokovnih prispevkov.

Tomaž Vidonja (tomaz.vidonja@ict-slovenia.net) ima 15 let izkušenj dela v gospodarstvu na področju informacijskih in komunikacijskih tehnologij. Trentno zaposlen kot vodja Kompetenčnega centra OpComm v okviru zavoda Tehnološka mreža ICT.

Janez Bešter (janez.bester@fe.uni-lj.si) je doktoriral leta 1995 in je zaposlen na Fakulteti za elektrotehniko v Ljubljani kot profesor in predstojnik Laboratorija za telekomunikacije. Njegovo raziskovalno, razvojno in pedagoško delo je povezano s področjem načrtovanja, realizacije in vodenja telekomunikacijskih sistemov in storitev ter uporabo informacijskih tehnologij in telekomunikacij na področju e-izobraževanja. Je član IEEE, ACM, IEICE ter mnogih drugih strokovnih organizacij s področja elektronskih komunikacij.

Internet stvari: spodbujanje ali regulacija?

Urban Kunc, mag. org. inf., Agencija za pošto in elektronske komunikacije RS

Povzetek — Internet stvari je tehnologija, ki vključuje množico med seboj in v internet povezanih nevsiljivih in nevidnih naprav in stvari. Skupaj s pripadajočimi aplikacijami lahko generira ogromno in raznoliko količino (občutljivih) podatkov. Četudi internet stvari med drugim prinaša mnogo koristi na področju transporta in logistike, okolja, energijske učinkovitosti in zdravstva, lahko neupoštevanje temeljnih človeških vrednot, kot so varstvo zasebnosti in osebnih podatkov, korenito zavre njegov razvoj in uvedbo.

V prispevku so predstavljeni potrebni ukrepi na podlagi katerih bo lahko internet stvari kot tudi državljani kos izzivom, povezanim z zaupanjem in varnostjo občutljivih podatkov ter uporabo nove tehnologije.

Ključne besede — Internet stvari, zakonodaja, regulacija

Abstract — The Internet of Things is a technology that comprises a number of connected non-intrusive and invisible devices and things. Together with its applications, it can generate an enormous and diverse amount of (sensitive) data. Although the Internet of Things offers benefits in the fields of transport and logistics, environment, energy efficiency and health care, its impact on the insufficient respect of fundamental human values, such as privacy and protection of personal data, might substantially inhibit its development and deployment.

The paper presents the necessary measures, to be pursued, that will allow the Internet of Things and the citizens to cope with dilemmas related to confidentiality and security of sensitive data as well as the usage of a new technology.

Keywords — Internet of Things, legislation, regulation

I. UVOD

Internetna arhitektura se sooča z vedno večjimi kompleksnimi izzivi. Narašča število stalno povezanih uporabnikov, naprav, storitev in aplikacij, obenem pa pomembno vpliva na družbene, sociološke in ekonomske spremembe v družbi. Internet se kot vsak drug živ sistem razvija skozi različne razvojne stopnje. Na prvi stopnji razvoja so se med seboj povezovali računalniki, izmenjevali so se podatki (internet in souporaba podatkov). Na drugi stopnji smo ljudje povezovali in souporabljali dokumente in vsebine (internet in souporaba vsebin). Trenutno smo v tretji razvojni stopnji interneta, kjer se preko njegovega omrežja povezujemo z drugimi ljudmi ter pletemo družbeno-komunikacijske vezi. Govorimo o internetu ljudi in o družbenih omrežjih (*angl.* Social Networks). Naslednja faza razvoja interneta ni le povezovanje ljudi, temveč povezovanje ljudi s stvarmi ter povezovanje in komuniciranje stvari z drugimi stvarmi in napravami. Danes je na svetu že blizu 7 milijard ljudi. To je potencial 'Interneta ljudi'. Po nekaterih ocenah imamo na svetu 50–70 milijard strojev[1], zato lahko govorimo o potencialu interneta strojev. Na svetu je tudi približno 50.000 milijard 'stvari', kar je potencial interneta stvari (*angl.* Internet of Things, IoT). To so vsakodnevni objekti – stvari, ki bodo berljive, prepoznane, locirane, naslovljene in celo nadzorovane preko interneta. V kontekstu interneta stvari to ne vključuje le nekaj elektronskih naprav, ki jih uporabljamo vsak dan, kot tudi ne le visokotehnoloških izdelkov kot so vozila ali druge naprave. Internet stvari predstavlja dejanske stvari, ki danes še niso povezane z elektroniko – stvari, kot so hrana, materiali, deli in podsestavi, blago in luksuzni predmeti, stavbe, prometna infrastruktura in mnogi drugi objekti, ki pripadajo množici približno 50.000 milijardam stvari, ki danes obstajajo na svetu. Internet stvari bo konvergenca nanotehnologije, biotehnologije, informacijsko-komunikacijske tehnologije in kognitivnih znanosti. Je globalno omrežje omrežij in podomrežij, ki bo temeljilo na standardiziranih in odprtih komunikacijskih protokolih, kjer so individualni inteligentni objekti med seboj povezani in ki lahko med seboj sodelujejo, si izmenjujejo podatke in celo sprejemajo odločitve in samostojno ustrezno ukrepajo. Količina podatkov, ki jih bodo generirale RFID oznake, senzorji in druge podobne IoT tehnologije, bo neprimerljivo večja od količine, ki jo generiramo danes ljudje. Večina teh podatkov se ne bo shranjevala in obdelovala samo v lokalnih strežniških sistemih, temveč se bo shranjevala v internetu, v oblakih (*angl.* Cloud Computing).

Postavlja se vprašanje, ali smo pripravljeni na vse te spremembe? Ne le tehnološko, temveč tudi sociološko, družbeno in ekonomsko. Ali se zavedamo vseh posledic, ki jih bo imel internet stvari na zasebnost, zaupnost in varstvo posameznikov oziroma njihovih podatkov? Podjetja praviloma gledajo predvsem na dobiček, manj pa na vpliv, ki ga ima dejavnost npr. na okolje ali pravice in zasebnost posameznikov. Tehnologija bo za uporabnika velikokrat nevidna in vseprisotna. Ali si lahko predstavljamo posledice, ki nastanejo, če smo odvisni od sistema interneta stvari in če takšen sistem odpove, ali pa ga prevzame

[1] Ta podatek navajajo različni avtorji, ker menijo, da je vsak človek povprečno obkrožen z okoli 10 stroji.

organizacija, nad katero nimamo vpliva? IoT zaradi samo nekaterih izpostavljenih vprašanj ne smemo prepustiti trgu. Na globalnem nivoju ga je potrebno vzpostaviti in razvijati v sodelovanju z akademsko sfero, civilno družbo, zasebnim sektorjem in državnimi inštitucijami. Vzpostaviti je potrebno trdne temelje in ravnotežje na različnih nivojih, ki vplivajo na bodoči razvoj IoT: arhitekture interneta stvari, varnosti, zasebnosti in varstva podatkov, upravljanje identitete, naslavljanje in medsebojne združljivosti (izdelkov in storitev), upravljanje radiofrekvenčnega spektra, etike (pravica do izklopa čipa), zdravja, (vpliv na povzročeno elektromagnetno sevanje), ekologije (recikliranje in ponovna raba) in standardizacija (ključno za masovno proizvodnjo in uporabo).

II. NEKATERA DEJSTVA O NASTANKU INTERNETA STVARI

Koncept 'Internet stvari' smo zasledili že leta 1984 (profesor Ken Sakamura – 'računalniki vsepovsod') in nato še leta 1988 (Mark Weiser – Xerox PARC 'vsepovsod prisotno računalništvo'). Besedna zveza Internet stvari (v nadaljevanju IoT) se je pojavila prvič leta 1998. Skoval jo je Kevin Ashton, britanski tehnološki pionir na področju radiofrekvenčne identifikacije (*angl*. RFID – Radio Frequency Identification) in brezžičnih senzorskih omrežij. IoT je Ashton, ki je soustanovitelj in izvršni direktor Auto-ID centra pri Massachusetts Institute of Technology, opisal kot računalnike, ki avtomatsko zaznavajo in identificirajo vsakodnevne objekte, ki jih obdajajo. Še istega leta (1998) je Nadzorni organ Evropske komisije za informacijsko-komunikacijsko tehnologijo (ISTAG – European Union's Information Society Technologies Program Advisory Group) neodvisno od Ashtona v svojem poročilu uporabil podoben termin s podobnimi značilnostmi 'Ambientna inteligenca' (*angl*. Ambient Intelligence). Pojem naj predstavljal konvergenco vsepovsod prisotnega računalništva, komunikacije in inteligentnega, do uporabnika prijaznega uporabniškega vmesnika. Gre torej za podobno vizijo, kjer so ljudje obkroženi z inteligentnimi in intuitivnimi vmesniki, ki so vgrajeni v vsakodnevne objekte. Leta 2003 je bila na simpoziju EPC (*angl*. Electronic Product Code) predstavljena prva platforma EPC omrežja. Že omenjeni Ashton je na tej konferenci napovedal, da bodo lahko omrežja EPC omogočala strojem, da bodo zaznavali druge objekte kjerkoli na svetu in s tem učinkovito ustvarili IoT. Dve leti kasneje, novembru 2005, se je odzval tudi ITU (*angl.* International Telecommunication Union) ter izdal znamenito poročilo o internetu stvari (ITU, 2005). Tudi ITU je IoT opisal kot vizijo stalne povezljivosti, kjer nove tehnologije, kot je RFID, vgrajeni sistemi, inteligentno računalništvo in nanotehnologija obljubljajo svetu omrežene in med seboj povezane naprave, ki omogočajo relevantno vsebino in informacije, kjer koli se uporabnik nahaja. ITU je v poročilu izpostavil, da IoT prinaša številne izzive, pri čemer bo igrala ključno vlogo zagotavljanje ustreznega varstva zasebnosti in podatkov. ITU ugotavlja, da bo nevidna in stalna izmenjava podatkov med ljudmi in stvarmi ter med samimi stvarmi pripeljala do tega, da ne bomo več razpoznali, kdo je lastnik in kaj je izvor podatkov. Izpostavlja se pomembno vprašanje, kdo bo preko vseh teh »oči in ušes« različnih tehnologij, ki bodo okoli nas, ultimativno nadzoroval v okolju zbrane podatke?

Da tehnologija RFID in druge naprave kratkega dosega predstavljajo pomembne ekonomske in socialne prednosti in priložnosti za razvoj, je prepoznala tudi Evropa. Evropska komisija je tako ob upoštevanju Odločbe Evropskega parlamenta o pravnem okviru politike radijskega spektra v Evropski skupnosti (Odločba o radijskem spektru[2]), leta 2006 izdala Odločbo št. 2006/771/EC, s katero je uskladila frekvenčne pasove in z njimi povezane tehnične parametre, ki zagotavljajo razpoložljivost in učinkovito rabo radijskega spektra za naprave kratkega dosega (*angl.* Short Range Devices). Leto kasneje, marca 2007, je Komisija izdala Sporočilo o radiofrekvenčni identifikaciji ((COM(2007)96[3]) v Evropi. Sporočilo predstavlja rezultate javnega posvetovanja o RFID, pri katerem so izpostavljena pričakovanja v zvezi z RFID tehnologijo ter pomisleki državljanov v zvezi z aplikacijami RFID, ki vključujejo identifikacijo in/ali sledenje osebam. Sporočilo tudi vključuje predloge za nadaljnje ukrepanje pri odpravljanju ovir za uveljavitev tehnologije, ki naj koristi družbi in gospodarstvu, ter hkratnemu vključevanju ustreznih zaščitnih ukrepov na področju varstva zasebnosti, zdravja in okolja.

V letu 2008 smo zasledili množico dogodkov in javnih napovedi o razvoju (evolucije) interneta, ki gre v smeri IoT. Revija Time je v letu 2008 IoT uvrstila med 50 najboljših iznajdb. Tudi Vint Cerf, Google evangelist, ki je prepoznan kot eden od očetov interneta, je septembra 2008 v uradnem Google blogu objavil[4], da bo ekspanzija interneta vključevala tudi IoT. Ameriški National Intelligence Council je novembra objavilo poročilo, v katerem je opisal globalne trende, ki jih lahko pričakujemo do leta 2025. Na podlagi tega poročila je SRI Consulting Business

[2] Evropska komisija 676/2002/ES(2002): Odločba o radijskem spektru

[3] Evropska komisija COM(2007)96 konč. Radiofrekvenčna identifikacija (RFID) v Evropi: naslednji koraki v okviru politike: dosegljvo na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:SL:PDF

[4] The offical Google Blog (2008): The next Internet: dosegljivo na: http://googleblog.blogspot.com/2008/09/next-internet.html

Intelligence internet stvari identificiral[5] kot eno od šestih prelomnih tehnologij, ki bo imela velik vpliv na ameriško nacionalno moč, ekonomski razvoj in vojaške zmogljivosti.

Novembra 2008 je Evropska komisija izdala Sporočilo o prihodnosti omrežij in interneta (COM(2008) 594 konč.[6]). V tem sporočilu Komisija sporoča, da internetna revolucija ni končana, da bo internet postal še hitrejši, kar bo omogočilo zagon novih interaktivnih medijskih storitev in ponujanje vsebin, ter da bo nastal IoT. Komisija v Sporočilu izpostavlja, da bo poleg razvoja in konvergence širokopasovnih žičnih in brezžičnih omrežij, socialnih mrež in interneta storitev, pomemben delež novega nastajajočega trenda predstavljal tudi IoT. Ocenjujejo, da se bo, predvidoma z nastajanjem novih inovativnih aplikacij, v prihodnosti tržni delež tehnologije RFID do leta 2018 povečal za petkrat[7].

V letu 2009 je Evropska komisija izdala Sporočilo Internet stvari – akcijski načrt za Evropo (COM(2009) 278 konč.). Komisija je s tem sporočilom, v katerem je izpostavila 14 področij ukrepanja, podala jasno vizijo, da želi postati vodilna mednarodna sila pri razvoju in implementaciji IoT. IoT po njenem mnenju ne gre razumeti zgolj kot nadgradnjo današnjega interneta, temveč za sklop novih neodvisnih sistemov, ki delujejo s pomočjo lastnih infrastruktur (ter se delno opirajo na obstoječe internetne infrastrukture). IoT, kot je tudi omenjen v poročilu ISTAG[8], bo uveden v sožitju z novimi storitvami in vključuje različne vrste komunikacij: stvari–oseba, stvar–stvar, vključno s komunikacijo stroj–stroj (M2M).

III. RADIJSKI SPEKTER IN STANDARDIZACIJA

Senzorska omrežja bodo zagotavljala platformo za mnogovrsten nabor vertikalnih aplikacij. Mnoge med njimi bodo imele unikatne zahteve, zato bo za razširjenost (naprav in aplikacij) in za zagotavljanje nizke cene ključno, da se bo na globalnem nivoju vzpostavila ustrezna standardizacija poenotenih elementov na nivoju frekvenčnega spektra, komunikacijskih protokolov, naslavljanja, varnosti, zagotavljanja kakovosti storitve, združljivosti med različnimi napravami, aplikacijami in storitvami. Večina današnjih aplikacij, ki bi izkoriščale potencial IoT, je še v testni fazi. Glavna ovira za masovni preboj je predvsem pomanjkanje ali počasni razvoj standardov ter zrelih poslovnih modelov. Standardizacija IoT vključuje številne izdelovalce, se prepleta med različnimi industrijskimi panogami, je široko raznolika zaradi različne uporabe aplikacij, kot je raznolika pri upoštevanju uporabniških zahtev. Vključuje horizontalne tehnične nivoje, kot tudi vertikalne industrijske aplikacijske nivoje.

Pri standardizaciji IoT naprav, omrežij ter pripadajočih storitev in aplikacij deluje vrsta standardizacijskih teles in delovnih skupin. Med njimi bi lahko izpostavili ISO/IEC JTC1, ITU-T (SG 13, 16 in 17 ter JCA-NID), 3GPP, CENELEC, CEN in ETSI, IETF (RFC in 6LoWPAN), IEEE (802.15 in 1415), ZigBee Alliance in druge.

IoT se že sedaj v glavnem povezuje z uporabo brezžičnih tehnologij. Večina teh stvari bo zaradi morebitnih radijskih motenj, škodljivega sevanja ter varčnosti porabe energije uporabljala nizke oddajne moči. To posledično pomeni, da bo doseg signala teh naprav relativno majhen in da je potrebno že sedaj dolgoročno načrtovati in rezervirati ustrezen frekvenčni spekter ter določiti pripadajoče tehnične parametre, s katerimi se lahko zagotovi razpoložljivost in učinkovita raba radijskega spektra za IoT naprave. Osnovna temeljna evropska odločba, ki usklajuje in predpisuje različne frekvenčne pasove, ki jih lahko uporabljajo naprave kratkega dosega, je 2006/771/EC[9]. Navedeno odločbo so od leta 2006 do danes večkrat spreminjali in dopolnjevali. Zadnja veljavna dopolnitev je Odločba št. 2010/368/EC, ki jo je Komisija izdala konec junija 2010.

Ker so naprave kratkega dosega opredeljene kot radijska oprema, se lahko v Evropi prodajajo in uporabljajo le, če so skladne z EU direktivo R&TTE (Equipment and Telecommunications Terminal Equipment). Direktiva (1999/5/EC) predpisuje, da morajo proizvajalci naprav kratkega dosega zagotoviti, da naprave učinkovito uporabljajo radiofrekvenčni spekter in ne motijo drugih naprav, so elektromagnetno združljive z drugimi napravami (Direktiva 2004/108/EC) ter so varne in zdravju neškodljive (Direktiva 2006/95/EC). CE znak na napravi potrjuje, da je naprava združljiva z vsemi relevantnimi evropskimi direktivami ter da jo lahko uporabljamo v vseh državah članicah. Evropske direktive večinoma ne vsebujejo tehničnih parametrov, temveč le evropske standarde (CENELEC, CEN in ETSI), ki so obligatorni za vse države članice EU. Predpostavlja se, da so vsi izdelki, ki ustrezajo harmoniziranim standardom v okviru določene direktive, tudi združljivi z zahtevami, ki jo predpisuje direktiva.

[5] SRI Consulting Business Intelligence (2008): Appendix F: The internet of things (Background), dosegljivo na: http://www.dni.gov/nic/PDF_GIF_confreports/disruptivetech/appendix_F.pdf

[6] COM(2008) 594 konč: dosegljivo na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0594:FIN:SL:PDF

[7] Tržne napovedi IDTechEc za RFID v obdobju od 2008 do 2018

[8] Revising Europe's ICT Strategy (2009): ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-revising-europes-ict-strategy-final-version_en.pdf

[9] EC 2006/771/ES: Odločba o uskladitvi radijskega spektra za uporabo naprav kratkega dosega: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:312:0066:01:SL:HTML

CEPT (European Conference of Postal and Telecommunications Administrations) je v skladu s členom 4(2) Odločbe o radijskem spektru dobil pooblastilo Evropske komisije, da kot koordinacijsko telo uskladi in pripravi regulatorna in tehnična priporočila za naprave kratkega dosega v Evropski skupnosti. Države članice lahko sicer na nacionalni ravni omogočijo delovanje opreme pod manj zahtevnimi pogoji, kot je določeno v Odločbi, vendar v tem primeru takšna oprema ne more delovati v vsej skupnosti brez omejitev (oprema je razvrščena v razred 2 R&TTE Direktive). CEPT je razdelil naprave kratkega dosega glede na namembnost v 13 različnih kategorij[10], ki uporabljajo različna frekvenčna področja ter različne tehnične parametre:

– nespecifične naprave kratkega dosega (Non-specific short range devices),
– sledenje, iskanje in zbiranje podatkov (Tracking, tracing and data acquisition),
– širokopasovni podatkovni sistemi (Wideband data transmission system),
– železniške aplikacije (Railway applications),
– radiodeterminacijske aplikacije (Radiodetermination applications),
– alarmi (Alarms),
– vodenje modelov (Model control),
– induktivne aplikacije (Inductive applications),
– radijski mikrofoni in pomožna sredstva (Radio microphone application including aids for hearing impaired),
– aplikacije z radiofrekvenčno identifikacijo (Radio frequency identification applications),
– aktivni medicinski vsadki in pripadajoče periferne naprave (Active medical implants and their associated peripherals),
– brezžične zvokovne aplikacije (Wireless audio applications).

V Sloveniji frekvenčno področje naprav kratkega dosega (kot tudi drugih radijskih naprav) predpisuje Splošni akt o načrtu uporabe radijskih frekvenc. Zadnjo veljavno spremembo in dopolnitev je Agencija za pošto in elektronske komunikacije Republike Slovenije (v nadaljevanju APEK) kot pristojni organ izdala v maju 2010 (Ur.l. RS št. 42/2010 – NURF-1a).

RFID naprave, senzorji in druge podobne IoT tehnologije, ki so opredeljene v okviru R&TTE in v drugih direktivah, so trenutno še relativno nove tehnologije, še posebej na področju komercialnih izdelkov in aplikacij. Iz tega razloga lahko pričakujemo, da bo še kar nekaj sprememb na področju zagotavljanja zasebnosti in regulatornih predpisov. Za široko razširjenost teh naprav in aplikacij je zato nujno, da se vzpostavi ustrezna standardizacija in regulacija. Ta se bo razvijala tako na tehničnem področju (tehnični parametri), kot na področju zagotavljanja elektromagnetne kompatibilnosti, bioloških učinkov izpostavljenosti na elektromagnetno polje (SAR vrednosti) ter radiofrekvenčnega sevanja, ki jih oddajajo IoT naprave, (negativnega) vpliva uporabljenega materiala na ekologijo (izraba naravnih virov, onesnaženje, poraba energije) ter zagotavljanja zasebnosti in varnosti podatkov.

IV. INTERNET STVARI, DODANA VREDNOST OPERATERJEM

V razvitih državah se danes mnogi operaterji soočajo z zasičenostjo (in končnim) številom uporabnikov ter upadanjem prihodkov predvsem na strani govornih storitev. Količina prometa in hitrost povezav se sicer povečuje, vendar število uporabnikov ne narašča. Za mnoge od teh operaterjev je morda velika priložnost, da svoja komunikacijska omrežja učinkoviteje izrabijo v povezavi s storitvami, ki izkoriščajo potencial IoT. Telemetrija, telematika ter centralizirano upravljanje in nadzor inteligentnih stvari na daljavo so samo ena od množice osnovnih storitev, ki jih lahko kot dodano vrednost ponudijo operaterji.

Mnoge informacije na spletu kažejo na to, da večji operaterji že vzpostavljajo strateška partnerstva z različnimi deležniki z namenom večje izrabe potenciala M2M (*angl*. Machine-to-Machine). Skupna vlaganja in strateška partnerstva se tako že vzpostavljajo z drugimi operaterji, dobavitelji električne energije, plina, vode, avtomobilskimi servisi, zdravstvenimi ustanovami in drugimi. Iz tega razloga tudi ni nenavadno, da je npr. globalni telekomunikacijski operater Orange februarja 2011 objavil[11] sodelovanje z Deutsche Telekom z namenom razvoja skupnih M2M standardov. Podjetji pričakujeta, da bosta s sodelovanjem znižala stroške pri testiranju in uvajanju M2M naprav in storitev, kot bosta tudi lažje zagotovila enako kakovost storitve, še posebej v času gostovanja.

Teoretično se lahko M2M storitve prenašajo čez različna omrežja, tako fiksna kot tudi mobilna. Mobilna omrežja so v primeru M2M storitev v prednosti, saj se z mobilnostjo lahko pokrije širši nabor storitev in aplikacij. Predpogoj za uspešen scenarij uvedbe je stalna povezljivost, širokopasovnost in majhna latenca, ki jo lahko zagotovijo le sodobnejše tehnologije, kot so HSPA(+) ter LTE (Advanced). Razvoj v smeri M2M storitev je tako praktična nuja za vse mobilne operaterje, ki se vse bolj osredotočajo na podatkovne

[10] ERC/REC 70-03 (priporočilo za naprave kratkega dosega v Evropi) http://www.ecodocdb.dk/doks/filedownload.aspx?fileid=1694&fileurl=http://www.erodocdb.dk/Docs/doc98/official/pdf/REC7003E.PDF

[11] Hilton, S. (2011): DT and FT/Orange join forces for M2M, dosegljivo na: http://www.connectedworldmag.com/latestNews.aspx?id=NEWS110211122446003

storitve, ki jih sedaj zagotavljajo 3G omrežja. Bodoči razvoj in strategije operaterjev mobilnih komunikacij je lahko tudi usmerjen v zagotavljanju M2M storitev, ki so lahko dobro nadomestilo ob izgubi dohodkov iz naslova govornega prometa.

Podobno lahko iz naslova M2M storitev dodatne prihodke pridobijo tudi operaterji fiksnih omrežij. Le-ti se lahko povežejo z dobavitelji električne energije, vode, plina, ponudniki zagotavljanja varnosti. Temu trendu so prisluhnili tudi razvijalci (rezidenčnih) usmerjevalnikov (npr. Cisco), ki že razvijajo naprave, ki poleg priklopa računalnikov in VoIP terminalov omogočajo priklop različnih senzorjev z uporabo protokolov kot so npr. ZigBee ali Z-Wave. Kot dober primer uspešne izrabe senzorjev v rezidenčnem okolju je npr. Švedska. Ta je leta 2007 sprejela zakon, ki obvezuje dobavitelje električne energije, da mesečno obračunavajo porabo električne energije le po dejanski porabi. Göteborg Energi, švedska javna gospodarska družba, ki dobavlja električno energijo, plin in ogrevanje, je vzpostavila po celem mestu Göteborg brezžično omrežje temelječo na tehnologiji ZigBee. V vsaki hiši in stavbi je števec električne energije (270.000 števcev), ki brezžično komunicira z lokalno zbiralno enoto. Enota je preko širokopasovne povezave neposredno povezana s centralnim upravljavskim centrom. Uporabljena tehnologija dobavitelju električne energije zmanjšuje stroške odčitavanja, potrošniki pa imajo stalen pregled nad porabljeno energijo. V načrtu je razširitev sistema na druge storitve (odčitavanje porabe in nepotrebno odtekanje vode, nadzor požarnih alarmov, zdravstvena oskrba ...).

V. ZASEBNOST IN VARNOST

Uvedbo IoT trenutno spremljajo številni pomisleki, predvsem glede možne zlorabe zasebnosti in podatkov. Številni avtorji navajajo, da lahko z uvedbo IoT zagotovimo gospodarske in družbene koristi, vendar je za njihovo masovno uvedbo ključno, da imamo predhodno vzpostavljene učinkovite ukrepe, s katerimi lahko zagotovimo ustrezno varstvo osebnih podatkov, zasebnosti in s tem povezanih pravnih in etičnih načel. Dejstvo je, da sta zasebnost in varstvo osebnih podatkov temeljni pravici, ki sta zapisani v Listini EU o temeljnih pravicah. Z direktivo o varstvu podatkov iz leta 1995 pa so se splošna načela o obdelavi osebnih podatkov ter pravici ljudi uskladila tudi v vseh nacionalnih zakonodajah članic držav EU (v Sloveniji: Zakon o varstvu osebnih podatkov, ZVOP-1 UPB1).

Uvedba nove tehnologije, kot je IoT, ne sme zmanjšati varnosti in pravice ljudi, in sicer ne le na nivoju svobode misli, vesti in veroizpovedi, temveč tudi na nivoju zagotavljanja zasebnosti in varnosti njihovih osebnih podatkov pri obdelavi, shranjevanju ali prenosu informacij. Zagotavljanje zasebnosti in varnosti podatkov in aplikacij na področju elektronskih komunikacij je ukrep, ki ni nov in ga ureja tako Zakon o elektronskih komunikacijah, kot tudi Zakon o varstvu osebnih podatkov.

Evropska Komisija si že vseskozi prizadeva, da bi v državah članicah EU dosegli čim manjšo obdelavo osebnih podatkov in uporabo anonimnih ali psevdonimnih podatkov, s katerimi bi zagotovili boljše varovanje zasebnosti. Maja leta 2009 je v sodelovanju z zainteresiranimi stranmi, med katerimi so bili predstavniki panoge RFID ter organizacij za varstvo podatkov in pravic potrošnikov, pripravila *Priporočilo* (2009/387/ES[12]) *o izvajanju načel varstva zasebnosti in varstva podatkov v aplikacijah, podprtih z radiofrekvenčno identifikacijo*. Namen Priporočila je vzpostavitev potrebnih smernic pri uporabi, zasnovi in delovanju RFID aplikacij in naprav. Smernice bi zagotovile, da se RFID aplikacije in naprave uporabljajo na zakonit, etičen ter družbeno in politično sprejemljiv način ter ob spoštovanju pravice do zasebnosti in zagotavljanju varstva osebnih podatkov. Komisija je želela s smernicami zagotoviti, da se vprašanje zasebnosti in varstva podatkov ne obravnava le pri sami uporabi RFID aplikacij in naprav, temveč tudi že pri načrtovanju, pred uvedbo RFID izdelka ali storitve. Priporočilo namreč navaja, da države članice zagotovijo, da upravljavci pred uvedbo opravijo oceno posledic izvajanja aplikacije RFID na varstvo zasebnosti in osebnih podatkov ter posledično sprejmejo ustrezne tehnične in organizacijske ukrepe za varstvo podatkov pred nepooblaščenim razkritjem ali dostopom ter druge varnostne obveznosti, ki so določene z nacionalno zakonodajo. Upravljavci aplikacij RFID bi morali sprejeti vse ustrezne ukrepe, s katerimi bi zagotovili, da se s sredstvi, ki bi jih lahko uporabil upravljavec aplikacije RFID ali katerakoli druga oseba, podatki ne nanašajo na določene ali določljive fizične osebe, razen če so taki podatki obdelani v skladu z veljavnimi načeli in pravnimi predpisi o varstvu podatkov. Z namenom, da bi bil okvir ocenjevanja učinkov na varstvo zasebnosti ustrezno obravnavan, je bila v juliju 2009 v skladu s Priporočilom vzpostavljena neformalna delovna skupina sestavljena iz različnih predstavnikov industrije, katere cilj je bil pripraviti ustrezen Okvir ocenjevanja učinkov na varstvo zasebnosti pri uporabi RFID aplikacij (OUV).

Pomembno spremembo pri uporabi RFID naprav v povezavi z elektronskimi komunikacijskimi omrežji je prinesla tudi Direktiva 2009/136/ES[13], objavljena novembra 2009. Direktiva spreminja tako Direktivo 2002/22/ES (Direktiva o univerzalnih storitvah) kot

[12] 2009/387/ES: Priporočilo Evropske komisije o izvajanju načel varstva zasebnosti in varstva podatkov v aplikacijah, podprtih z RFID

[13] EC 2009/136/ES: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:SL:PDF

tudi Direktivo 2002/58/ES (Direktiva o obdelavi osebnih podatkov na področju elektronskih komunikacij). V direktivi je navedeno, da je pri uporabi naprav za radiofrekvenčno identifikacijo, ki so priključene na javno dostopno elektronsko komunikacijsko omrežje, ali če uporabljajo elektronske komunikacijske storitve kot osnovno infrastrukturo, potrebno uporabljati ustrezne določbe Direktive o zasebnosti in elektronskih komunikacijah (2002/58/ES), vključno z določbami o varnosti, podatkih o prometu in lokaciji ter o zaupnosti.

Poleg tega mora ponudnik javno razpoložljive elektronske komunikacijske storitve sprejeti ustrezne tehnične in organizacijske ukrepe, da zagotovi varnost svojih storitev. Do osebnih podatkov ima lahko dostop le pooblaščeno osebje za zakonite oziroma dovoljene namene, shranjeni ali preneseni osebni podatki ter omrežja in storitve pa morajo biti zaščiteni. Z namenom odkritja morebitnih pomanjkljivosti sistema je potrebno vzpostaviti varnostno politiko za obdelavo osebnih podatkov in poskrbeti za redno spremljanje in izvajanje preventivnih, korektivnih in blažilnih ukrepov.

O tem, kako operaterji kot izvajalci storitev zagotavljajo tajnost, zaupnost in varnost elektronskih komunikacij v Sloveniji, govori Splošni akt o tajnosti, zaupnosti in varnosti elektronskih komunikacij ter hrambi in zavarovanju hranjenih podatkov (Ur.l. RS št. 126/2008).

V aprilu 2010 je bil s strani predstavnikov industrije pripravljen predlog Okvirja OUV[14]. Objavljen je bil na spletnih straneh Komisije ter hkrati predan v odobritev Delovni skupini za varstvo podatkov iz člena 29 (Article 29 Working Party), ki jo sestavljajo predstavniki evropskih organov za varstvo podatkov. O navedenem dokumentu se je izjasnila[15] tudi Evropska agencija za varnost omrežij in informacij (ENISA). V predlaganem PIA Okvirju (Privacy Impact Assessment) so se identificirali vsi glavni vplivi in tveganja, ki se nanašajo na zasebnost in varnost podatkov pri uporabi vseh RFID aplikacij. Okvir vsebuje priporočila kako naj ocenjujemo tveganja, vključno s sorazmernimi ukrepi, ki jih moramo sprejeti za zagotavljanje ustreznega varstva zasebnosti uporabnikov in podatkov. V smislu preventivnega pristopa Okvir spodbuja RFID operaterje, da že v fazi razvoja in pri vzpostavljanju arhitekture razvijejo takšne RFID aplikacije, ki nimajo vpliva na zasebnost oziroma ne zbirajo in obdelujejo osebnih podatkov ali pa že vsebujejo ustrezne mehanizme in kontrole, ki zlorabo teh podatkov preprečujejo. Delovna skupina v zvezi s tem meni, da razvoj OUV prispeva h konkurenčnosti evropske panoge RFID, saj pospešuje inovativne pristope k obravnavanju vprašanj varstva podatkov in zasebnosti s tehnologijami, kot so anonimiziranje podatkov, delno deaktiviranje oznak, lahke kriptografske storitve itd. Pomemben del predstavljenega okvirja pa je tudi t.i. PIA proces, na podlagi katerega lahko operaterji RFID aplikacij ocenijo – klasificirajo vpliv aplikacij na zasebnost in varstvo podatkov.

Okvir je RFID aplikacije razvrstil na več nivojev. Na najnižjem nivoju so aplikacije, ki ne obdelujejo osebnih podatkov in katerih oznake upravljajo uporabniki – zaposleni (aplikacija ni narejena za spremljanje zaposlenih). V tem primeru varstvo podatkov in zasebnosti ni ogroženo (dokumentacija ni potrebna). Naslednji nivo so aplikacije, v katerih se osebni podatki ne obdelujejo, posamezniki (fizične osebe) pa nosijo/imajo RFID oznake. Naslednji nivo vključuje aplikacije, s katerimi se obdelujejo osebni podatki, vendar oznake osebnih podatkov ne vsebujejo (aplikacije povezujejo neosebne RFID oznake z osebami in osebnimi podatki). Na najvišjem nivoju so aplikacije, kjer so osebni podatki shranjeni na RFID oznaki. Za te aplikacije je potrebno vzpostaviti poseben 'varnostni' režim v skladu z varstvom osebnih podatkov. Ti podatki se lahko npr. nanašajo na: ime, datum rojstva in naslov osebe, biometrične ali zdravstvene podatke osebe, ali pa na podatke, ki določeno številko postavke RFID povezujejo z osebnimi podatki, shranjenimi drugod v sistemu. Štirinivojski model klasifikacije RFID aplikacij v povezavi z uporabo osebnih podatkov nazorno predstavlja Tabela 1.

Tabela 1: PIA Okvir: klasifikacija RFID aplikacij

Nivo	Ali RFID oznake vsebujejo osebne podatke?	Ali se RFID aplikacije povezujejo z osebnimi podatki?	Ali imajo posamezniki dostop do več-nivojsko označenih RFID izdelkov?
0	Ne	Ne	Ne
1	Ne	Ne	Da
2	Ne	Da	Da
3	Da	Da	Da

Zbiranje različnih podatkov, ki se nanašajo na isto osebo, kot je npr. aktualno zdravstveno stanje, sledenje posameznikom po javnih prostorih (letališčih, železniških postajah, trgovinah), profiliranje s spremljanjem vedenja potrošnikov v trgovinah ter branje podatkov o oblekah, dodatkih in zdravilih, ki jih nosijo ali uporabljajo potrošniki, pomeni primere vrst uporabe tehnologije, ki marsikomu zbuja številne

[14] Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications (2010), dosegljivo na: http://ec.europa.eu/information_society/policy/rfid/documents/d31031industrypia.pdf

[15] Enisa (2010): ENISA Opinion on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications: http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia

pomisleke. Ker gre z vidika zasebnosti in varstva osebnih podatkov za posebej kritične podatke, je potrebno v RFID oznake, senzorje in aplikacije, s katerimi upravljamo z generiranimi podatki, pred njihovo širšo uporabo vgraditi določene varovalne lastnosti oz. funkcije, ki bodo zagotavljale ustrezno varstvo zasebnosti in informacij (načelo varstva zasebnosti pri snovanju sistemov). Tisti, ki uvajajo tovrstno tehnologijo so odgovorni, da posameznikom zagotovijo informacije o uporabi teh informacij ter ustrezne varnostne ukrepe, ki bodo onemogočali njihovo razkritje ali dostop nepooblaščenim osebam skozi celoten življenjski cikel njihove uporabe.

V zvezi z navedenim bi izpostavili nekaj pomembnih dejstev, s katerimi bi lahko zagotovili transparentnost obdelave podatkov in s katerimi bi lahko povečali zaupanje uporabnikov do RFID in podobnih IoT tehnologij. Uporabnik oziroma potrošniki bi morali imeti:

- pravico do informacije o prisotnosti RFID oznak (informacija o prisotnosti RFID oznak bi morala biti vidno označena),
- pravico do odstranitve, deaktivacije ali uničenja RFID oznake, ko je izdelek kupljen (oznaka bi se morala samodejno uničiti najkasneje, ko npr. potrošnik zapusti trgovino),
- pravico vedeti, katere informacije so shranjene na RFID oznaki oziroma jih popraviti, v kolikor so napačne,
- pravico vedeti kdaj, kje in s kakšnim namenom je bila določena RFID oznaka prebrana, pri čemer imajo lahko dostop do podatkov samo pooblaščeni uporabniki,
- organizacije bi morale jasno označiti prostore, kjer se uporablja RFID sprejemnike,
- RFID oznake s spominom, bi morale hraniti informacijo kolikokrat in kdaj so bile prebrane.

Pri klasifikaciji posameznih aplikacij, RFID oznak in senzorjev glede na predstavljen Okvir si lahko pomagamo z naslednjimi vprašanji:

- Ali RFID aplikacija obdeluje osebne podatke?
- Ali RFID oznaka vsebuje osebne podatke?
- Ali je RFID aplikacija povezuje informacije na RFID oznaki z osebnimi podatki?
- Ali naj bi bili označeni predmeti v lasti posameznikov?

V kolikor lahko na zgornja vprašanja odgovorimo z *Ne*, gre za najnižjo stopnjo 0, kjer obdelava osebnih podatkov ni vprašljiva. Okvir določa, da v kolikor aplikacija RFID izpolnjuje vsaj stopnjo 1 (aplikacija ne obdeluje osebnih podatkov in RFID oznake ne vsebujejo osebnih podatkov, vendar naj bi bili v lasti posameznika), mora upravljavec opraviti podrobno štiridelno analizo aplikacije, katere rezultat je poročilo, ki je na razpolago pristojnemu organu.

V najvišji, tretji stopnji aplikacije RFID obdelujejo osebne podatke in RFID oznake vsebujejo osebne podatke (npr. medicinski ali biometrični podatki), zato je potrebno vzpostaviti ustrezne mehanizme za zagotavljanje zasebnosti in varstva podatkov. Ta mora biti sorazmerna z ugotovljenimi posledicami, ki jih ima le-ta na varstvo zasebnosti in podatkov.

Predlog Okvirja je dobil določene pripombe tako s strani Delovne skupine za varstvo podatkov iz člena 29, kot s strani agencije ENISA. Zaradi tega je šel predlog v ponovno branje in prenovo. Končni Okvir[16], ki določa obravnavo RFID aplikacij in ki vključuje tudi vse pripombe, je bil sprejet 12.1.2011.

Značilnosti sprejetega PIA okvirja so naslednje:

- omogoča harmonizacijo potrebnih pogojev, ki jih morajo izpolnjevati operaterji RFID aplikacij,
- operaterji RFID aplikacij morajo razviti PIA proces za vsako RFID aplikacijo, ki jo upravljajo (če operaterji uporabijo eno RFID aplikacijo za več izdelkov, storitev ali procesov, je lahko PIA poročilo eno samo).

PIA Okvir v povezavi z mednarodnim standardom ISO/IEC 27005, ki zagotavlja priporočila pri upravljanju varnosti informacij bi moral postati splošno sprejeta shema samoocenjevanja RFID aplikacij. Na njuni podlagi lahko podjetja uvedejo nove ali razširijo obstoječe RFID aplikacije (javni prevoz in druge javne storitve, maloprodaja in logistika, službene izkaznice, mobilni telefoni z NFC[17] in drugo). Končno poročilo analize mora biti na vpogled pristojnem organu. Za državljane in potrošnike, ki pridejo v stik s takimi aplikacijami RFID, pa je objava takšnega poročila možnost, da preverijo ali njihova uporaba ne ogroža njihove zasebnosti ali varstva podatkov.

VI. ZAKLJUČEK

RFID trenutno igrajo prevladujočo vlogo, in sicer kot podatkovni vir za internet stvari. RFID sprejemniki oddajajo v realnem svetu stvari zbrane informacije v navidezni svet ERP sistemov podjetij. RFID oznake bodo nasledili senzorji, lokalni ERP sistemi bodo migrirali v računalništvo v oblaku. Uvedba novih tehnologij, kot so RFID oznake in aplikacije ter druge IoT tehnologije, ne sme v ničemer zmanjševati varnosti osebnih podatkov oziroma kratiti pravice ljudi do zasebnosti. Samo, če bodo ljudje prepričani, da so njihove pravice zavarovane tudi z ustrezno zakonodajo, skupaj z ustreznimi možnostmi do pravnega varstva v primeru njihovih kršitev, bodo IoT tehnologije in

[16] Article 29 Working Party (2011): Privacy and Data Protection Impact Assessment Framework for RFID Applications, dosegljivo na: http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf

[17] NFC: Near Field Communication

pripadajoče aplikacije masovno sprejete. V Evropi je sprejet Okvir, ki podrobno določa na kakšen način moramo obravnavati uporabo RFID oznak in pripadajočih aplikacij. Čeprav Okvir eksplicitno obravnava samo RFID in ne tudi brezžičnih senzorjev, ki bodo tehnološki naslednik RFID oznakam, je zaradi skupnih elementov trenutno najustreznejši pravni okvir tudi za vse podobne IoT tehnologije, ki bodo omogočale zaznavanje in identificiranje lastnosti okolja, naprav in ljudi.

Kljub vsemu je PIA Okvir le generična shema, ki bi se morala dopolnjevati s prakso in predlogami, ki bi podrobneje določale specifične primere uporabe RFID aplikacij. Razvoj aplikacij, še posebej tistih, ki obdelujejo osebne podatke, je namreč izredno pomemben, s porastom IoT senzorjev in naprav pa bo to postalo še toliko pomembneje. Le-ti bodo sprejeti le, če bodo odobreni s stani pristojnih organov in če bodo uživali zaupanje potrošnikov/uporabnikov. Vzpostavitev krhkega ravnotežja med zagotavljanjem zasebnosti in varnosti na eni strani ter ekonomskih potreb na drugi, prav tako pa tudi nizka cena, standardizacija ter zaupanje in soglasje vseh vpletenih deležnikov, bodo ključni faktorji pri nadaljnjem razvoju interneta stvari.

LITERATURA

[1] ISTAG (1999): Orientation for Workprogramme 2000 and Beyond, dosegljivo na: ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-99-final.pdf

[2] ITU (2005): Internet Reports 2005: The Internet of Things: http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf

[3] ITU (2008): Ubiquitous Sensor Networks (USN), dosegljivo na: http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000040001PDFE.pdf

[4] Article 29 Working Party (2011): Privacy and Data Protection Impact Assessment Framework for RFID Applications, dosegljivo na: http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf

[5] EC 2009/387/EC konč.: Priporočilo komisije o izvajanju načel varstva zasebnosti in varstva podatkov v aplikacijah, podprtih z radiofrekvenčne identifikacijo

[6] EC COM(2007)96 konč. Radiofrekvenčna identifikacija (RFID) v Evropi: naslednji koraki v okviru politike: dosegljvo na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0096:FIN:SL:PDF

[7] EC COM(2009) 278 konč.: Sporočilo Internet stvari – akcijski načrt za Evropo

[8] EC 2010/368/EU: SKLEP KOMISIJE z dne 30. junija 2010 o spremembi Odločbe 2006/771/ES o uskladitvi radijskega spektra za uporabo naprav kratkega dosega, dosegljivo na: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:166:0033:0041:SL:PDF

[9] Raunio, B. (2010): The Internet of things, A report from the November 5, 2009 Seminar, dosegljivo na: http://www.iis.se/docs/The-Internet-of-things.pdf

[10] Weber, H.R. (2009): Internet of things – Need for a new legal environment?, SceinceDirect 2009 (522-527)

[11] Weber, H.R. (2010): Internet of things – New security and privacy challenges, ScienceDirect 2010 (23-30)

[12] Garcia-Hernando, A, Martinez-Ortega, J., Lopez-Navarro, J. Prayati, A., Redondo-Lopez, L. (2008): Standards and Safety Regulations for WSNs, Computer Communications and Networks, 2008, Problem Solving for Wireless Sensor Networks, Pages 1-11

[13] Santucci, G. (2009): From Internet of Data to Internet of Things, Paper for the International Conference on Future Trends of the Internet, dosegljivo na: http://ec.europa.eu/information_society/policy/rfid/documents/Iotconferencespeech012009.pdf

Urban Kunc je magistriral na Fakulteti za organizacijske vede s področja informatike. Aktivno spremlja sodobne tehnologije. Trenutno je zaposlen na Agenciji za pošto in elektronske komunikacije RS na področju inšpekcijskega nadzora Je član strokovnega sveta Zavoda go6 ter aktiven promotor uvedbe protokola IPv6 v Sloveniji.

Internet stvari in vgrajena zasebnost

mag. Andrej Tomšič, namestnik informacijske pooblaščenke, Informacijski pooblaščenec RS

Povzetek — Članek se ukvarja z vprašanji zasebnosti v informacijski družbi s poudarkom na internetu stvari. Kot orodje za obvarovanje zasebnosti na primeru elektronskega cestninjenja v prostem prometnem toku predstavlja koncept vgrajene zasebnosti in opozarja na pojav širitve prvotnega obsega obdelave podatkov.

Ključne besede — internet stvari, zasebnost, varstvo osebnih podatkov, vgrajena zasebnost.

Abstract — This article deals with the challenges for privacy in the information society. It presents the concept of privacy by design in the case of electronic toll collection and warns about the inherited dangers of the function creep effect.

Keywords — internet of things, privacy, personal data protection, privacy by design.

I. UVOD

Internet stvari prinaša številne družbeno-ekonomske posledice, namen tega prispevka pa je dotakniti se vidika varstva zasebnosti s poudarkom na informacijski zasebnosti (varstvu osebnih podatkov). Čeprav je govora o internetu stvari, namreč ne moremo mimo tega, da stvari uporabljamo ljudje, z zmožnostmi hrambe in obdelave podatkov o delovanju in uporabi stvari, pa neizogibno trčimo ob osebne podatke. Pametna elektrodistribucijska omrežja, inteligentni transportni sistemi in RFID značke v maloprodaji so le nekateri od primerov, ko bo prišlo do obdelave podatkov o tem, kako porabljamo energijo, kje in kdaj se vozimo, kakšne so naše nakupovalne navade. Pomembno vprašanje na tej točki je, kako lahko v internetu stvari obvarujemo temeljno človekovo pravico do zasebnosti in ali lahko zakonodaja sploh učinkovito sledi tehnološkemu razvoju?

II. KONCEPT VGRAJENE ZASEBNOSTI

Direktiva o varstvu osebnih podatkov[1] iz leta 1995, ki postavlja zakonodajni okvir za varstvo osebnih podatkov v EU, ni poznala ne Googla, ne Facebooka, ne iPhona, še manj pa interneta stvari. Spremembe zakonodajnega okvira EU na tem področju, ki so najavljene za poletje 2011, bodo morale biti tehnološko nevtralne, dolgoročne in dobesedno vizionarske.

Eno od ključnih orodij novega okvira naj bi bil koncept vgrajene zasebnosti (angl. Privacy By Design), po katerem bi morali razvijalci informacijskih sistemov, produktov in storitev – prav tako pa tudi oblikovalci zakonodaje – že v fazi oblikovanja paziti na načelo minimizacije in sorazmernosti obdelave osebnih podatkov glede na zasledovane cilje ter upoštevati ostala temeljna načela varstva osebnih podatkov (namenskost, zavarovanje itd.). Potencialne težave z vidika varstva osebnih podatkov in zasebnosti naj bi pravočasno predvideli in dizajn sistema vnaprej prilagodili na način, ki zmanjšuje tveganja za zlorabe namesto čakanja na udejanjenje teh tveganj.

Bistven element koncepta vgrajene zasebnosti je zagotavljanje polne funkcionalnosti – z vgradnjo zasebnosti ne bi smeli žrtvovati učinkovitosti delovanja sistema ali drugih legitimno zasledovanih ciljev. Pogosto namreč slišimo, da moramo žrtvovati zasebnost zaradi višje varnosti, praktičnosti ali ekonomičnosti, koncept vgrajene zasebnosti pa temelji na iskanju rešitev, ki nas ne silijo v izbiranje med navedenimi, temveč zagotavljajo oboje. S pričakovano uvedbo obveznega poročanja o varnostnih incidentih v evropskem prostoru (npr. ob izgubah podatkov o strankah) in s tem povezanimi stroški ter izgubo ugleda, bo pomen pravočasne vgradnje zasebnosti v poslovne prakse še toliko večji.

Koncept vgrajene zasebnosti je deležen aktivne promocije v Kanadi, EU in v Sloveniji, kjer je Informacijski pooblaščenec pripravil Smernice za razvoj informacijskih rešitev, od leta 2010 pa bo vsako leto podeljeval tudi posebno priznanje Ambasador zasebnosti. Tega bo prejela organizacija, ki bo na konkretnem primeru uspela pokazati, da je možno ohraniti zasebnost, obenem pa doseči zasledovane cilje. Prvo tovrstno priznanje je v letu 2010 prejel Urad za meroslovje RS za predlog, ki minimizira obdelavo osebnih podatkov in zagotavlja ustrezne postopke zavarovanja podatkov pri izvedbi sekcijskega merjenja hitrosti na avtocestah.

III. ŠIRITEV PRVOTNEGA NAMENA OBDELAVE

Eden od pojavov, ki v krogih varuhov zasebnosti in nadzornih organov na področju varstva osebnih podatkov vzbuja največ skrbi, je pojav širitve prvotnega namena obdelave (angl. function creep).

[1] Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL L 281, 23.11.1995, s spremembami).

Omenjeni pojav je povsem realna možnost tudi pri internetu stvari. V grobem gre za to, da se podatke sprva zbere za določene namene, s časom pa se podatke začne uporabljati še za druge, prvotno nepredvidene namene, ali pa da se dostop do podatkov omogoči prej nenačrtovanim novim uporabnikom. Več kot je podatkov, bolj kot so centralizirani in višja kot je njihova uporabna vrednost, večji bodo apetiti po podatkih, pa čeprav so bili zbrani za prvotno povsem drugačne in legitimne namene. Pojav je posebej zaskrbljujoč, saj ga težko prepreči tudi zakonodaja – če namreč obstaja zadostna politična moč ali moč različnih interesnih skupin, potem se pojav širitve prvotnega namena obdelave dejansko lahko zakonito omogoči s spremembo zakonodaje. Karikirano povedano državi ni treba kršiti zakonov, saj jih lahko spreminja.

Predstavimo pojav širitve prvotnega namena obdelave in koncept vgrajene zasebnostina konkretnem primeru iz domene interneta stvari. Inteligentni transportni sistemi (angl. Intelligent Transport Systems) obetajo korenite spremembe na področju upravljanja prometa, v sklop teh sprememb pa sodi tudi elektronsko pobiranje cestnine v prostem prometnem toku, kar zahteva Direktiva Evropskega parlamenta in Sveta 2004/52/ES z dne 29. aprila 2004 o interoperabilnosti elektronskih cestninskih sistemov v Skupnosti (UL L 166, 30. 4. 2004, v nadaljevanju: Direktiva 2004/52/ES).

Uvodoma je treba poudariti, da elektronsko cestninjenje v prostem prometnem toku po naravi stvari vključuje obdelavo velike količine osebnih podatkov, in sicer lokacijske in časovne podatke o prevoženi poti oziroma nahajališču osebnega vozila. Mnenje glede varstva osebnih podartkov pri tovrstnem cestninjenju je zato še pred uvedbo takšnega načina cestninjenja že pripravil Informacijski pooblaščenec. Končni cilj Direktive 2004/52/ES je namreč uvesti plačevanje po načelu »plačaj, kolikor prevoziš«, prav tako pa naj bi vseevropsko delujoči sistem omogočal cestninjenje vseh vrst plačljivih cest, vključno z viadukti, predori in drugimi objekti, pri tem pa brez obdelave omenjenih osebnih podatkov ne gre. Z novim cestninskim sistemom naj bi bilo možno plačevanje cestnine brez vsakršnega oviranja in ustavljanja, poleg tega bi z isto napravo lahko plačevali cestnino na vseh evropskih cestah, ki bodo opredeljene kot cestninske ceste. Direktiva 2004/52/ES dopušča uvedbo obeh najpogosteje preučevanih tehnologij, in sicer tehnologije mikrovalov kratkega dosega (DSRC) ter sistem na osnovi satelitskega določanja položaja vozila in prenosa podatkov po zmogljivih brezžičnih komunikacijskih omrežjih (GNSS/CN) – za slednje se pogosto uporablja kar izraz satelitsko cestninjenje. Možni sta torej obe tehnologiji. Tako ena kot druga imata svoje prednosti in slabosti, mikrovalovne tehnologije so na primer že precej bolj razširjene in preizkušene, niso pa primerne za cestninjenje vseh cest. Prednost satelitskega cestninjenja je predvsem v fleksibilnosti, po drugi strani pa sistem v širšem evropskem prostoru še ni dovolj preizkušen.

Pri elektronskem cestninjenju v prostem prometnem toku bo namen obdelave podatkov o prevoženih poteh jasen – pobiranje cestnine in takšna bo predvidoma tudi pravna podlaga za obdelavo osebnih podatkov. Koga bi ti osebni podatki – če bodo zbrani v lepi centralizirani zbirki – še zanimali? Organe pregona, zavarovalnice, oglaševalce … Brez upoštevanja koncepta vgrajene zasebnosti je glede na izkušnje iz preteklosti zloraba namenskosti – zakonita ali nezakonita – neizogibna in zbirka podatkov o naših prevoženih poteh je za marsikoga zelo mamljiva. Verjetno edina možnost, ki lahko prepreči pojav širitve prvotnega namena obdelave in ohrani zasebnost voznikov, je pristop, ko so podatki, ki so potrebni za izvedbo samega cestninjenja, pod izključnim nadzorom uporabnika. V tem primeru se obračun cestnine izvrši v napravi sami (t.i. inteligentna naprava ali Smart Client), nadzornemu centru pa se posreduje samo seštevek potrošene vsote. Vse štiri faze obračunskega postopka pri elektronskem cestninjenju se torej v tem primeru izvedejo v sami napravi:

1. določitev lokacije,
2. določitev cestninskega segmenta in ustrezne tarife,
3. izračun porabljene vsote za ta segment,
4. seštevek porabljenih vsot.

V takšnem primeru lahko govorimo o tem, da ohranjamo anonimnost voznika, saj ima uporabnik vse lokacijske in časovne podatke shranjene pri sebi, identificirati pa se mora le v primeru, da se pojavijo nepravilnosti, ki to dejansko terjajo: npr. ko uporabnik ne plača pravilno obračunane cestnine, ko mu je bilo ukradeno osebno vozilo, ko njegova naprava za cestninjenje ne deluje pravilno oziroma ne deluje takrat, ko bi morala (med vožnjo po cestninski cesti). Vse dokler ne nastopi ena od takšnih situacij, je potrebno zagotoviti zgolj to, da naprava v vozilu, ki obračunava cestnino po prevoženih kilometrih, na cestninski cesti deluje in da deluje pravilno. Seveda terja takšen pristop tudi določene varovalke, tako je potrebno poskrbeti za ustrezne standarde certificiranja, nameščanja in popravljanja naprav, gotovo pa ne gre odmisliti tudi nekaterih tehničnih izzivov (npr. napajanje, preverjanje pravilnosti delovanja) in stroškovnih vidikov – pametna naprava je gotovo dražja. Nadzorni center pri takšni zasnovi sistema nima podatkov o dejanskih lokacijah osebnega vozila in zgolj preverja pravilnost delovanja naprave. Da

vprašanje zasebnosti ni postranskega pomena pri uvajanju takšnega sistema kažejo izkušnje iz Nizozemske, kjer so se ob vladnem predlogu centralizirane obdelave podatkov na ulicah zbrali protestniki, ki so javno nasprotovali sledenju oseb in vlada je morala predlog umakniti.

V opisanem primeru gre za upoštevanje koncepta vgrajene zasebnosti, kjer se že ob definiranju funkcionalnosti pri dizajnu rešitve upošteva načelo minimizacije osebnih podatkov in ostala temeljna načela varstva osebnih podatkov, kot so sorazmernost, namenskost in zavarovanje podatkov. Obdelava podatkov pod nadzorom posameznika seveda ne pomeni, da drugi nameni uporabe teh podatkov niso mogoči. Če se recimo posameznik strinja, da zavarovalnica spremlja njegove vožnje in mu v zameno ponudi določene ugodnosti pri avtomobilskem zavarovanju, lahko podatke s privolitvijo posameznika še vedno dobi. Brez upoštevanja koncepta vgrajene zasebnosti pa je scenarij širitve prvotnega namena obdelave povsem realen in verjetno je le vprašanje časa, kdaj bi dostop do podatkov dobili organi pregona, zavarovalnice, oglaševalci in drugi.

IV. ZAKLJUČEK

Internet stvari predstavlja le enega v množici izzivov za zasebnost v informacijski družbi; računalništvo v oblaku, družbena omrežja, virtualne identitete so le nekateri od teh izzivov. Obvarovanje zasebnosti v informacijski družbi je ob upoštevanju hitrosti tehnološkega razvoja in po drugi strani »hitrosti« prilagajanja zakonodajno-regulativnega okvira težka naloga. Rešitve morajo biti tehnološko nevtralne in dovolj dolgoročne. Med njimi se kot pomembno orodje kaže koncept vgrajene zasebnosti. Da pa bi koncept vgrajene zasebnosti dejansko zaživel, ga bodo morali upravljavci zbirk osebnih podatkov dojeti kot investicijo in ne kot strošek. Bodoči zakonodajni okvir na področju varstva osebnih podatkov v EU bo moral to dojemanje zagotoviti tako s spodbudami, kakor tudi z ostrejšimi sankcijami v primeru zlorab.

LITERATURA

[1] Mnenje Informacijskega pooblaščenca o varstvu osebnih podatkov pri elektronskem cestninjenju, 14.7. 2008, dosegljivo na: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/odlocbe-in-mnenja-varstvo-osebnih-podatkov/?tx_jzvopdecisions_pi1[showUid]=1802&cHash=73fdc0f4db

[2] Andrej Tomšič in Alenka Jerše: Elektronsko cestninjenje – na račun zasebnosti? Pravna praksa, št. 46/2007.

[3] Why Privacy by Design is the next crucial step for privacy protection"; Simon Davies, London School of Economics & Privacy International, http://www.i-comp.org/blog/wp-content/uploads/2010/10/privacy-by-design.pdf

[4] Privacy by Design, Enterprise Privacy Group; dosegljivo na: http://www.ico.gov.uk/upload/documents/pdb_report_html/index.html

[5] Privacy by Design Resolution, 32nd International Conference of Data Protection and Privacy Commissioners, 27-29 October 2010, Jerusalem, Israel, dosegljivo na: http://www.privacybydesign.ca/content/uploads/2010/11/pbd-resolution.pdf

[6] Smernice informacijskega pooblaščenca za razvoj informacijskih rešitev, 6. 12. 2010, dosegljivo na: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice

Andrej Tomšič je namestnik informacijske pooblaščenke, ukvarja pa s pravnimi, tehnološkimi in družbeno-ekonomskimi izzivi zasebnosti v informacijski družbi. Je član mednarodne delovne skupine IWGDPT in Article 29 Working Party Technology Subgroup. Opravljen ima tečaj in izpit za vodilnega presojevalca za standard varovanja informacij ISO/IEC 27001:2005.

Vloga IK tehnologij pri uvajanju konceptov pametnih omrežij

Andrej Souvent, Elektroinštitut Milan Vidmar
Tomaž Pfajfar, 2e d.o.o.
Igor Papič, Univerza v Ljubljani, Fakulteta za elektrotehniko

Povzetek — Tradicionalna omrežja, za katera so značilne velike proizvodne enote in centralno vodenje, bodo evolucijsko prešla v pametna omrežja, ki bodo poleg centralne proizvodnje vključevala veliko število majhnih proizvodnih enot – razpršene vire. V članku so podani glavni razlogi, zaradi katerih uvajamo pametna omrežja. Predstavljenih je nekaj ključnih konceptov pametnih omrežij, predvsem v luči potrebnih informacijsko komunikacijskih tehnologij.

Ključne besede — pametna omrežja, elektroenergetski sistem, informacijsko komunikacijske tehnologije

Abstract — Traditional networks with their typical large generation units and centralized control will evolve into smart grids. These will, in addition to centralized generation, include numerous small production units – distributed generation. The main reasons for introducing smart grids are presented in the paper and some key smart grids concepts described from the standpoint of required information communication technologies.

Keywords — SmartGrids, electrical power system, information communication technologies.

I. UVOD

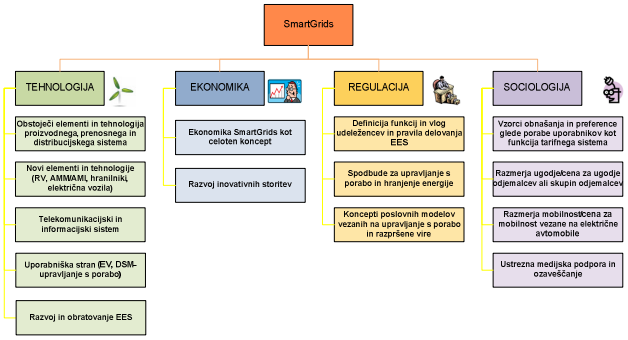
Splošno pomanjkanje energije v Evropi, težave pri umeščanju energetskih objektov v prostor in zagotavljanje tehničnih pogojev za delovanje energetskega trga narekujejo nov tehnološki razvoj elektroenergetike. Zahteve po varčni ter učinkoviti rabi, zahteve po večjem deležu proizvodnje električne energije iz obnovljivih razpršenih virov in nove tehnologije, kot je na primer uporaba električnih avtomobilov in pripadajoče polnilne infrastrukture, pomenijo za elektroenergetski sistem (EES) nov izziv, predvsem, kako tudi v prihodnje zagotavljati zanesljivo, varno in kakovostno oskrbo z električno energijo.

Tradicionalno omrežje, za katerega so značilne velike proizvodne enote in centralno vodenje, bo evolucijsko prešlo v pametno omrežje, ki bo poleg centralne proizvodnje vključevalo veliko število majhnih proizvodnih enot – razpršene vire. Pametna omrežja tudi pomenijo, da bodo imeli uporabniki pomembnejšo vlogo, aktivno bodo prilagajali svojo porabo razmeram v omrežju in kot lastniki malih proizvodnih enot nastopali na trgu kot ponudniki električne energije.

Razvoj omrežij v skladu s konceptom pametnih omrežij prinaša nove rešitve, temelječe na sodobnih informacijsko komunikacijskih tehnologijah (IKT).

II. PAMETNA OMREŽJA

Pametna omrežja (SmartGrids) predstavljajo posodobljen koncept načrtovanja, obratovanja in vodenja elektroenergetskih sistemov v vseh vertikalno razdeljenih nivojih: od proizvodnje, prenosa, distribucije in porabe. Koncepti pametnih omrežij ne zajemajo le tehnologije, temveč tudi druga pomembna področja, brez katerih pametnih omrežij ne bo mogoče vpeljati – potrebno je namreč usklajeno delovanje na tehnološkem, ekonomskem, regulatornem in sociološkem področju (Slika 1).



Slika 1: Področja koncepta pametnih omrežij [1]

Pametna omrežja niso sama sebi namen, ampak poskušajo biti ekonomsko zdržen način reševanja težav, ki so posledica spremenjenih razmer v EES, ki smo jih podali v uvodu. S temi težavami se v precejšnji meri soočamo že danes, realno pa je pričakovati, da se bo nabor težav samo še večal.

Od konceptov pametnega omrežja pričakujemo take rešitve, ki bodo obstoječo infrastrukturo izkoristile stroškovno optimalno. Ojačitve omrežja – investicije v t.i. primarno opremo (vode, transformatorje,...) bodo seveda potrebne tudi v bodoče, vendar se bo pred tem lahko izkoristilo rešitve, ki jih v dosedanjih praksah ni bilo in ki pomenijo predvsem dodatne investicije v t.i. sekundarno opremo (merilni sistemi, sistemi za

avtomatizacijo in zaščito, sistemi vodenja ...) temelječo na IKT.

Področja, ki bodo v prihodnje najbolj vplivala na IKT v elektroenergetiki, so naslednja:
- pametni sistemi za prenosno omrežje,
- napredno upravljanje distribucijskega omrežja,
- avtomatizacija distribucijskega omrežja,
- razpršeni viri energije in koncept virtualne elektrarne,
- napredna merilna infrastruktura (AMI – Advanced Metering Infrastructure),
- upravljanje s porabo (DSM/DR – Demand Side Management/Demand Response),
- pametne zgradbe in pameten dom,
- hranilniki energije,
- e-mobilnost (električna vozila in pripadajoča polnilna infrastruktura).

Uvajanje novih tehnologij pametnih omrežij bo potekalo postopno. Korake za prehod na koncepte SmartGrids lahko razdelimo v naslednje faze [1]:
1. vpeljava tehnologij, ki so na voljo že danes (npr. AMI),
2. oblikovanje novih kriterijev načrtovanja omrežja in oblikovanje novega koncepta obratovanja z upoštevanjem vseh novih elementov v sistemu,
3. agregiranje razpršenih virov in ostalih elementov konceptov SmartGrids v virtualne elektrarne, s katerimi bo mogoče v večji meri nadzorovati obratovanje posameznih elementov in opravljati del sistemskih storitev,
4. postopno vključevanje novih tehnologij, ki šele prihajajo, kot so električna vozila in njihove možnosti vračanja električne energije v elektroenergetski sistem prek pametnih polnilnih mest ter hranilnikov električne energije, vključevanje novih diagnostičnih sistemov za hitro detektiranje okvar v omrežju in sistemov za samoodpravo okvar ipd.

III. Stanje IKT v Slovenskem EES

IKT že vrsto let igrajo pomembno vlogo v poslovnih in tehničnih procesih elektroenergetskih podjetij. Če se v okviru tega prispevka omejimo na tehnične procese, lahko podamo naslednje ugotovitve:
- IKT so že vrsto let temelj sistemov vodenja, avtomatizacije in zaščitnih sistemov, pri čemer so informatizirana visokonapetostna (VN) in srednjenapetostna (SN) omrežja,
- nizkonapetostna (NN) omrežja niso informatizirana,
- omrežja, tako prenosna kot distribucijska, so vodenja centralno iz t.i. centrov vodenja (SCADA – Supervisory Control And Data Acquisition, EMS – Energy management System, DMS – Distribution Management Systems),
- v sistem vodenja so vključene velike proizvodnje enote,
- razpršeni viri niso vključeni v sistem vodenja,
- končni uporabniki s priključno močjo 41 kW ali več so opremljeni s števci, ki omogočajo daljinsko odčitavanje, na voljo so jim dnevni 15-minutni obremenilni diagrami,
- gospodinjski uporabniki in uporabniki na širokem odjemu v veliki večini (96 %) še niso opremljeni s pametnimi števci, ki bi jih tudi informacijsko povezali z elektroenergetskim sistemom,
- uporabniki niso aktivno vključeni s prilagajanjem svojega odjema glede na potrebe EES, razen nekaterih izjem, v glavnem velikih odjemalcev, ki vodijo svojo porabo glede na tržne zahteve in zahteve po zmanjševanju konične obremnitve, glede na katero se zaračunava obračunska moč.

Komunikacijske tehnologije, ki so v glavnem v uporabi so:
- TDM (PDH, SDH ...) in
- paketne tehnologije (X.25, Ethernet, IP, MPLS).

V nadaljevanju poglejmo zahteve nekaterih novih tehnologij do IKT, ki jih prinašajo pametna omrežja.

IV. Nove tehnologije in zahteve

A. *Prenosno omrežje*

Na področju prenosnih omrežij se v koncept nadzora in vodenja omrežja uvajajo sistemi WAMS (Wide Area Monitoring Systems). Tradicionalnim meritvam moči, napetost in tokov se tako pridrožujejo nove, v tem primeru meritve fazorjev napetosti in toka. Te merijo PMU (Phasor Measurement Units) senzorji.

WAMS omogoča sinhrono opazovanje dinamike EES in daje hitro in zanesljivo informacijo o morebitnih stabilnostnih težavah EES, ki lahko pripeljejo do razpada le-tega. Sistem WAMS bo omogočili nove adaptivne zaščite (WAMPAC – Wide Area Monitoring, Protection and Control) ter posodobljene avtomatizirane sheme zaščite sistema (SIPSs – System Integrity Protection Schemes).

Potreben bo prenos ogromnih količin podatkov (predvsem sinhroniziranih meritev) v realnem času, ki je v primeru WAMS 20 ms! To je tudi resulucija shranjevanja podatkov v bazo, ki bi naj bila na voljo vsaj za nekaj dni. Na primer, če imamo v omrežju 1000 PMU enot, je ocenjen tok podatkov, ki jih moramo zapisovati v bazo, cca. 100 Mbps [2].

B. *Distribucijsko omrežje*

Vključevanje razpršenih virov v distribucijsko omrežje prinaša številne težave, ustaljenim in preizkušenim sistemom avtomatizacije distribucijskega omrežja pa nove izzive. Med drugim bo aktualna naslednja tematika:

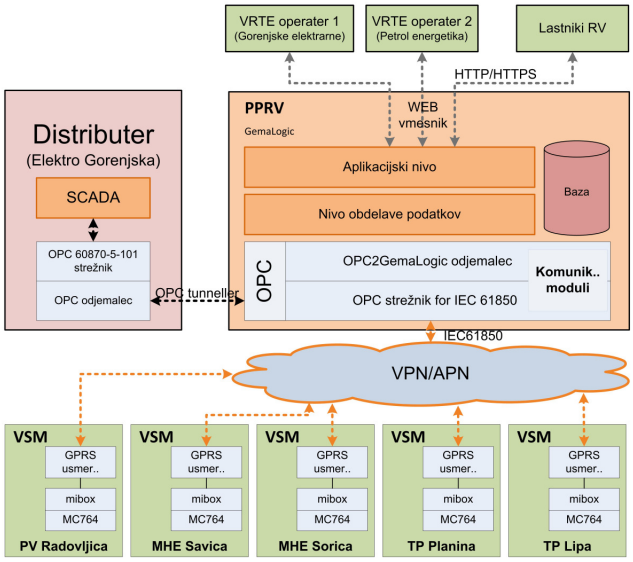
– obvladovanje pretokov in termičnih obremenitev vodov,
– vpliv razpršenih virov na kakovost napetosti:
  – vzdrževanje napetostnega profila vdolž voda;
  – problem napetostnih nihanjih, ki jih nekatere vrste razpršenih virov vnašajo v omrežje ter
  – napetostne nesimetrije;
– vpliv razpršenih virov na zanesljivost ter stabilnost obratovanja sistema, ki na današnji stopnji razvoja ni zagotovljena (večina razpršenih virov ima naključni karakter),
– novi principi zaščit,
– možnost otočnega obratovanja ob izpadih omrežja in pomoč pri restavraciji napajanja po izpadih.

Za reševanje zgoraj naštetih težav prinašajo pametna omrežja predvsem še več meritev: obratovalne meritve in meritve kakovosti napetosti bodo v določenem obsegu nujne tudi na NN omrežju. V prvi fazi bodo meritve potrebne v transformatorskih postajah in na stičnih mestih priključevanja razpršenih virov v omrežje. Pri tem ni nujno, da bodo vse meritve prišle preko sistema avtomatizacije, torej preko procesnega sistema distribucije. Izvor podatkov bo tudi v drugih sistemih, kot je na primer virtualna elektrarna, ter v nekaterih primerih tudi sistem naprednega merjenja AMI. Nadaljnje faze bodo boleg merjenja omogočale tudi določene funkcije avtomatizacije, kot na primer nastavljanje transformatorskih stopenj distribucijskih transformatorjev glede na meritve napetosti vzdolž izvoda, regulacijo jalove energije, ipd.

Nadzor in vodenje razpršenih virov pa ni smiselno le zaradi sistemskih storitev, temveč je lahko vezano tudi na tržne storitve. Ko vire opremimo z ustrezno procesno opremo, jih lahko daljinsko povežemo v sistem virtualne elektrarne ter agregiramo energijo vseh virov ter s tem skupnim portfeljem nastopimo na trgu z energijo.

Kot del opreme za priključevanje razpršenjih virov na omrežje se uveljavlja vmesnik stičnega mesta (VSM, ang. PCCI – Point of Common Coupling Interface), ki omogoča daljinsko vodenje – informacijsko povezavo s centrom vodenja virtualne elektrarne ali drugim nadzornim sistemom in s tem:
– zajem in posredovanje meritev (obratovalne meritve in meritve kakovosti napetosti),
– posredovanje komand in nastavitev,
– posredovanje alarmov,
– druge funkcije (zaščitne ipd.),
– možnost lokalnega obratovanja vira:
  – karakteristika jalove energije glede na lokalne meritve napetosti,
  – izvedbe zaščitnih funkcij.

Prototip VSM in programske opreme virtualne elektrarne (PPRV) je bil izdelan in preizkušen v okviru projekta »Inteligentna elektroenergetska platforma za nadzor in vodenje razpršenih virov in porabnikov – SUPERMEN« (slika 2) [3].



Slika 2: Pilotni projekt SUPERMEN

C. *Napredna merilna infrastruktura - AMI*

AMI sistemi so namenjeni predvsem za merjenje in upravljanje porabe gospodinjstev in poslovnih odjemalcev na široki potrošnji. Ti sistemi prvič informatizirajo do sedaj skoraj povsem neinformatizirano NN omrežje in vzpostavljajo dvosmerno komunikacijo s končnimi odjemalci.

Od sistema AMI pričakujemo predvsem posodobitev obstoječega sistema merjenja za namen obračunskih meritev v smislu informatizacije vseh procesov – od avtomatskega odčitavanja do priprave podatkov za obračun po dejanski mesečni porabi, podporo naprednim tarifnim sistemom in drugim funkcijam, ki bodo omogočala izvajanje ukrepov upravljanja s porabo, možnost izrabe infrastrukture za odčitavanje porabe drugih energentov in vode, podporo tehničnim procesom, kot so spremljanje pretokov, merjenje izgub in detekcija kraj in goljufij ter spremljanje nekaterih parametrov kakovosti (izpadi, upadi napetosti).

Direktiva [4] nalaga državam članicam, da do leta 2020 uvedejo sistem naprednega merjenja za vsaj 80 % odjemalcev, za katere ekonomska analiza kaže pozitivne rezultate. Zaradi te direktive in relativno kratkega roka (do leta 2020), se moramo lotiti uvedbe sistema AMI z opremo, ki je danes na voljo.

Problem zadnjega kilometra – torej povezave do končnega uporabnika – je trenutno cenovno in organizacijsko najugodneje rešiti z uporabo PLC/DLC tehnologije, vsaj za področja, kjer je na transformatorsko postajo priključenih več kot 5 odjemalcev (v Sloveniji je to 95 % vseh odjemalcev). Za povezavo med koncentratorji in merilnim centrom

lahko uporabimo omrežja mobilnih operaterjev (npr. GPRS) ter še Ethernet in brezžična omrežja, kjer je to mogoče (predvsem v transformatorskih postajah).

Tehnologiji PLC in GPRS imata velike omejitve glede pasovne širine in sistemskih zmogljivosti. Bistveno pa je, da izbrana tehnologija zadostuje za izvajanje zahtevanih funkcij, ki ekonomsko upravičijo naložbo v sistem AMI.

Ker sistem AMI ne bo deloval v realnem času (zahteva se najmanj dnevni prenos 15-minutnih obremenilnih diagramov), predstavlja za IKT izziv le iz vidika obvladovanja velikega števila naprav (v Sloveniji je cca. 900.000 merilnih mest) in količine podatkov, ki se bodo nabirali v bazah merilnih centrov.

D. Upravljanje s porabo (DSM/DR)

Upravljanje s porabo je eden izmed ključnih inštrumentov za izvajanje ukrepov učinkovite rabe električne energije. Kratkoročno upravljanje s porabo (pogosto imenovano tudi DR – Demand Response), je namenjeno kratkoročnim spremembam v porabi odjemalcev, katerega glavni namen je premikanje porabe znotraj dnevnega diagrama v čas, ko to izvajalcu upravljanja s porabo najbolj koristi. S kratkoročnimi programi upravljanja s porabo podjetja, bodisi operaterji omrežja bodisi trgovci z električno energijo, odjemalcem ponudijo vzpodbude za zmanjšanje njihove porabe v času konične obremenitve elektroenergetskega omrežja ali v času izredno visokih cen na trgu z električmno energijo.

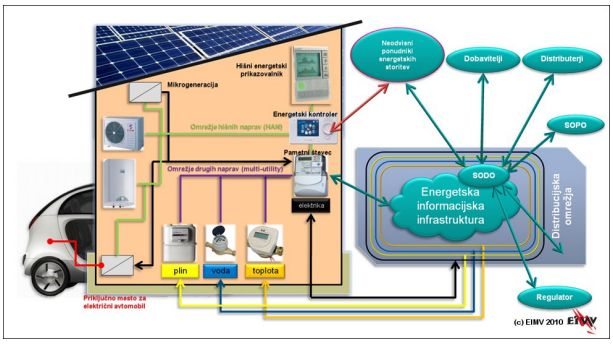
Izvedba ukrepov upravljanja s porabo je lahko:

– s posredovanjem uporabnika, ko določene naprave sam izključi ali ne vključi in
– avtomatska.

Za učinkovito izvajanje ukrepov DSM/DR je nujen sistem AMI.

E. Pametni dom

Avtomatsko upravljanje z napravami v smislu prilagajanja odjema in optimiranja stroškov za energijo glede na želeno ugodje zahteva ustrezno IKT infrastrukturo v hiši. Z razvojem koncepta pametnih hiš oziroma pametnega doma (SmartHome) se naprave v hiši tudi informacijsko povezujejo – običajno govorimo o omrežju hišnih naprav oziroma hišnih omrežjih (HAN – Home Area Network), ali v primeru večjih stavb, o BAN (Building Area Network).



Slika 3: Koncept povezave pametnega doma s pametnim omrežjem

Stična točka med pametnim omrežjem oziroma njegovim podsistemom AMI in hišnim omrežjem – HAN, je lahko pametni števec (slika 3). Le-ta lahko poleg informacijskih povezav z merilnim centrom elektrodistribucijskega podjetja omogoča še povezave z omrežjem hišnih naprav (HAN), kot tudi z merilniki drugih energentov in vode, kar pomeni, da lahko učinkovito rabo energije razširimo tudi na druge energente.

Poleg povezave s pametnim števcem je predvidena še povezava hišnega omrežja oziroma njegovega strežnika preko interneta s ponudnikom naprednih energetskih storitev (npr. storitvenim centrom za upravljanje s porabo), preko katerega bo tudi mogoče izvajati ukrepe upravljanja s porabo in končnim uporabnikom nuditi nove inovativne energetske storitve.

V nekaterih državah (npr. v Nemčiji) se zavzemajo za koncept posebnega komunikacijskega kontrolerja (MUC – Multi Utility Communication Controller) na katerega se priključijo vsi števci enakopravno. Električni števec v tem primeru nima več vloge komunikacijskega prehoda. Storitve odčitavanja lahko v tem primeru opravljajo operaterji TK omrežij ali pa podjetja, ustanovljena posebej za ta namen.

F. E-mobilnost

Električni avtomobil je lahko dosti več kot le porabnik električne energije – parkirane električne avtomobile lahko uporabimo tudi kot hranilnike energije, seveda, ob dovolj velikem številu in ob ustrezni infrastrukturi (V2G – Vehicle-to-Grid). Lastnik avtomobila si bo izbral najprimernejši tržni paket oskrbe glede na njegove potrebe. Določeni paketi oskrbe bodo vključevali sodelovanje avtomobila, oziroma njegovih električnih akumulatorjev, v sistemskih storitvah, kar pomeni, da bo na primer v času, ko bo avtomobil parkiran, dovoljeno izprazniti akumulatorje za vnaprej določen odstotek ali pa prekiniti polnjenje. Polnilna mesta bodo morala biti zato primerno opremljena – ne le z ustreznim priključkom na električno omrežje, temveč tudi s priključkom na informacijsko infrastrukturo, ki bo

upravljalcu omogočala v realnem času prenos informacij o tem, koliko energije je v danem avtomobilu na voljo in za koliko časa. Seveda bo sodelovanje avtomobila pri sistemskih storitvah ustrezno finančno nagrajeno, kar pomeni, da bo paket oskrbe ugodnejši.

V. ZAKLJUČEK

Pametna omrežja prinašajo številne nove tehnologije, ki temeljijo na sodobnih informacijsko komunikacijskih tehnologijah. Z vidika le-teh se je treba zavedati, da bomo imeli opravka z velikim številom razpršenih inteligentnih naprav, ki zahtevajo povezljivost. Zahteve za te t.i. M2M (Machine-to-machine) komunikacije so večinoma zelo visoke, predvsem v smislu zanesljivosti, nizkih stresanj in zakasnitev, ki morajo omogočati prenos podatkov v realnem času tudi pod 20 ms. IK tehnologije za potrebe pametnih omrežij bodo morale obladovati velike količine podatkov ter zagotavljati najboljši možen nivo informacijske varnosti, ob vseh pestrostih omrežij, ki bodo v uporabi (od hišnih, prek omrežij sosesk, povezovalnih, do jedrnih omrežij).

Od konceptov pametnih omrežij pričakujemo predvsem rešitve, ki bodo obstoječo elektroenergetsko infrastrukturo izkoristile stroškovno optimalno.

LITERATURA

[1] Vizija razvoja koncepta SmartGrids v Sloveniji, Elektroinštitut Milan Vidmar, študija št.: 2026. Ljubljana, 2010.

[2] Young-Jin Kim, Marina Thottan, Vladimir Kolesnikov, Wonsuck Lee. A Secure Decentralized Data-centric Information Infrastructure for Smart Grid. IEEE Communications Magazin, November 2010.

[3] http://www.projekt-supermen.si [16.4.2010].

[4] DIREKTIVA 2009/72/ES EVROPSKEGA PARLAMENTA IN SVETA o skupnih pravilih notranjega trga z električno energijo, julij 2009.

Andrej Souvent je diplomiral leta 1999 na Fakulteti za elektrotehniko Univerze v Ljubljani. Po diplomi je delal v industriji na področju procesne informatike in avtomatizacije procesov. Od leta 2007 je zaposlen kot svetovalec na Elektroinštitutu Milan Vidmar. Področje njegovega dela so sistemi nadzora in vodenja EES, sistemi AMI in druga področja pametnih omrežij.

Tomaž Pfajfar je diplomiral leta 2004 in doktoriral leta 2009 na Fakulteti za elektrotehniko Univerze v Ljubljani. Trenutno je zaposlen kot vodja raziskav in razvoja v podjetju 2e d.o.o., ki je odcepljeno podjetje Univerze v Ljubljani. Njegovo raziskovalno delo obsega področje kakovosti električne energije, razpršenih virov in aktivnih distribucijskih omrežij.

Igor Papič je diplomiral leta 1992, magistriral leta 1995 in doktoriral leta 1998 na Fakulteti za elektrotehniko Univerze v Ljubljani. Od leta 2009 je redni profesor na Fakulteti za elektrotehniko v Ljubljani. Njegova raziskovalna dejavnost vključuje aktivne kompenzatorje, naprave FACTS, kakovost električne energije in vključevanje razpršenih virov v omrežje.

Uporaba prilagajanja odjema in razpršene proizvodnje električne energije

dr. Gregor Černe, dr. Zoran Marinšek, Mitja Bizjak, u. d. i. s., vsi INEA d. o. o. Ljubljana

Povzetek — Prispevek skozi dva razvojna projekta – Kibernet in Mirabel – osvetljuje različna vprašanja in probleme pri uporabi prilagajanja odjema in razpršene proizvodnje za uravnavanje stabilnosti elektroenergetskega omrežja. Opisani sta izvirni rešitvi algoritma avtomatskega uravnavanja odjema in komunikacije s končnimi odjemalci. Poleg tehničnih rešitev so v prispevku nakazani tudi problemi in možne rešitve pri umeščanju sistema pri potencialnih uporabnikih in ekonomski upravičenosti njegove uporabe. Poseben in nezanemarljiv problem je tudi sociološko vprašanje – sprejemljivost sistema pri končnih udeležencih.

Ključne besede — aktivna omrežja, pametna omrežja, upravljanje z odjemom in razpršeno proizvodnjo, navidezna elektrarna

Abstract — The two smart grid development projects – Kibernet and Mirabel – are used to expose the problems and unresolved issues of the demand side management (DSM) usage from several aspects. The article describes two different approaches of automatic controlling of the demand and consumer communication. Beside the technical solution, the article exposes the problems at defining the user of the DSM system in the EE scheme and its economic justification. Separate and significant problems are also the social problems of accepting the system by the end consumers.

Keywords — smart grid, demand side management, virtual power plant

I. UVOD

Prilagajanje odjema in razpršene proizvodnje (s tujko Demand Side Management – DSM) je eden bistvenih elementov t. i. aktivnih omrežij (»smart grid«), katerih namen je aktivno vodenje tako omrežnih komponent kot tudi komponent porabnika ozioma proizvajalca električne energije.

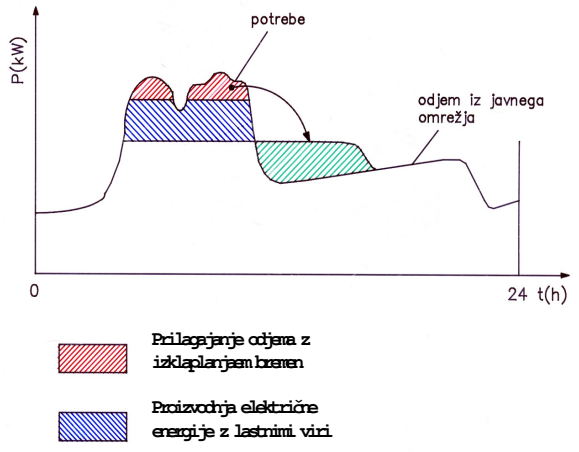
Aktivno omrežje in prilagajanje odjema sta začela pridobivati na veljavi v želji po doseganju evropskega cilja 20 % obnovljivih virov energije (OVE) do leta 2020 in njihovim intenzivnim vključevanjem v obstoječe elektroenergetsko omrežje. Prednost OVE je predvsem okoljska sprejemljivost, medtem ko je slaba lastnost nepredvidljivost proizvodnje električne energije. Zaradi nepredvidljivosti naravnih danosti proizvodnjo obnovljivih virov lahko samo napovedujemo, ne pa tudi planiramo kar povzroča upravljavcem omrežij težave pri izdelavi dnevnih voznih redov in nestabilnosti pri obratovanju EES.

Zahteve po povečanju deleža proizvodnje energije iz obnovljivih virov, zahteve po spodbujanju učinkovite rabe energije, ekonomika in nove tehnologije, ki prihajajo (npr. električni avtomobili, gorivne celice, prilagajanje odjema) prinašajo potrebo uvajanju upravljanja z odjemom in razpršeno proizvodnjo, saj brez tega ni mogoča njihova učinkovita integracija in zagotavljanje varnost ter zanesljivost elektro energetskega sistema.

II. BREMENA ZA PRILAGAJANJE ODJEMA IN RAZPRŠENE PROIZVODNJE

Prilagajanje odjema in razpršene proizvodnje se izvaja s konkretnimi bremeni v gospodinjstvih poslovnih zgradbah in industriji. Vsem bremenom je skupno, da morajo shranjevati električno energijo – bodisi v obliki materiala (v industriji), v obliki toplote (hladilnice, peči) ali na kakšen drug način.

Pri razpršeni proizvodnji so za prilagajanje primerne predvsem razne kogeneracije, plinske turbine, dizel generatorji ipd. Slika 1 prikazuje primer odjema pri odjemalcu brez prilagajanja odjema in s prilagajanjem odjema ter z aktivacijo notranjih virov.



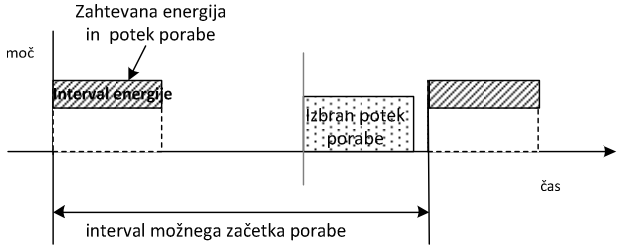
Slika 1: Primer prilagajanje odjema z izklapljanjem bremen in uporabo lastnih virov [7]

S povezovanjem odjemalcev, ki razpolagajo z bremeni za prilagajanje in razpršeno proizvodnjo, se lahko oblikuje virtualna elektrarna. Le ta lahko poveča

ali zmanjša trenutno proizvodnjo oziroma odjem električne energije.

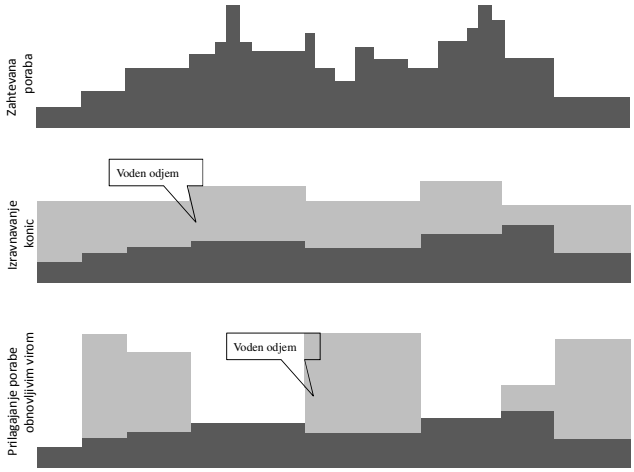
III. PROJEKT MIRABEL

Glavni cilj [8] je razvoj koncepta in IT infrastrukture, ki omogoča elektro energetskim podjetjem učinkovito upravljanje z obnovljivimi viri in uravnavanje porabe s proizvodnjo.



Slika 2: Oblika mikro-zahteve za prilagajanje in njena realizacija

Bistvena ideja projekta je, da končni uporabniki omrežja (proizvajalci in odjemalci) ponudijo v upravljanje svoj odjem in proizvodnjo za prilagajanje v obliki t.i. »mikro-zahtev«. Mikro-zahteva vsebuje parametre za zahtevani odjem energije in variabilnost teh parametrov. Tako vsebuje območje količine energije porabe (ali proizvodnje), časovni interval začetka porabe energije, časovni potek porabe energije, ceno … V enostavnem primeru tako končni odjemalec za del svojega odjema (ena naprava) v »mikro-zahtevi« določi zanj sprejemljivi časovni interval, ko mora biti zahtevana energija dostavljena (Slika 2).



Slika 3: Nereguliran odjem (zgoraj), zniževanje konice (sredina), prilagajanje glede na proizvodnjo OVE (spodaj)

Na drugi strani sistem Mirabel nameščen pri elektro energetskem podjetju zbira zahteve o možni porabi in proizvodnji množice končnih uporabnikov ter na podlagi ekonomskega kriterija določi optimalno razporeditev pretokov energije. Z vsemi odjemalci, ki so oddali »mikro-zahteve«, se sklene pogodba, ki točno določa parametre o dostavi zahtevane energije.

Primera prilagajanja odjema prikazuje Slika 3, kjer je zgoraj zahtevani odjem odjemalcev brez prilagajanja, v sredini prilagajanje odjema s ciljem zmanjšanje konične porabe in spodaj prilagajanje odjema glede na proizvodnjo obnovljivih virov.

Sistem Mirabel vsebuje tri pomembnejše elemente:

– Zbiranje in združevanje »mikro-zahtev« – algoritem združevanja podobnih zahtev naredi algoritem razporejanja bolj učinkovit
– Napovedovanje – napovedovanje proizvodnje obnovljivih virov in porabe odjemalcev
– Razporejanje pretokov energije za proizvodnjo in porabo – na podlagi omejitev v mikro zahtevah algoritem optimalno razporedi proizvodnjo in porabo.

Algoritmi zbiranja, napovedovanja in razporejanja, se izvajajo v realnem času.

S pomočjo tega koncepta je možna učinkovitejša integracija obnovljivih virov kot tudi zmanjšanje stroškov iz naslova nižanje konična porabe oziroma preusmerjanja porabe na čas, ko je cena energije nižja.

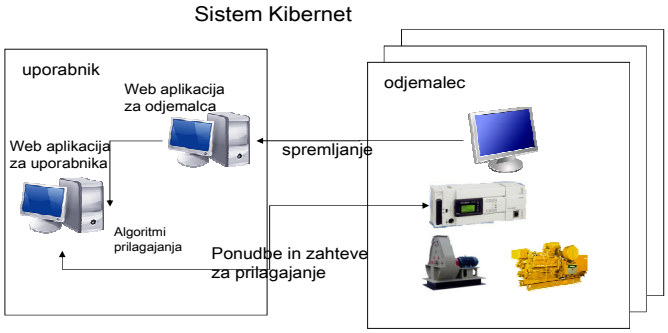
Sistem uvaja tudi nove poslovne odnose med odjemalce/proizvajalce na eni strani in podjetja za dobavo električne energije na drugi. Dosedanje odprte pogodbe, ko odjemalci plačajo energijo porabljeno v preteklosti, se dopolnijo z zaprtimi pogodbami, ki jih odjemalec sklene za del svojega odjema in se obveže o porabi svojega odjema v prihodnosti.

Skladnost dejanskega odjema s pogodbami se zagotavlja z neposrednim nadzorom nad bremenom. Kakršnakoli odstopanja se ne kaznujejo temveč se obračunavajo po ceni odprte pogodbe, ki je višja od pogodbene cene v zaprti pogodbi.

IV. PROJEKT KIBERNET

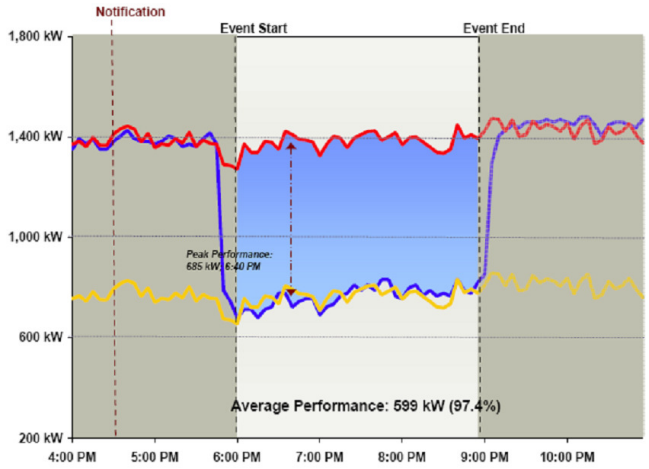
Sistem Kibernet, ki je bil razvit v okviru istoimenskega projekta [7], omogoča prilagajanje odjema industrijskih odjemalcev in razpršenih virov električne energije. V okviru projekta so sodelovali tudi dejanski odjemalci (Koto, Livar, Papirnica Vevče in Količevo), katerih odjem je sistem Kibernet prilagajal.

Sistem Kibernet se sestoji iz dveh delov (Slika 4) in sicer, merilno krmilnega sistema pri odjemalcu in storitvenega centra pri uporabniku.



Slika 4: Arhitektura sistema Kibernet

Sistem spremlja odjem odjemalcev električne energije in razpršenih virov in od njih pridobiva ponudbe za prilagoditev njihovega odjema. Ponudba obsega podatke o možni spremembi odjema (Slika 5, rumena črta) in tudi ceno povračila odjemalcu, v kolikor pride do intervencije.



Slika 5: Izvedba prilagajanja: rdeče – predvideni odjem, modro – dejanski odjem, rumeno – ponujeni odjem

Storitveni center nato na zahtevo uporabnika izvede izbor najustreznejših odjemalcev in razpršenih virov, ki sodelujejo pri prilagajanju odjema. Po izboru optimalnega nabora odjemalcev in razpršenih virov dobijo le ti vozni red svojega odjema. Procesni del sistema Kibernet, ki je vgrajen pri odjemalcih in razpršenih virih poskrbi za izvedbo prilagajanja odjema. Aktivacija sistema Kibernet je znotraj ene (1) minute. Postopek je povsem avtomatiziran in ne potrebuje človeškega posredovanja. Skladnost dejanskega odjema s ponudbami se ugotavlja iz meritev in sicer se izračuna razlika med dejanskim odjemom (modra črta) in predvidenim odjemom (rdeča črta). Sistem omogoča tako povečanje kot tudi zmanjševanje odjema. V okviru pilotne postavitve sistem z izbranimi odjemalci s skupno priključno močjo 30 MW omogoča do 5MW kapacitete prilagajanja za trajanje vsaj 1 ure.

V. CILJNI UPORABNIKI SISTEMA ZA PRILAGAJANJE

V primeru Mirabel je za uporabo prilagajanja odjema in razpršene proizvodnje ključni igralec elektro energetskega trga tisti, ki ima vlogo odgovornega bilančne skupine. Ta vloga omogoča nastopanje na organiziranem trgu in dovoljuje sklepanje zaprtih pogodb z odjemalci in proizvajalci [3]. S pomočjo sistema za prilagajanje odgovorni bilančne skupine lažje vključuje nepredvidljive obnovljive vire in manjša odstopanja od voznega reda.

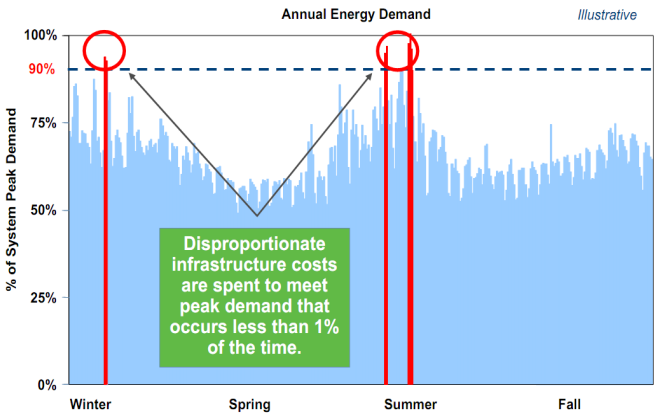
Uporabnik sistema za prilagajanje je lahko tudi sistemski operater prenosnega omrežja, ki sistem uporablja kot nadomestilo za terciarno rezervo ali celo sekundarno rezervo pri uravnavanju omrežja. Ker sistemski operater po svoji vlogi ne more sklepati pogodb o dobavi energije s končnimi odjemalci, lahko postane uporabnik le preko odgovornega bilančne skupine. To lahko stori s pogodbo (npr. najem sistemske storitve) ali pa preko izravnalnega trga.

Podobno kot pri sistemu Mirabel lahko tudi sistem Kibernet uporabljata odgovorni bilančne skupine in sistemski operater prenosnega omrežja.

Uporabnik sistema Kibernet pa lahko postane tudi operater distribucijskega omrežja. Uporablja ga lahko tako za uravnavanje pretokov energije na distribucijskem omrežju kot tudi za nudenje sistemske storitve operaterju prenosnega omrežja. Vendar takšna uporaba še ni najbolje zakonodajno podprta. Operater distribucijskega omrežja ima namreč priključene odjemalce več bilančnih skupin in pri izvajanju prilagajanja odjema lahko povzroči dodatna odstopanja od njihovih voznih redov ter dodatne stroške.

VI. EKONOMSKI POTENCIALI

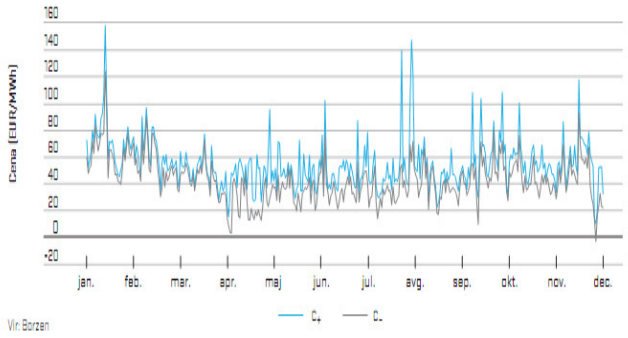
Gledano v celoti ima prilagajanje odjema in razpršene proizvodnje velik ekonomski potencial. Analiza iz tujine [4] zatrjuje, da nezanemarljiv del proizvodnje električne energije deluje zelo omejen čas.



Slika 6: Normirana konica odjema električne energije prenosnega omrežja (vir [4])

Slika 6 prikazuje normirano konično porabo električne energije za obdobje enega leta. Iz nje je razvidno da 10 % instaliranih kapacitet proizvodnje deluje manj kot 1 % možnega obratovalnega časa in je namenjeno samo za pokrivanje maksimalnih kapacitet. Ob uporabi prilagajanja odjema in razpršene provizvodnje bi rabili ustrezo manjšo količino novozgrajenih proizvodnjih kapacitet in ostale infrastrukture elektro energetskega omrežja.

Odgovorni bilančne skupine uporabo sistema lahko opravičuje z zmanjšanjem odstopanj dejanskega odjema od napovedanega voznega reda. V primeru odstopanj mora odgtovorni bilančne skupine plačati kazenske penale, ki so vezani na ceno električne energije v času odstopanj.



Slika 7: Ceni odstopanj za bilančne skupine [5]

Iz diagrama (Slika 7), je razvidno da preseganje trikratnika cene povprečne električne energije ni posebna redkost. Pri uporabi sistema za prilagajanje lahko odgovorni bilančne skupine ta strošek zmanjša.

Skupna cena (zakup in predvidena uporaba) terciarne rezerve v Sloveniji [6] za leto 2011 predvideva okoli 13.000,000 EUR stroškov oziroma okoli 600 EUR stroškov na uporabljeno MWh. Z uporabo prilagajanja odjema se lahko ta strošek zmanjša.

VII. Sprejemanje sistema pri končnih odjemalcih

V okviru projekta Mirabel je bila opravljena raziskava [2] o sprejemljivosti prilagajanja odjema v samih gospodinjstvih, ki je dala naslednje rezultate:

– svoje sodelovanje pri prilagajanju odjemalci povezujejo bolj s finančnimi učinki kot z ekološkimi
– za novosti je mnogo bolj dovzetna mlajša populacija kot starejša
– večina si ne zna predstavljati učinkov sistema na njihov vsakdanjik

Tabela 1: Pričakovano znižanje cene električne energije za prilagajanje za gospodinjstva [2]

determination of energy consumption in advance / saving costs in percent	nothing	1-5%	6-15%	16-30%	>30%
1-2 days	11%	1%	14%	40%	29%
6-24 hours	12%	7%	37%	33%	5%
6 hours or less	12%	29%	45%	5%	3%
1 hour at most	32%	42%	18%	1%	1%

V tujini, kjer uporabljajo sisteme za prilagajanje, uspejo pridobiti tako gospodinjstva kot tudi industrijske odjemalce za ceno od 30 EUR/kW ponujene kapacitete prilagajanja na leto, ob predpostavki, da se bo ponudba uporabila okoli trideset krat letno.

VIII. Zaključek

Prilagajanje odjema in razpršene proizvodnje se v Sloveniji izvaja in uporablja na nivoju razvojnih projektov. Projekt Kibernet je pokazal, da je prilagajanje tehnično izvedljivo in da pri uporabnikih obstaja tehnični potencial. Rezultat projekta Mirabel bo nakazal tudi potencial prilagajanja za obvladovanje OVE. Pri dejanski uporabi prilagajanja so še določeni zakonodajni problemi in problemi pri motivaciji odjemalcev. Prvi se odpravljajo s splošnim trendom razvoja elektro energetike, kar je tudi zabeleženo v strateških dokumentih [9], slednje pa je potrebno odpravljati z ugotavljanjem ustreznih ekonomskih potencialov, za katere se pričakuje, da se bodo z vztrajanjem pri obnovljivih virih in izhodom gospodarstva iz krize, še povečevali.

Zahvale

Za nastanek tega dela gre zahvala sodelujočim partnerjem in institucijam na projektih in sicer na projektu Mirabel, ki je sofinanciran v okviru 7OP, so SAP (koordinator projekta), Technishe Universitaet Dresen (TUD), Netherlands Organisation for Applied Scientific Research (TNO), Aalborg Universitet Danmark(AAU), Institut Jožef Stefan (IJS), Centre for Renewable Energy Sources Greece (CRES) in Energie Baden-Württemberg AG (EnBW) ter na projektu Kibernet, ki je sofinanciran iz strukturnih skladov, so IJS, Elektro Institut Milan Vidmar, Fakulteta za Elektrotehniko, Koto, Livar in papirnici Vevče in Količevo.

Literatura

[1] T. Pfajfar, I. Papič, B. Bletterie, H. Brunner, Aktivna distribucijska omrežja z razpršeno proizvofnjo, 8. Konferenca slovenskih elektroenergetikov, Čatež 2007.
[2] Johannes Lischka, Katharina Löwenstein, René Müller, Technishe Ubiversitaet Dresden, Miracle project user study, 2010.
[3] ETSO, The Harmonized Electricity Market Role model
[4] Enernoc, D R Initiatives for Public Power Utilities, 2009.
[5] JARSE, Poročilo na področju energetike v Sloveniji v letu 2009.

[6] ELES, Rezultati javne dražbe za nakup rezerve delovne moči za terciarno regulacijo frekvence za leto 2011
[7] INEA, Analiza potreb in idejne specifikacije, PI 1.1.1. projekta Kibernet, 2009.
[8] SAP, INEA, IJS, TUD, TNO, AAU, CRES, EnBW, Mirabel – Descritpion of Work, FP7-ICT-Energy-2009-1, 2009.
[9] Vlada Republike Slovenije, Nacionalni akcijski načrt za energetsko učinkovitost za obdobje 2008-20016, 2008.

dr. Gregor Černe je diplomiral iz fizike na Fakulteti za Matematiko in fiziko, ter nato doktoriral na IJS na Odseku za jedrsko tehniko. V podjetju Inea je od leta 2008 kot vodja projektov zaposlen v poslovni enoti za energetiko, kjer dela na aktivnih omrežjih, vodenju elektroenergetskih sistemov in sistemov za meritve ter nadzor energentov.

Infrastruktura za implementacijo pametnih omrežij – Zaključki projekta SUPERMEN

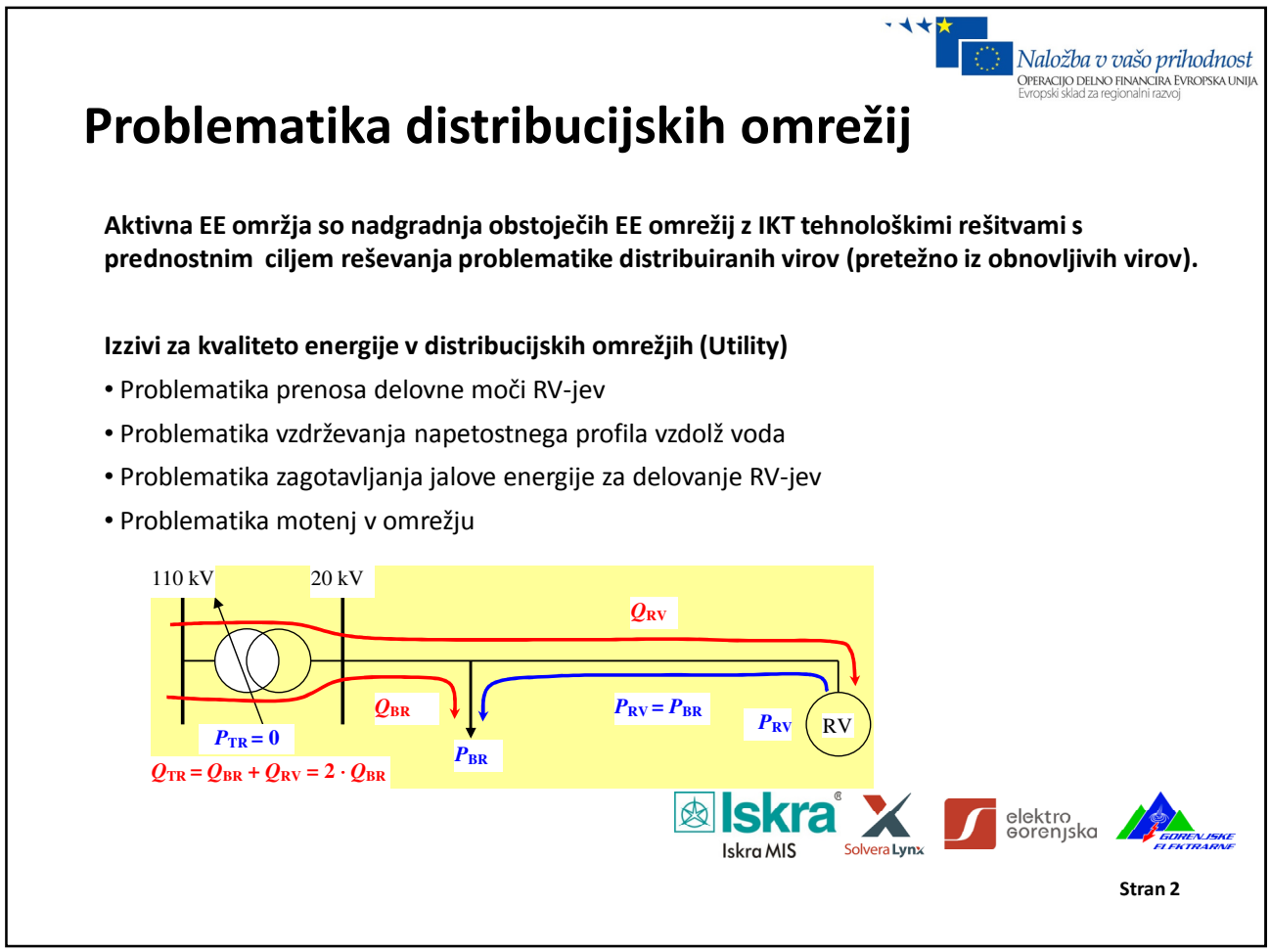
Janez Šmid, Iskra MIS, Kranj

Povzetek — Glavni cilji projekta SUPERMEN so bili analiza, razvoj in demonstracija koncepta infrastrukture »Pametnih omrežij. V projektu so bile demonstrirane osnovne aplikacije nadzora in upravljanja razpršenih virov in aplikacije upravljanja energije. Demonstrirana infrastruktura je osnova za razvoj novih storitev in aplikacij, ki bodo podpora novim poslovnim modelom v proizvodnji in trženju električne energije. Celotni strošek projekta je bil 2.080.000 EUR, od tega sta EU in Slovenija prispevala 777.430 EUR. Vse ostale stroške so krili industrijski partnerji na projektu.

Ključne besede — pametna omrežja, vmesnik stičnega mesta, povezovalno programje, distribucijska omrežja, IEC61850, razpršeni viri, center vodenja, virtualna elektrarna, upravljanje s porabo

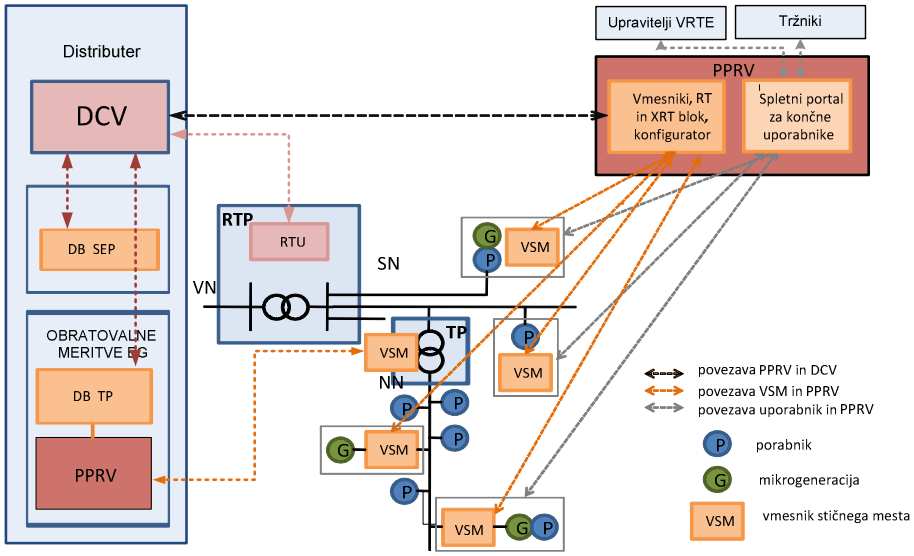
Abstract — Main objectives of project SUPERMEN were study, development and demonstration of "Smart Grids" infrastructure. Project demonstrates some basic application for supervision and control of distributed resources and energy management applications. The infrastructure is a base for further development of new services and application supporting new business models. Overall budget of the project was 2.080.000 EUR, where EU and Slovenian Government cover 777.430 EUR. All other expenses were covered by industrial partners on the project.

Keywords — Smart Grids, Point of common coupling interface, Middleware, Distribution networks, IEC61850, Distributed generation, Distribution control centre, Virtual power plant, Demand side management



Naložba v vašo prihodnost
OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski sklad za regionalni razvoj

Koncept SUPERMEN

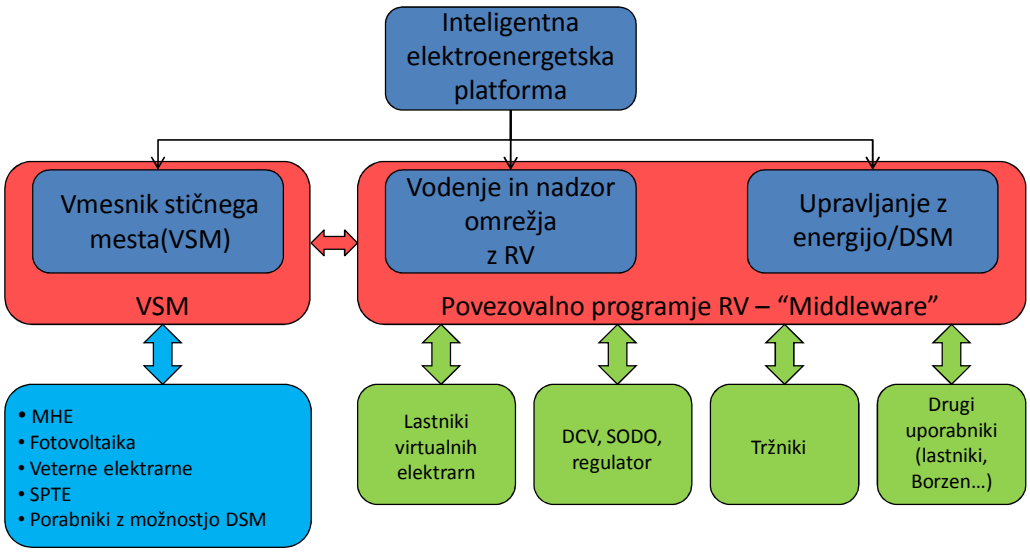


Iskra MIS Solvera Lynx elektro gorenjska GORENJSKE ELEKTRARNE

Stran 3

Naložba v vašo prihodnost
OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski sklad za regionalni razvoj

Vodenje razpršenih virov in porabnikov

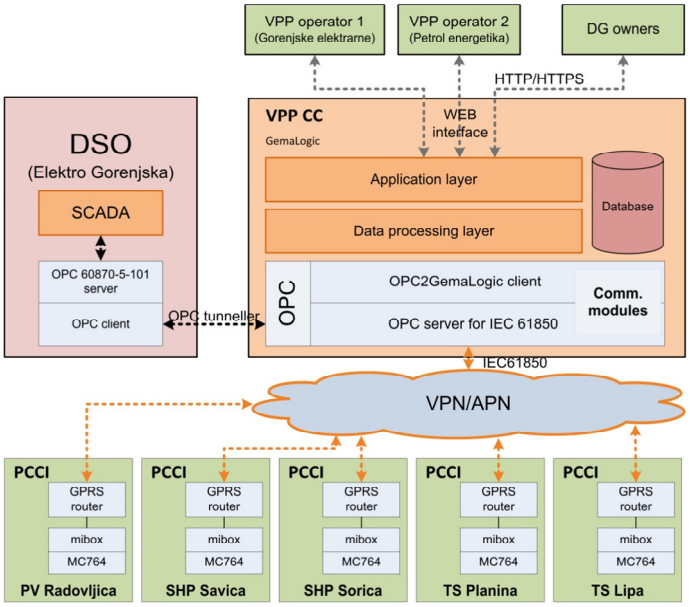


Iskra MIS Solvera Lynx elektro gorenjska GORENJSKE ELEKTRARNE

Stran 4

Naložba v vašo prihodnost
OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski sklad za regionalni razvoj

Demonstracijski primer

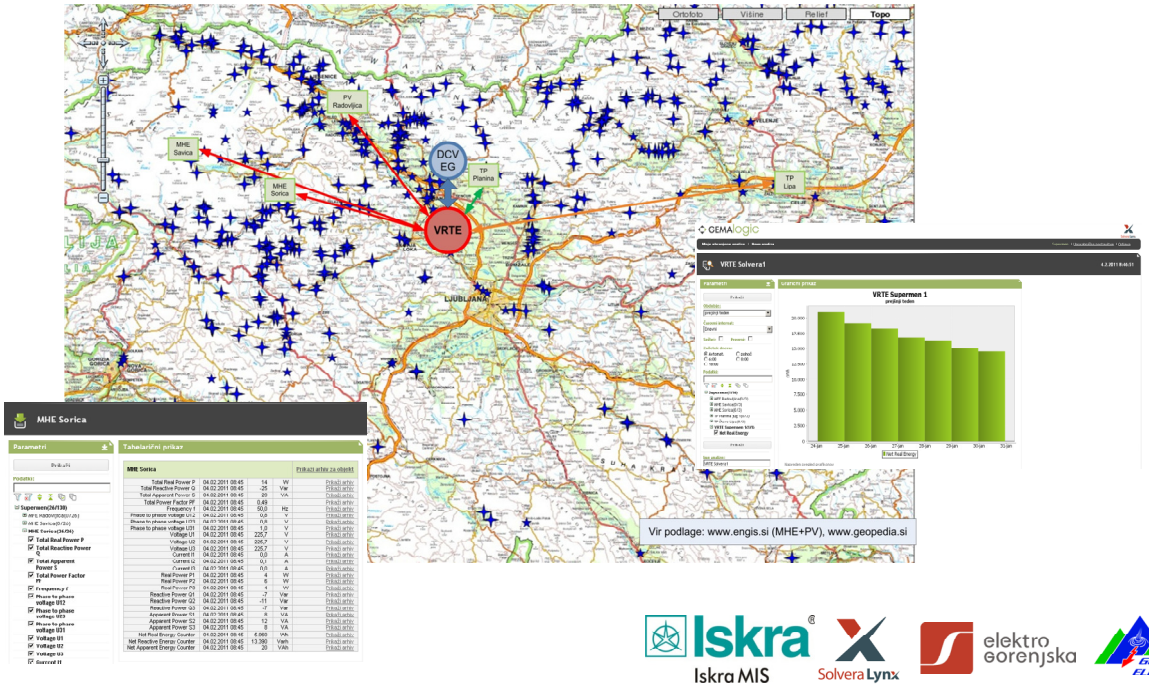


Iskra MIS Solvera Lynx elektro gorenjska GORENJSKE ELEKTRARNE

Stran 5

Naložba v vašo prihodnost
OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski sklad za regionalni razvoj

VRTE Supermen



Iskra MIS Solvera Lynx elektro gorenjska GORENJSKE ELEKTRARNE

Stran 6

Naložba v vašo prihodnost
OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski sklad za regionalni razvoj

Vmesnik stičnega mesta

"VSM je merilni center (pretvornik) z okolico za nadzor in kontrolo priključnih točk omrežja"

MERJENJE PROIZVEDENE / PORABLJENE ENERGIJE
- (4 neodvisni števci za merjenje energije)

MERJENJE KVALITETE NAPETOSTI
- (spremljanje kazalcev kvalitete po SIST EN 50160)

ZAŠČITNE FUNKCIJE
- (<>U, <>f, >I, LoM; glede na SONDO in SIST EN 50438)

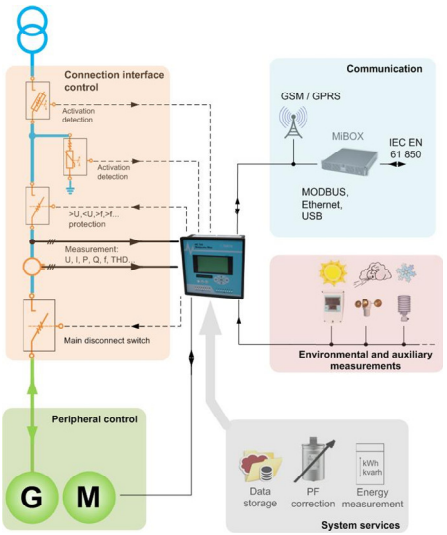
ODKLOPNO STIKALO ZA LOČITEV OD OMREŽJA
- (glavno stikalo s preklopko za onemogočenje ločilnega mesta)

MERJENJE PARAMETROV 3f OMREŽJA
- (U, I, P, Q, f, THD, harmoniki do 63...)

MERJENJE PARAMETROV OKOLICE
- (temp., hitrost vetra, pretok, jakos sončnega sevanja...)

REGULACIJA IN ALARMIRANJE
- (do 16 digitalnih I/O za potrebe krmiljenja in alarmiranja)

KOMUNIKACIJA
- (ETHERNET, USB, GSM/GPRS, LPR, RS232/485, MODBUS, IEC EN 61850)

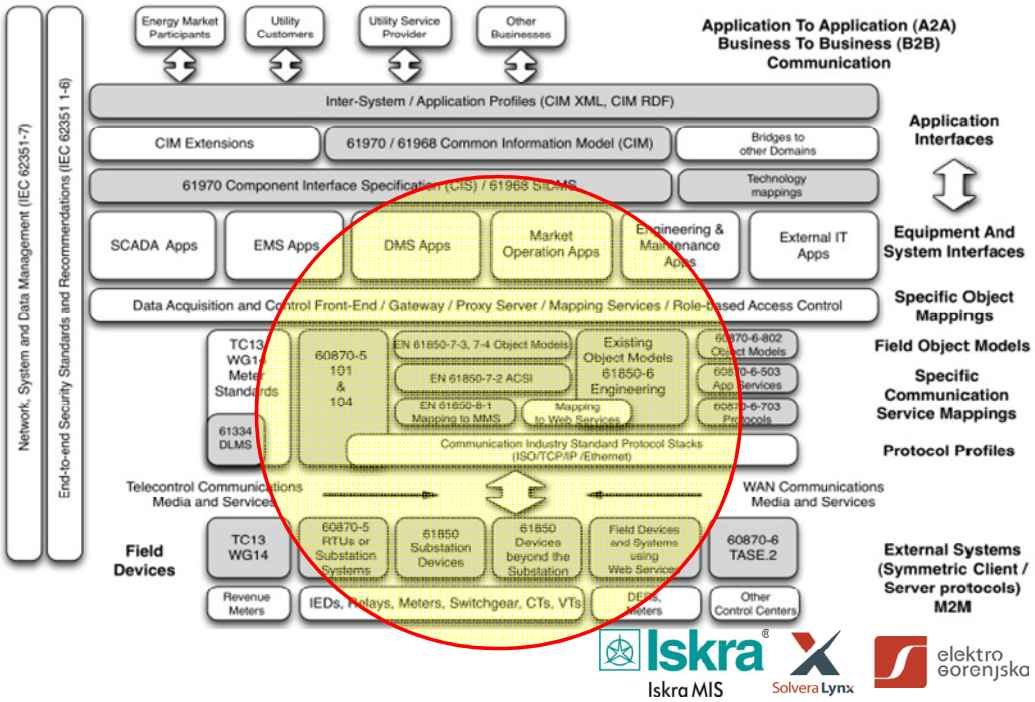


Iskra Iskra MIS · Solvera Lynx · elektro gorenjska · GORENJSKE ELEKTRARNE

Stran 7

Naložba v vašo prihodnost
OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski sklad za regionalni razvoj

Protokol IEC61850 in TC57

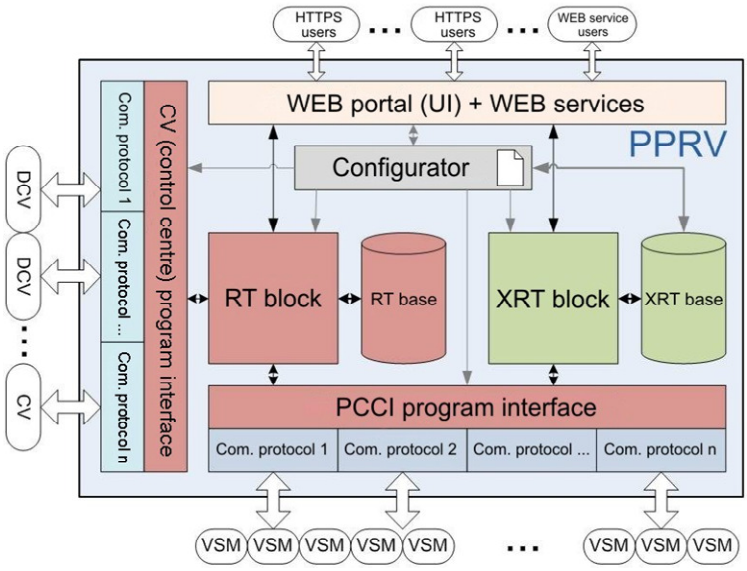


Iskra Iskra MIS · Solvera Lynx · elektro gorenjska · GORENJSKE ELEKTRARNE

Stran 9

Naložba v vašo prihodnost
OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski sklad za regionalni razvoj

Povezovalno programje



Connection	Eligible protocols	Preferential protocols
PCCI ↔ distributed sources middleware	IEC 61850 IEC 60870-5-104 Modbus TCP DNP3	IEC 61850
distributed sources middleware ↔ distribution control centre (SCADA)	IEC 60870-6 TASE.2 (ICCP) OPC IEC 61970 IEC 60870-5-104	IEC 60870-6 TASE.2 (ICCP)
distributed sources middleware ↔ final users	HTTPS – web access to user inetrfaces and avaliable Web sedistributed sourcesices	HTTPS, WEB distributed services

DCV - distribution control centre
VSM - Point of Common Coupling Interface (PCCI)
PPRV - distributed sources middleware

Iskra Iskra MIS · Solvera Lynx · elektro gorenjska · Gorenjske elektrarne

Stran 10

Naložba v vašo prihodnost
OPERACIJO DELNO FINANCIRA EVROPSKA UNIJA
Evropski sklad za regionalni razvoj

Aplikacije in storitve

TRŽNE STORITVE

- **agregiranje razpršenih virov** v virtualno elektrarno, kar omogoča nastop na trgu z energijo na debelo (ang. wholesale energy market), kar za posamezen majhen vir sicer ne bi bilo mogoče in kar je zdaj omogočeno le velikim proizvodnim enotam,
- **upravljane s porabo** (Demand Side Management (DSM) oziroma Demand Side Bidding (DSB)) v smislu signaliziranja za to zmožnih in v sistem vključenih uporabnikov, da v obdobjih zelo visokih cen energije zmanjšajo porabo glede na predviden vozni red, prihranjena energija pa se potem proda na trgu,
- **nastop na trgu sistemskih storitev**, ki niso lokalno pogojene, kot je na primer nudenje terciarne rezerve.

SISTEMSKE STORITVE

- omejevanje pretokov zaradi ozkih grl v omrežju
- zagotavljanje ustreznih napetostnih profilov – regulacija napetosti, regulacija jalove moči
- nadzor nad kvaliteto napetosti
- nudenje terciarne rezerve
- možnost lokalnega otočnega obratovanja
- pomoč pri vzpostavljanju omrežja po razpadu

Iskra Iskra MIS · Solvera Lynx · elektro gorenjska · Gorenjske elektrarne

Stran 12

Zaključek

Projekt SUPERMEN je bil končan v januarju 2011. Demonstracija projekta še vedno deluje v distribucijskem omrežju Elektro Gorenjske in zaključenem gospodarskem območju Petrol Energetike. Na podlagi tega projekta je pri partnerjih nastalo ali je v nastajanju več novih končnih izdelkov in sistemskih rešitev. Nekatere aktivnosti začete v tem projektu se nadaljujejo v sklopu Kompetenčnega centra za pametna omrežja in v drugih raziskovalnih in izvedbenih projektih industrijskih partnerjev projekta SUPERMEN.

Zahvale

Zahvaljujem se projektni skupini projekta SUPERMEN, ki je pomagala izvesti ta zahtevni projekt in je soustvarila tudi to predstavitev. Še posebna zahvala gre prof. dr. Igorju Papiču, ki je vodil strokovni del projekta SUPERMEN.

Janez Šmid, direktor razvoja in raziskav v Iskra MIS, skrbnik projekta SUPERMEN

Upravljanje storitev jedrnega omrežja

Goran Uršič, ELES, Hajdrihova 2, Ljubljana, vodja kompetenčnega centra za TK storitve
Uroš Juvan, Iskra Sistemi, d. d., Stegne 21, Ljubljana, specialist za napredne IP rešitve
Janez Jurjevec, Iskra Sistemi, d. d., Stegne 21, Ljubljana, specialist za napredne IP rešitve

Povzetek — Telekomunikacijsko omrežje ELES je podporni steber informacijske infrastrukture, ki vključuje tako povezljivost notranjih in zunanjih uporabnikov, kot tudi nadzor in upravljanje energetskih naprav v omrežju. Obstoječa tehnologija za spremljanje in upravljanje jedrnih storitev kompleksnega telekomunikacijskega omrežja ELES ni več primerna. Infoblox Grid tehnologija je kos kompleksnosti omrežja z učinkovitim spremljanjem in upravljanjem naslovnega prostora IPv4 in IPv6 (IPAM), storitvijo za dodeljevanje naslova IP (DHCP) ter storitvijo za preslikavo iz imena v naslov IP in obratno (DNS). SmartGrid je množica pametnih energetskih naprav, ki bo v prihodnosti reševala mnogo obstoječih problemov v energetiki. Zaradi svoje narave je pri implementaciji SmartGrid nujno vpeljati internetni protokol prihodnosti (IPv6).

Ključne besede — SmartGrid, ELES, Infoblox Grid, IMAP, DHCP, DNS, IPv6

Abstract — ELES telecommunications network is an underlying infrastructure, on which power transmission process control, monitoring, internal user-to-user, and external user communications are based. Plain monitoring of existing network core services is not sufficient any more. Infoblox Grid technology is capable of management and monitoring of complex networks, including IPv4 and IPv6 address management (IPAM), IP address allocation service (DHCP) and mapping between hostname and IP address and vice versa (DNS). SmartGrid is a set of smart power generation, consumption and monitoring devices, which is going to solve many existing power generation and transmission related problems in the future. For the very nature of SmartGrids, it is neccessary to introduce future internet protocol (IPv6) in its implementation.

Keywords — SmartGrid, ELES, Infoblox Grid, IMAP, DHCP, DNS, IPv6

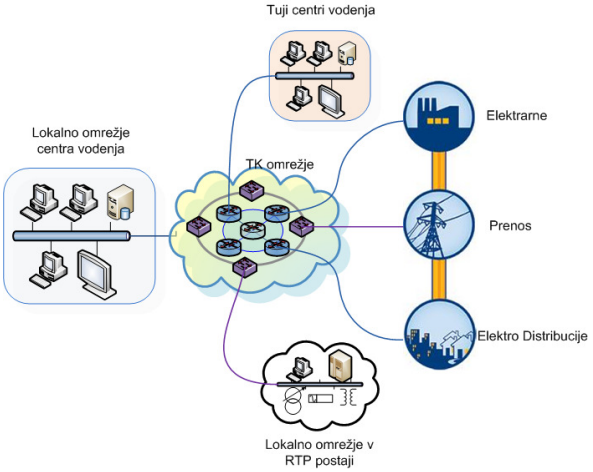
I. Uvod

Pod storitve jedrnega omrežja štejemo storitve za dodelitev IP naslova (DHCP), pretvarjanje internetnih imen v IP številke in obratno (DNS) ter upravljanje IP naslovnih prostorov (IPAM). Brez integracije naštetih storitev je skoraj nemogoče učinkovito nadzorovati ter upravljati omrežja. Še posebej se problem pojavi pri IP naslavljanju nove generacije (IPv6), s povečanjem števila omrežij ter naslovov IPv6.

Integracija storitev jedrnega omrežja je v organizacijah z velikim številom IP omrežij in IP naprav ključnega pomena. Brez integracije je potrebno ročno posodabljati zasedenost IP naslovnih prostorov (največkrat tabelarično) ter ločeno popravljati nastavitve DHCP in DNS strežnikov. Informacije med DHCP in DNS strežniki ter zasedenost IP naslovnih prostorov med seboj niso povezane. To povečuje količino dela za vnos posameznega IP naslova ter omogoča napake zaradi treh ločenih vnosov. Do tega spoznanja je prišel tudi ELES, saj ima veliko število IP omrežij ter naprav. Z vpeljavo pametnega SmartGrid omrežja bo nujen prehod na IPv6, število naprav in omrežij se bo znatno povečalo.

II. Predstavitev okolja

Obstoječe telekomunikacijsko omrežje ELES se je začelo intenzivno razvijati po letu 1995 z nameščanjem optičnih vlaken na daljnovode. Pred tem se je uporabljalo PLC komunikacijo preko visoko napetostnega omrežja. Telekomunikacijsko omrežje ELES predstavlja podporni sistem in je prvenstveno namenjeno interni uporabi za lastne potrebe, kar vključuje upravljanje prenosnega omrežja za prenos električne energije, prenos podatkov za potrebe sekundarnih energetskih sistemov ter storitve poslovne informatike. Poleg tega se telekomunikacijski sistem uporablja še za povezavo z drugimi elektroenergetskimi podjetji v Sloveniji in tujini. Viški kapacitet v omrežju so na voljo tudi zunanjim poslovnim uporabnikom, kar trenutno s stališča podjetja predstavlja dopolnilni segment.



Slika 1: Prikaz segmentov omrežja za zagotavljanje TK storitev EE sistema

Omrežje se gradi na podlagi zahtev internih uporabnikov, ki zahtevajo visoko stopnjo razpoložljivosti in zanesljivosti telekomunikacijskih storitev znotraj elektroenergetske infrastrukture ELES.

Med storitvami internih uporabnikov so ključne:

– prenos kriterija distančne zaščite,
– nadzor zaščit,
– vodenje energetskega sistema,
– števčne meritve,
– tehnična informatika.

Med ostale storitve za interno uporabo spadajo še storitve:

– govorne telefonije,
– podatkovnega prenosa,
– nadzora oddaljenih napajalnih sistemov,
– nadzora kakovosti električne energije,
– nadzor transformatorjev,
– prenosa drugih telemetričnih podatkov (nadzor zaledenitev daljnovodov, vremenske postaje, temperature, vodostaji, kamere, pristopna kontrola ipd.).

V primeru povezovanja z ostalimi elektroenergetskimi distribucijskimi podjetji mora telekomunikacijski sistem na točkah medoperaterskih povezav zadoščati zahtevanim omrežnim kriterijem podjetja ELES ter drugih elektroenergetskih podjetij. Priporočila izvedbe komunikacijskega sistema za potrebe povezljivosti med elektroenergetskimi operaterji podaja UCTE. Priporočila in tehnične zahteve poleg opredeljevanja načina izvedbe povezljivosti med elektroenergetskimi operaterji posledično določajo tudi karakteristike segmenta komunikacij znotraj infrastrukture operaterja.

Tretji segment storitev telekomunikacijskega omrežja ELES se nanaša na komercialno ponudbo viškov kapacitet v omrežju, ki se izvaja preko hčerinske družbe Stelkom d. o. o.

Podjetje Stelkom d. o. o. je relativno malo podjetje, ki so ga ustanovila slovenska Elektro podjetja. Zaradi lastniškega ozadja ima podjetje velike možnosti za razvoj, saj mu lastniška struktura omogoča velik investicijski potencial.

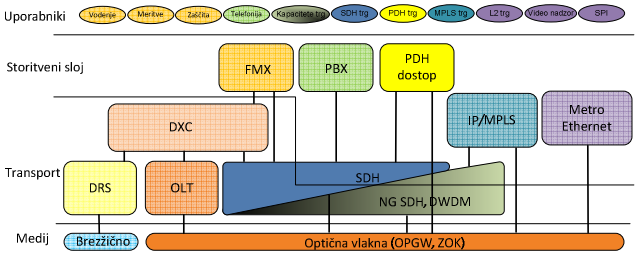
Storitve namenjene za trg:

Tabela 1: Storitve na sloju optičnega

– E1, E3	– 10 GbE
– STM-1/4/16/64	– FC
– 10/100 Mb/s Ethernet	– Λ
– GbE	

Tabela 2: Storitve IP MPLS / Ethernet podatkovnega

– E-Line	– L2 VPN
– E-LAN	– L3 VPN
– MPLS	– PWE
– VPLS	



Slika 2: Prikaz tehnologij in storitev TK omrežja ELES

III. PROBLEMATIKA OBVLADOVANJA IP NASLOVNEGA PROSTORA IN RAZLOGI ZA INTEGRACIJO STORITEV JEDRNEGA OMREŽJA

Kompleksnost TK omrežja in podsistema, ki medsebojno vplivajo drug na drugega, je zelo visoka. Dimenzija kompleksnosti omrežja posega tudi v obvladovanje in upravljanje IP naslovnega prostora.

Poleg arhitekturne in topološke plati omrežja (razpršenost objektov po širšem območju Slovenije, kjer so ELES-ovi in drugi energetski objekti) je potrebno upoštevati tudi to, da naročnikom TK storitev zagotavljamo transparentne povezave, kjer uporabniki storitev sami določajo in upravljajo IP naslovni prostor. V določenih primerih predlagajo naslovne prostore tudi integratorji oziroma proizvajalci energetske opreme. Nekatera starejša energetska oprema lahko komunicira z nadzornimi sistemi pod točno določenimi pogoji naslavljanja in povezovanja.

Večina uporabnikov ima več lokalnih omrežij, kjer so nameščeni sistemi za vodenje in spremljanje sistemov. Glede na potrebe po povezovanju z ostalimi omrežji in partnerji so uporabljeni različni načini varovanja in upravljanja omrežij. Dodatni problem pri obvladovanju naslovnega prostora je veliko število storitev, katerih naslovni prostor je segmentiran glede na regijske obroče.

Spremljanje naslovnega prostora IP za celotno podjetje je skorajda nemogoče, saj ni celotnega pregleda in administracije IP naslovnega prostora. Del naslovnega prostora se obvladuje z programskimi orodji. Večji del načrtovanja in spremljanje zasedenosti naslovnega prostora pa se izvaja v Excel dokumentih, kateri pa niso nujno vedno posodobljeni.

IV. INTEGRACIJA STORITEV JEDRNEGA OMREŽJA

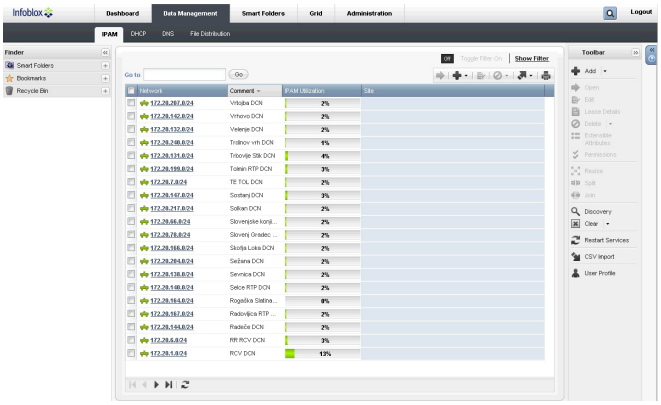
Integracija storitev jedrnega omrežja je pomembna tako za notranje (lokalni uporabniki, partnerska

energetska omrežja), kot tudi za zunanje (Internet) uporabnike. Vse ostale višje nivojske storitve namreč temeljijo na osnovnih storitvah (pridobivanje IP naslova, preslikava internetnega imena v IP naslov in obratno).

ELES integrira storitev jedrnega omrežja sloneč na tehnologiji Infoblox grid. Grid tehnologija omogoča distribucijo naprav Infoblox v različna omrežja, pri čemer naprave med seboj komunicirajo preko protokola IP. Grid povezava omogoča centralni nadzor in upravljanje distribuiranih naprav, distribuiranje baze po napravah, itd. Grid je lahko sestavljen iz fizičnih ali virtualnih elementov. Fizični elementi so lahko različno zmogljive naprave z vgrajeno programsko opremo. Virtualni elementi so virtualni računalniki, ki tečejo znotraj VMware virtualnega okolja. Tako fizični, kot tudi virtualni elementi, vsebujejo vse zahtevane storitve jedrnega omrežja (IPAM, DHCP ter DNS). Poleg zahtevanih storitev vsebujejo tudi storitev NTP, TFTP, FTP in HTTP. Slednje tri so namenjene predvsem izmenjavi podatkov med napravami povezanimi v grid. Programska oprema poleg protokola IPv4 seveda podpira tudi protokol IPv6 v vseh podprtih storitvah.

ELES se je odločil za uporabo fizičnih elementov oziroma naprav. Jedrni napravi, imenovani master in master candidat, se nahajata v jedru omrežja. Dve napravi sta izbrani zaradi redundance. V primeru izpada naprave master njeno delo prevzame naprava master candidat. Obe napravi vsebujeta celotno bazo vseh naprav v gridu. Ostale naprave so razporejene po zunanjem omrežju, partnerskem energetskem omrežju ter ostalih robnih omrežjih. Vse naprave so povezane v grid, ki omogoča večjo zanesljivost, centralno upravljanje in nadzor, centralno posodabljanje naprav itd. Razporeditev naprav po različnih omrežjih omogoča medsebojno neodvisnost omrežij (tudi do jedrnega) v primeru, da je povezava med njimi prekinjena. To pomeni, da sta strežnika DHCP in DNS, ki tečeta na lokalni napravi, še vedno dostopna za lokalne uporabnike oziroma strežnike. Posledica dostopnosti je, da lokalni uporabniki kljub nepovezanosti z zunanjim svetom, še vedno lahko komunicirajo med seboj in z lokalnimi strežniki.

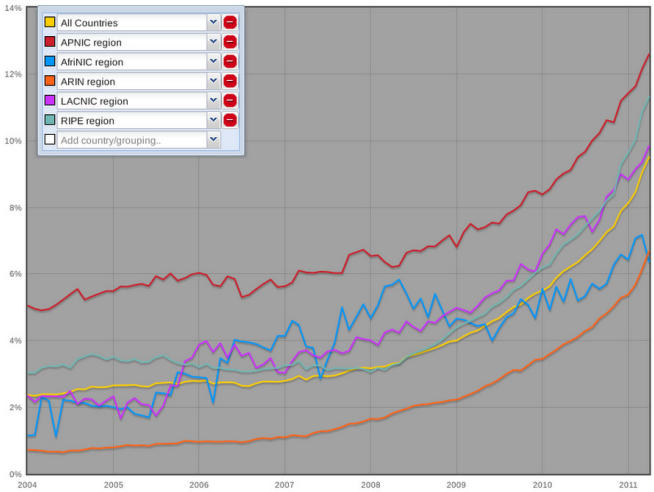
Celoten nadzor in upravljanje naprav v gridu opravljamo preko jedrnih naprav. Imamo vpogled v zasedenost vseh vnesenih omrežij. Nova omrežja lahko dodajamo s posebno funkcijo odkrivanja omrežja. Funkcija poskuša za vsak IP naslov v omrežju identificirati tip naprave, ime naprave ter MAC naslov naprave. Te informacije so dovolj za samodejen vnos najdene naprave v IPAM, DHCP in DNS servis bodisi jedrnih ali obrobnih naprav.



Slika 3: Pregled zasedenosti posameznih omrežij (IPAM)

V. IPv6 V OMREŽJU SMARTGRID

IPv6 je prihodnost IP omrežja. Razlog je poplava IP omogočenih naprav ter izčrpanost naslovnega prostora IPv4. V preteklosti se je v izogib hitremu uvajanju protokola IPv6 žal uvedel tako imenovani način delovanja NAT z rezerviranimi zasebnimi omrežji. NAT v nasprotju s prepričanjem velikega števila ljudi ne omogoča neposrednega povezovanja računalnikov iz zasebnega omrežja v Internet ali drugo zasebno omrežje, brez dodatnega dela mrežnih strokovnjakov. Prav tako ne povečuje varnosti naprav v zasebnem omrežju itd.



Slika 4: Število dodeljenih IPv6 mrež (AS) v odstotkih po svetovnih internetnih regijah (vir RIPE)

Prihodnost energetskega omrežja je tako imenovano omrežje SmartGrid. Omrežje SmartGrid vsebuje veliko število pametnih energetskih naprav, priklopljenih v IP omrežje. Preko teh naprav lahko spremljamo stanje energetskega omrežja (senzorji) ter aktivno spreminjamo parametre energetskega omrežja, glede na določene situacije v energetskem omrežju. V primeru izpada določenega voda se količina izpada električne energije prerazporedi preko delujočih vodov.

Pametne energetske naprave v SmartGrid omrežju omogočajo samodejno spremljanje porabo električne energije pri posameznih velikih in malih odjemalcih. Ni potrebno posebej poudarjati, da se s tem zmanjšajo stroški zbiranja podatkov o porabi električne energije. Zmanjša se možnost zlorab, ki jih ponuja trenutni način zbiranja informacij. Pametne naprave pri odjemalcih omogočajo izklop ali vklop oskrbe električne energije na daljavo.

Lahko si predstavljamo, kakšno število pametnih naprav je potrebno za zgoraj opisano delovanje. Brez uvedbe IPv6 omrežja in s tem pametnih naprav, ki delujejo preko protokola IPv6, je skoraj nemogoče uvesti omrežje SmartGrid.

ELES je že v postopku pridobivanja svojega PI (Provider Independent) IPv6 naslovnega prostora. Sledila bo priprava robnih mrežnih naprav za uvedbo IPv6 mreže do notranjega omrežja ELES. Prehod na IPv6 bo najprej izveden na od zunaj dostopnih strežnikih in storitvah. Sledila bo uvedba povezljivosti IPv6 za notranje uporabnike. V tem obdobju se bodo strokovnjaki za omrežja na ELES-u pobliže seznanili s protokolom IPv6. Sledi IPv6 povezljivost s partnerskimi energetskimi omrežji. V zadnji fazi sledi izgradnja SmartGrid omrežja, slonečega na protokolu IPv6.

VI. ZAKLJUČEK

Nadzor in upravljanje jedrnih storitev velikih IP omrežij je zaradi vsaj treh nepovezanih storitev (IPAM, DHCP in DNS), ki upravljajo s sorodnimi informacijami, zapleten proces. Zahvaljujoč napravam, ki vsebujejo vse te elemente storitev velikih omrežij povezane, se zelo poenostavi nadzor in upravljanje velikih IP omrežij.

IPv6 je IP (internetni) protokol prihodnosti. Zgodnje uvajanje in seznanjanje inženirjev s tem protokolom je bilo v preteklosti zaželeno, sedaj pa je nujnost. Letos je IANA namreč izdala zadnje bloke IPv4 omrežij. S tem je svetovna zaloga internetnih naslovov IPv4 izčrpana. Predvsem je treba poudariti, da protokol IPv6 rešuje težave tudi v večjem notranjem omrežju z veliko priključenimi napravami.

Goran Uršič se je rodil v Kopru leta 1971. 1998 je diplomiral na Fakulteti pomorstvo in promet. Zaposlen je na Elekto Slovenija kot vodja kompetenčnega centra za področje telekomunikacijskih storitev. Od leta 2000 je delal na področju SDH in PDH sistemov, po letu 2003 izvajal dela na področju načrtovanja in upravljanja IP/MPLS omrežij. V zadnjih letih predvsem načrtuje omrežja in vodi projekte v sektorju za informacijske in komunikacijske tehnologije.

Janez Jurjevec se je rodil v Trbovljah leta 1974. Diplomiral je leta 2001 s področja telekomunikacij na Fakulteti za elektrotehniko v Ljubljani. Že pred diplomo se je zaposlil v podjetju Mibo komunikacije d.o.o, kjer je opravljal dela sistemskega inženirja. Po združitvi podjetij je nadaljeval strokovno delo v podjetju Iskra Transmission d.o.o. Delal je na različnih področjih IP podatkovnih omrežij. Pri svojem delu se je srečal tudi z SDH in PDH tehnologijami ter mobilnimi omrežji. Sedaj deluje kot produktni vodja in vodja tehnike v oddelku podatkovnih komunikacij v podjetju Iskra Sistemi d.d.

Uroš Juvan se je rodil v Ljubljani leta 1976. Po študiju na Fakulteti za organizacijske vede je leta 2004 diplomiral s področja programiranja. Prvo zaposlitev si je izbral že pred koncem študija v javnem zavodu Arnes, kjer je delal 10 let na področju razvoja programske opreme v okolju UNIX/Linux. Bil je glavni razvijalec programske opreme za avtomatizirano registracijo vseh domen *.si*, napisane predvsem v programskem jeziku Java. Zadnjih nekaj let je sodeloval v mednarodnem projektu JRA1 krovne organizacije evropskega akademskega omrežja Géant2, kjer je razvil TCMP Web Service za pasivni nadzor omrežja. Svojo kariero nadaljuje z razvijanjem omrežne programske opreme ter aktivnostmi na področju IP omrežij v podjetju Iskra Sistemi d. d., kjer je zaposlen od začetka leta 2008.

Postavitev senzorskega omrežja na infrastrukturi javne razsvetljave

Miha Smolnikar, Carolina Fortuna, Matevž Vučnik, Marko Mihelin, Mihael Mohorčič
Odsek za komunikacijske sisteme, Institut "Jožef Stefan"

Povzetek — Skladno s paradigmo Interneta stvari se na najrazličnejših področjih uveljavlja uporaba senzorskih in aktuatorskih omrežij, ki tako postajajo vse pomembnejši sestavni del okolja v katerem živimo. Namen tega prispevka je predstaviti izkušnje pri nadgradnji infrastrukture javne razsvetljave z brezžičnim senzorskim in aktuatorskim omrežjem. Testno senzorsko omrežje je osnovano na Vsestranskem senzorskem vozlišču (VSN). Vsa vozlišča so opremljena s senzorji temperature, vlage, zračnega tlaka in svetilnosti ter preko posebnega vmesnika sposobna krmiliti svetilnost posameznih svetilk. Senzorski podatki se agregirajo v podatkovni bazi, ki je del povezovalne platforme (angl. middleware). Slednja poleg hranjenja podatkov služi tudi kot vmesnik med senzorskim in aktuatorskim omrežjem ter skupkom spletnih aplikacij (angl. mashup). Del povezovalne platforme pa sta tudi Global Sensor Networks (GSN) in orodje za rudarjenje podatkov StreamSense, ki ga uporabljamo kot osnovo za izris grafov na zahtevo.

Ključne besede — brezžično senzorsko in aktuatorsko omrežje, javna razsvetljava, LED svetila, vsestransko senzorsko vozlišče (VSN), povezovalna platforma

Abstract — This paper introduces a new outdoor testbed for Wireless Sensor and Actuator Networks (WSAN) deployed on the public lighting infrastructure. Currently it consists of 25 sensor nodes attached to light poles and 2 gateways, one for xDSL and the other for GSM/GPRS. The sensor nodes control dimming of the public LED lights and collect temperature, humidity, air pressure, luminance and battery voltage measurements. The sensor nodes and gateways are implemented on a Versatile Sensor Node (VSN) that runs a proprietary networking protocol for their interconnection. VSN is a fully modular WSAN platform featuring a powerful microcontroller and custom power supply with battery charger and optional solar cell extension. It supports numerous on board peripherals to cover different application requirements as well as several communication technologies to realize local sensor network and implement gateways to other existing fixed or mobile networks. The data is gathered, stored and processed by custom developed middleware, which represents the interface between WSAN and mashups. It consists of Message server, Database, Global Sensor Networks (GSN) and StreamSense. The latter is one of JSI analytic tools, in our case used to support real-time drawing of measurements graphs.

Keywords — Wireless Sensor and Actuator Network (WSN), Public Lighting, LED Lighting, Versatile Sensor Node (VSN), Middleware

I. UVOD

S pojavom koncepta Interneta stvari (angl. Internet of Things, IoT) smo priča razvoju brezžičnih senzorskih in aktuatorskih omrežij, ki segajo od namenskih, običajno homogenih, omrežij manjšega obsega proti souporabi senzorskih in aktuatorskih virov v obsežnih heterogenih omrežjih. S tem v omrežja povezani senzorji in aktuatorji postajajo vse pomembnejši del okolja, v katerem živimo in delamo. Obseg in heterogenost zahtevata postavitev ustreznih testnih omrežij, ki predstavljajo podlago za pridobivanje prepotrebnih izkušenj iz realnih okoliščin obratovanja.

V preteklih letih so senzorska omrežja postala zanimiva predvsem za aplikacije nadzora okolja. Brezžično senzorsko omrežje sestavlja množica povezanih vozlišč s senzorji, ki generirajo velike količine podatkov, ki so na voljo tako raziskovalcem kot drugim uporabnikom. V svetu je že kar nekaj raziskovalnih testnih senzorskih omrežij, ki pa so večinoma postavljena v zaprtih prostorih in so, z izjemo omrežja TWIST na Tehnični univerzi v Berlinu, katerega sestavlja okoli 200 vozlišč Tmote Sky, manjšega obsega. Zunanja omrežja so zaradi višjih stroškov postavitve in vzdrževanja redkejša. Med njimi zasledimo Swiss Experiment, v okviru katerega pri postavitvi nadzornih postaj v švicarskih Alpah sodeluje večje število raziskovalnih skupin s področij okoljevarstva in računalništva. Postavitev trenutno obsega preko 4000 senzorskih virov, ki jih vzdržujejo ročno. Drugi primer testnega omrežja v zunanjem okolju predstavlja omrežje CitySense, v katerem je 100 senzorskih vozlišč postavljenih na različnih lokacijah v mestu Cambridge, ZDA. Senzorji sestojijo iz vgrajenega osebnega računalnika z mrežno kartico 802.11a/b/g. Tretji primer predstavlja projekt Copenhagen Wheel, v katerem so mobilna senzorska vozlišča vgrajena v kolesa [1].

Ta prispevek predstavlja sestavne dele, funkcionalno delovanje in pridobljene izkušnje pri postavitvi zunanjega testnega brezžičnega senzorskega in aktuatorskega omrežja na infrastrukturi javne

razsvetljave v občini Miren-Kostanjevica. Omrežje trenutno obsega 25 senzorskih vozlišč na drogovih javne rzsvetljave. Do sredine leta 2011 naj bi se omrežje povečalo na 100 vozlišč, nato pa na več sto vozlišč. Zasnovano je na uporabi Vsestranskega senzorskega vozlišča (angl. Versatile Sensor Node, VSN) in namensko razvitega omrežnega protokola. Vozlišča so opremljena s senzorji temperature, vlage, zračnega tlaka in svetilnosti ter omogočajo individualno zatemnjevanje svetilk.

V nadaljevanju prispevka v drugem poglavju na kratko opisujemo značilnosti javne razsvetljave in zahtev za senzorsko omrežje. Tretje poglavje podaja arhitekturo, sestavne dele testnega omrežja in primere uporabe, četrto poglavje pa zaključuje prispevek.

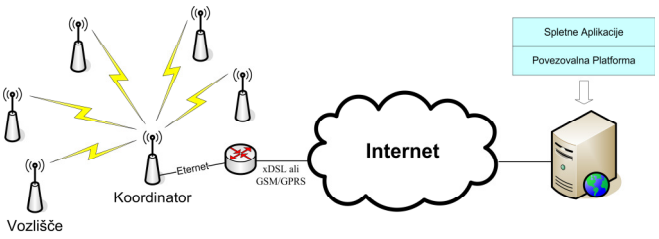
II. SENZORSKO IN AKTUATORSKO OMREŽJE NA INFRASTRUKTURI JAVNE RAZSVETLJAVE

Javna razsvetljava v svetovnem merilu predstavlja približno 20% porabe električne energije, zaradi česar so se nedavno pojavile direktive o zamenjavi neučinkovitih svetilk z žarilno nitko. V EU se prehodno obdobje zamenjave z učinkovitejšimi svetilkami končuje leta 2015. Kot ena izmed zanimivejših tehnologij za javno razsvetljavo se je pričela vse močneje uveljavljati tudi tehnologija LED (angl. Light Emitting Diode), ki je zaradi svetlobnega izkoristka blizu 100 lm/W postala zanimiva za velikoserijsko proizvodnjo. Poleg visokega izkoristka tehnologija LED ponuja še druge prednosti kot so dolga življenjska doba, usmerjenost svetlobnega snopa, odpornost na udarce in tresljaje, majhen volumen, delovanje izven UV dela spektra in inherentna podpora zatemenjevanju in napajanju preko obnovljivih virov energije (npr. kombinacija sončnih celic in baterijskega napajanja). Izračuni kažejo, da lahko že samo z zamenjavo klasičnih svetilk s tehnologijo LED zmanjšamo porabo električne energije do 40 %, s pametnim zatemenjevanjem pa lahko prihranimo še dodatnih 25 % energije. Poleg neposrednih ekonomskih prihrankov pa velja omeniti tudi manjše izpuste topologrednih plinov in zmanjšanje svetlobnega onesnaževanja.

Tehnologija LED se torej ponuja kot zelo prikladna rešitev za sektor javne razsvetljave, v kombinaciji s senzorskimi in/ali komunikacijskimi omrežji pa odpira priložnost za razvoj povsem novih aplikacij. To smo med drugim želeli pokazati s postavitvijo testnega senzorskega omrežja za infrastrukturo javne razsvetljave, ki temelji na tehnologiji LED. Trenutna postavitev senzorskega omrežja uporablja namensko razvit komunikacijski protokol, nadaljnje postavitve pa bodo zasnovane na tehnologijah ZigBee in Wireless M-BUS, ki delujejo v ISM (angl. industrial, scientific and medical) frekvenčnih pasovih pri 2,4 GHz in 868 MHz.

III. ARHITEKTURA TESTNEGA SISTEMA

Arhitekturo testnega senzorskega in aktuatorskega omrežja na infrastrukturi javne razsvetljave v občini Miren-Kostanjevica prikazuje slika 1. Tri glavne funkcionalne sklope predstavljajo: (*i*) senzorsko omrežje, (*ii*) povezovalna platforma (angl. middleware) ter (*iii*) podatki in aplikacija. V nadaljevanju je podan podrobnejši opis VSN, ki predstavlja osnovo strojne opreme, na kateri sta realizirana tako senzorsko vozlišče kot prehod. Temu sledi predstavitev ostalih sestavnih delov arhitekture testnega senzorskega omrežja.



Slika 1: Arhitektura testnega senzorskega omrežja

A. *Vsestransko senzorsko vozlišče*

Namen testnega senzorskega in aktuatorskega omrežja na infrastrukturi javne razsvetljave je med drugim preučevanje uporabe namensko razvite rekonfigurabilne strojne in programske opreme, ki podpira enostaven razvoj novih aplikacij kot tudi drugačno povezovanje že obstoječih. Zgradba testnega omrežja temelji na VSN[1], ki z modularno zasnovo omogoča hitro in enostavno prilagoditev potrebam različnih aplikacij.

Jedrni modul (angl. Versatile Sensor Core, VSC) je zasnovan okrog visoko zmogljivega 32-bitnega mikrokrmilnika z jedrom ARM Cortex-M3. Izbrani mikrokrmilnik STM32F103 ponuja odlično razmerje med procesorsko močjo in porabo energije, podpira frekvenco procesorske ure do 72 MHz in ima 512 kB programskega spomina in 64 kB podatkovnega spomina. Kot dodaten spomin je na voljo 128 kB hitrega stalnega spomina na namenskem vodilu SPI (angl. Serial Peripheral Interface) s frekvenco ure vodila do 18 MHz. Za shranjevanje večje količine podatkov je predvidena reža za mini SD kartice do velikosti 32 GB. S stališča priključevanja perifernih naprav so na voljo digitalni vmesniki kot so I^2C (angl. Inter-Integrated Circuit), SPI, UART (angl. Universal asynchronous receiver/transmitter) in USB (angl. Universal Serial Bus), ter analogni vmesniki z

[1] http://sensorlab.ijs.si/

12-bitnim analogno-digitalnim (AD) in 12-bitnim digitalno-analognim (DA) pretvornikom.

Senzorsko vozlišče podpira različne vrste napajanja od možnosti priključitve na zunanje napajanje do baterijskega napajanja z vgrajenim napajalnikom in po izbiri tudi sončne celice. Za varčevanje z energijo lahko izbiramo med tremi stanji varčnega delovanja, ki so spanje, ustavitev in pripravljenost, poleg tega pa obstaja še stanje globoke hibernacije v katerem celotno vezje porabi manj kot 7 μA.

Na radijskem modulu (angl. Versatile Sensor Radio, VSR) smo za testno omrežje izbrali XBee-PRO, ki deluje v ISM frekvenčenm pasu pri 868 MHz. Z izbrano anteno ima v notranjih prostorih oz. urbanem okolju doseg do 500 m, z uporabo dipolne antene v idealnih razmerah brez ovir pa tudi do 40 km.

Osnovnima moduloma VSC in VSR lahko dodamo razširitveni modul (angl. Versatile Sensor Expansion, VSE), ki v skladu z zahtevami posamezne aplikacije določa dejansko fukncionalnost vozlišča. Na vozlišču prehoda smo v testnem senzorskem omrežju modul VSE opremili z vmesnikom Ethernet, ki je nadalje priključen na xDSL ali na GSM/GPRS modem. Na senzorskem vozlišču pa so na modulu VSE realizirani: senzorji temperature, vlažnosti, zračnega tlaka, svetilnosti in baterijske napetosti; aktuator za zatemenjevanje luči; in zaščitno vezje. Zatemnitev luči nadziramo preko merjenja svetilnosti, pri čemer imajo nekatera vozlišča za večjo natančnost po dva senzorja svetilnosti, enega usmerjenega proti nebu in drugega proti tlom.

B. Protokol senzorskega in aktuatorskega omrežja

Trenutna testna postavitev sestoji iz dveh ločenih testnih senzorskih omrežij topologije zvezda. Senzorska vozlišča so povezana s koordinatorskim vozliščem, ki hkrati predstavlja prehod za xDSL ali GSM/GPRS omrežje. Vloga koordinatorja je nadzor lokalnega senzorskega omrežja, odkrivanje senzorskih vozlišč, zajem in zbiranje podatkov, nastavljanje parametrov senzorskih vozlišč (npr. nastavitev zatemenjevanja) in komunikacija s strežnikom. Senzorska vozlišča se odzivajo na koordinatorjeve zahteve, nadzirajo luči in upravljajo z napajanjem. Ker je zunanje napajanje v trenutni testni postavitvi na voljo le preko noči, ko so luči prižgane, senzorska vozlišča preko dneva obratujejo na baterije, ki se preko noči polnijo.

Namenski protokol senzorskega omrežja je zasnovan na principu klicanja perifernih vozlišč. Po vključitvi in nato vsakih 30 sekund koordinator razpošlje vsem vozliščem sporočilo s svojim naslovom. Temu sledi proces povezovanja, ko posamezna vozlišča odgovorijo s posebnimi statusnimi sporočili, v katerih se nahaja naslov vozlišča, njegov status in nastavitve. Status trenutno vsebuje informacijo o stanju napajalnega vira (baterija/napajanje/zunanje), v nastavitvah pa je informacija o tem, ali je luč prižgana ali ugasnjena ter kakšen je nivo zatemnitve (0-100%). Po sprejemu posebnega statusnega sporočila koordinator vpiše vozlišče v svojo omrežno tabelo. Ko je omrežje vzpostavljeno koordinator bodisi zbira meritve posameznih senzorjev, bodisi preko ustreznih sporočil konfigurira posamezna senzorska vozlišča. Po sprejemu zahteve senzorska vozlišča izvedejo meritev in odgovorijo s podatkovnim sporočilom, pri čemer je odzivni čas v mejah 0,5 sekunde. Koordinator podatkovnemu sporočilu doda časovno značko in ga posreduje na strežnik.

Zaradi izvajanja funkcionalnosti prehoda koordinator po tem, ko mu je dodeljen IP naslov strežniku periodično sporoča svoj status. To je zlasti pomembno s stališča nadzora, ko aplikacija na strežniški strani pošilja zahteve za senzorsko omrežje.

Ker senzorska vozlišča podatkov ne pošiljajo zgolj določenemu koordinatorju ampak vsem znotraj radijskega dosega, se lahko izmnenično uporabljajo različni koordinatorji, kar povečuje robustnost omrežja. Odločitev, kateri koordinator zahteva podatke z določenega senzorskega vozlišča, se sprejme na podlagi omrežnih tabel dostopnih koordinatorjev na strani strežnika.

C. xDSL in GPRS prehoda

Za posredovanje podatkov iz senzorskega omrežja v povezovalno platformo na strežniku je VSN opremljena z modulom VSE, na katerem se nahaja pretvornik iz serijskega vodila na Ethernet, t.j. Lantronix XPort. Slednji omogoča, da vozlišče prehoda komunicira s HTTP strežnikom neposredno preko UART vmesnika brez potrebe po implementaciji protokolnega sklada TCP/IP na mikrokrmilniku. XPort se obnaša kot običajni modem in se ga upravlja preko standardnega nabora AT ukazov. Seveda pa njegova uporaba znatno poveča potrebe po napajanju, zato je VSE modul na vozlišču prehoda opremljen tudi z dodatnim napajanjem.

Opisan modul VSE je lahko priključen na fiksni internet preko xDSL modema ali pa na mobilni internet preko GPRS modema.

D. Senzorji in aktuatorji

V postavitvni testnega senzorskega omrežja na vsakem vozlišču uporabljamo tri različne senzorje za zajem okoljskih podatkov. SHT11 je digitalni senzor temperature in relativne vlage, ki se na VSN priključi preko serijskega vmesnika podobnega I^2C. SCP1000 je digitalni senzor absolutnega tlaka in temperature z vmesnikom SPI, TLS2561 pa je senzor svetilnosti in se na VSN povezuje preko vmesnika I^2C. Ti senzorji se nahajajo na tiskanem vezju izven ohišja senzorskega

vozlišča in so pred zunanjimi vplivi zaščiteni z epoxy smolo.

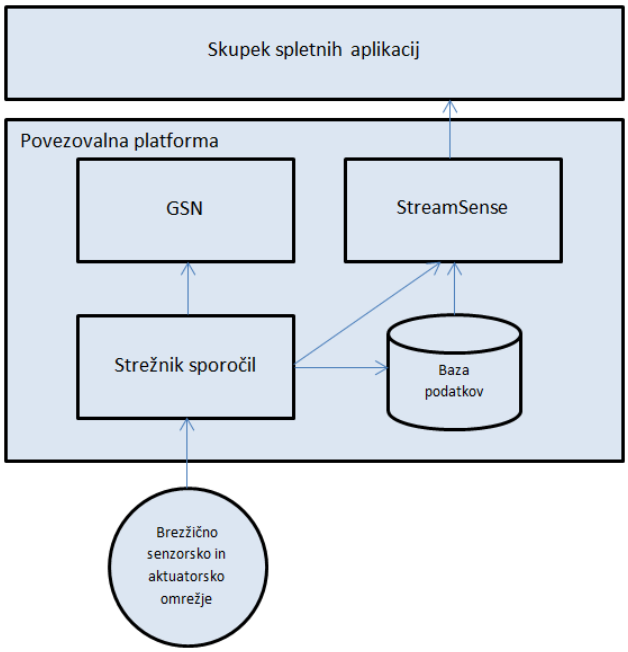
Zatemenjevanje luči preko ustreznega vmesnika nastavljamo z enosmerno napetostjo med 1 in 10 V. Nadzorno napetost za zatemenjevanje generiramo z pulzno-širinsko modulacijo, jo povprečimo z RC filtrom in pomnožimo, tako da se ujema z napetostjo vmesnika.

E. Povezovalna platforma

V splošnem je naloga povezovalne platforme, da poveže heterogena senzorska vozlišča v brezžičnem senzorskem omrežju z aplikacijami. Tako mora podpirati razvoj, vzdrževanje, postavitev in izvrševanje aplikacij, ki uporabljajo senzorje [2]. To vključuje komuniciranje s senzorskim omrežjem, združevanje podatkov na način, da zagotovimo sledljivost nazaj do izvora, ter zagotavljanje visokonivojske abstrakcije heterogenih vozlišč. Zelo pomembna lastnost povezovalne platforme je tudi skalabilnost, saj mora tudi ob povečevanju obsega senzorskega omrežja zagotavljati sprejemljiv nivo delovanja [3].

Povezovalno platformo lahko postavimo na različne nivoje arhitekture senzorskega omrežja, tipično pa se nahaja na vozlišču ali pa na samem robu omrežja, kjer se uporabljajo kovencionalni strežniki. V prvem primeru je podatkovna baza porazdeljena preko senzorskega omrežja, uporabniku pa je za dostopanje do senzorskih podatkov zagotavljen podoben vmesnik kot do SQL baze. Primera takega pristopa sta TinyDB in COUGAR [4]. V drugem primeru pa je senzorsko omrežje ločeno od upravljanja s podatki, kar znatno razbremeni vozlišča in jim s tem omogoča večjo energetsko učinkovitost. Primera tega pristopa sta Senceive [5] in Global Sensor Networks (GSN) [6]. V robnem pristopu se za zanesljivo dostavo podatkov do povezovalne platforme uporabljajo ponorna vozlišča. To je vozlišče, ki je priključeno na zmogljivejši računalnik, na katerem teče povezovalna platforma [7]. Za shranjevanje podatkov se uporabljajo konvencionalne podatkovne baze, primerne za shranjevanje velikih količin podatkov.

Ker smo želeli v čim krajšem času zbrati čim več podatkov iz okolja, smo našo povezovalno platformo zasnovali na rešitvi GSN[2], omogočili pa smo njen razvoj proti lastni povezovalni platformi. Slednja poleg GSN obsega še strežnik sporočil, podatkovno bazo in orodje za rudarjenje podatkov StreamSense, ki temelji na analitičnih orodij IJS [8]. Strežnik sporočil komunicira s ponornim vozliščem preko HTTP protokola. Kot prikazuje slika 2, strežnik periodično sprejme podatke iz ponornega vozlišča in jih multipleksira v ustrezno obliko za GSN, podatkovno bazo in StreamSense.



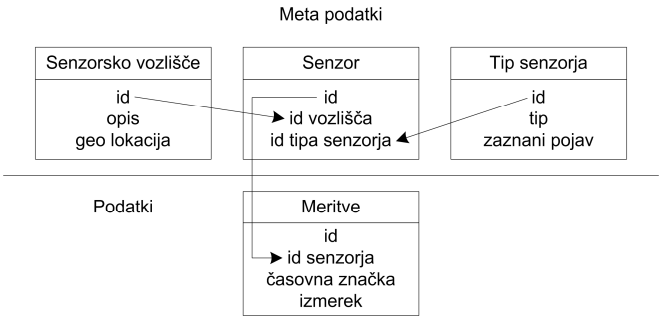
Slika 2: Shema povezovalne platforme

Osnovna abstrakcija platforme GSN je virtualni senzor [7], ki omogoča, da uporabnik v formatu XML (angl. Extensible Markup Language) specificira opis senzorjev ali celotnega senzorskega vozlišča. Virtualni senzor je lahko karkoli od mobilnega telefona, spletne kamere ali poljubnega drugega senzorskega vira. Za obdelavo vhodnih podatkovnih tokov GSN uporablja različne programske vmesnike (angl. Wrappers), ki podatke sprejete iz senzorskih virov prilagodijo standardnemu GSN podatkovnemu modelu. To uporabniku omogoča izgradnjo podatkovno orientiranega senzorskega spleta, ki sestoji iz senzorskih omrežij medseebojno povezanih preko GSN [7]. V naši implementaciji za prilagoditev podatkov uporabljamo programski vmesnik CSV (angl. Comma Separated Values). Podatki prihajajo v izvorni obliki, metapodatki pa se shranjujejo v virtualni senzor. Nadalje GSN vključuje tudi spletni strežnik za objavo podatkov in grafični prikaz rezultatov, omogoča pa tudi izvoz podatkov v različnih formatih.

Struktura podatkovne baze za shranjevanje izmerjenih vrednosti odraža strukturo strojne opreme, kjer senzorska vozlišča vsebujejo večji nabor senzorjev. Shematični prikaz strukture podatkovne baze iz štirih tabel prikazje slika 3.

Zgornje tri tabele z imeni Senzorsko vozlišče (angl. Sensor Node), Senzor (angl. Sensor) in Tip senzorja (angl. Sensor Type) shranjujejo metapodatke, ki opisujejo fizične naprave in opazovane pojave. Tabela senzorsko vozlišče shranjuje informacijo o vsakem postavljenem senzorskem vozlišču v omrežju, zagotavlja enovito identifikacijsko številko, opis in geo lokacijo postavljenih senzorskih vozlišč. Tabela senzor je namenjena enoviti identifikaciji senzorskih elementov, ki so priključeni na senzorsko vozlišče.

[2] http://gsn.ijs.si/



Slika 3: Struktura podatkovne baze

Opisi teh elementov so zbrani v tabeli tip senzorja, ki vsebuje informacijo o posameznih senzorjih in veličinah ter pojavih, ki jih le ti zaznavajo.

Spodnja tabela po imenu Meritve (angl. Measurement) shranjuje izmerke senzorjev z dodano časovno značko in identifikacijsko številko senzorja. S tako shranjenimi podatki in metapodatki zmanjšamo režijo podatkovne baze, hkrati pa lahko po potrebi vsako meritev povežemo nazaj do senzorskega vozlišča in senzorja. Ločevanje podatkov in metapodatkov pa nadalje omogoča tudi vzpostavitev virtualnega senzorskega omrežja na višjem nivoju abstrakcije.

Razlikovanje med metapodatki in podatki ni vedno enolično. Primer za to je na primer podatek o lokaciji. Ker so senzorska vozlišča v testnem omrežju fiksna, so tudi GSP koordinate vozlišč shranjene kot metapodatki. V primeru mobilnih senzorskih vozlišč pa se GPS sprejemnik smatra kot senzor za geo lokacijo, zato bi se GPS koordinate shranjevale v tabelo meritev.

Na vsakem senzorskem vozlišču je lahko priključenih več senzorjev, pri čemer gre lahko za različne ali enake senzorje, ki lahko spremljajo isti ali različne fizikalne pojave. V splošnem ni nujno, da imajo vsa vozlišča v omrežju enak nabor in število senzorjev, vendar pa imajo vsa vozlišča v našem testnem omrežju enak set šestih senzorjev.

Zadnji del povezovalne platforme je orodje za rudarjenje velikega obsega podatkov StreamSense. Uporabljamo ga za podlago spletni aplikaciji[3], ki je skupek aplikacij (angl. mashup) na podlagi podatkov s senzorjev in ostalih spletnh storitev. Gre za zmogljivo in skalabilno orodje, ki tudi pri več milijonih podatkov zagotavlja izris grafov na zahtevo v realnem času. Trenutni podatki se posredujejo v StreamSense preko stežnika sporočil, arhivirane podatke in metapodatke pa naloži StreamSense iz baze podatkov. Hiter odziv je še posebno pomemben pri izrisovanju grafov za daljša časovna obdobja. Povezovanje podatkov v testnem omrežju temelji na spletnih storitvah in vključuje geografsko karto z lokacijami senzorskih vozlišč, pri izbiri posameznega senzorskega vozlišča z miško pa se pojavijo različne možnosti prikaza senzorskih podatkov in izrisa grafov na dnevni, tedenski, mesečni ali letni osnovi. Po zaslugi orodja za rudarjenje StreamSense se ti grafi izrisujejo v realnem času ne glede na izbrano časovno obdobje.

IV. ZAKLJUČEK

Iniciative za zmanjševanje porabe energije časovno sovpadajo z razvojem učinkovitejše tehnologije LED, zaradi česar se v prihodnjih letih pričakuje obširna prenova infrastrukture javne razsvetljave. Senzorska omrežja pri tem lahko zagotovijo še dodatne prihranke energije, poleg tega pa odpirajo možnosti za vrsto novih aplikacij. Prav to je vzpodbudilo postavitev testnega senzorskega omrežja na infrastrukturi javne razsvetljave v občini Miren-Kostanjevica. Omrežje sestoji iz senzorskih vozlišč na osnovi VSN, ki komunicirajo preko namenskega protokola, zajemajo izbrane okoljske podatke, predvsem pa je njihova vloga zatemenjevanje svetilk v skladu z zahtevano svetilnostjo, kar omogoča pomembne dodatne prihranke energije. Testno omrežje je povezano s povezovalno platformo na strežniku preko prehoda na xDSL ali GSM/GPRS. Povezovalna platforma upravlja z omrežjem, shranjuje podatke in omogoča različne tekstualne in grafične prikaze podatkov.

ZAHVALE

Avtorji se zahvaljujejo občini Miren-Kostanjevica in podjetju Envigence d.o.o. za omogočanje postavitve testnega omrežja in sodelavcem SensorLaba za podporo in pomoč pri razvoju opisanih rešitev.

LITERATURA

[1] N. Savage, "Cycling through data," Communications of the ACM, Vol. 53, No. 9, September 2010.
[2] K. Romer, O. Kasten and F. Mattern, "Middleware Challenges for Wireless Sensor Networks," Mobile Computing and Communications Review, Vol. 6, No. 2, October 2002.
[3] S. Hadim and N. Mohamed, "Middleware: Middleware Challenges and Approaches for Wireless Sensor Networks," IEEE Distributed Systems Online, Vol. 7, No. 3, March 2006.
[4] K. Henricksen, R. Robinson, "A Survey of Middleware for Sensor Networks: State-of-the-Art and Future Directions," in Proc. of the International workshop on Middleware for sensor networks (MidSens'06), Melbourne, Australia, December 2006.
[5] C. Hermann and W. Dargie, "Senceive: A Middleware for a Wireless Sensor Network," in Proc. Of the 22nd International Conference on Advanced Information Networking and Applications (AINA 2008), Okinawa, Japan, March 2008.
[6] H. Jeung, et al., "Effective Metadata Management in Federated Sensor Networks," in Proc. Of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2010), California, USA, June 2010.
[7] K. Aberer, M. Hauswirthy and A. Salehi, "Infrastructure for data processing in large-scale interconnected sensor networks," in Proc. of the International Conference on Mobile Data Management (MDM2007), Mannheim, Germany, May 2007.
[8] B. Fortuna, C. Fortuna and D. Mladenić, "Real-time News Recommender System," ECML/PKDD, Barcelona, Spain, September 2010.

[3] http://sensors.ijs.si/

Miha Smolnikar je diplomiral leta 2005 na Fakulteti za elektrotehniko Univerze v Ljubljani in se zaposlil kot mladi raziskovalec na Odseku za komunikacijske sisteme Instituta "Jožef Stefan". Trenutno zaključuje doktorski študij elektrotehnike na Fakulteti za elektrotehniko Univerze v Ljubljani. V okviru raziskovalnega dela se ukvarja z medplastnim načrtovanjem protokolnega sklada, kognitivnim radijem, adaptivnimi brezžičnimi komunikacijskimi sistemi in senzorskimi omrežji.

Carolina Fortuna je diplomirala leta 2006 iz telekomunikacijskega inženiringa na Univerzi v Cluj-Napoci v Romuniji. Od leta 2007 je kot mlada raziskovalka zaposlena na Odseku za komunikacijske sisteme Instituta "Jožef Stefan". Trenutno zaključuje doktorski študij na Mednarodni podiplomski šoli Jožefa Stefana na smeri Informacijsko komunikacijske tehnologije. Njeno raziskovalno delo sodi na področja kognitivnih, brezžičnih in senzorskih omrežij, strojnega učenja, semantičnih tehnologij in rudarjenja podatkov v telekomunikacijskih omrežjih.

Matevž Vučnik je diplomiral leta 2010 na Fakulteti za elektrotehniko Univerze v Ljubljani. Od leta 2010 je zaposlen na Odseku za komunikacijske sisteme Instituta "Jožef Stefan", na Mednarodni podiplomski šoli Jožefa Stefana pa je vpisan na tretjo stopnjo bolonjskega študija smer Informacijsko komunikacijske tehnologije. Raziskovalno se ukvarja s senzorskimi omrežji, predvsem s protokoli za njihovo integracijo v senzorski splet.

Marko Mihelin je diplomiral leta 2009 na Fakulteti za elektrotehniko Univerze v Ljubljani. Od leta 2010 sodeluje z Odsekom za komunikacijske sisteme Instituta "Jožef Stefan", na Fakulteti za elektrotehniko Univerze v Ljubljani pa je vpisan na tretjo stopnjo bolonjskega študija smer elektrotehnika. V okviru raziskovalnega dela se osredotoča na strojno učenje in razpoznavo močnostnih dogodkov v energetskem omrežju.

Mihael Mohorčič je višji znanstveni sodelavec in vodja Odseka za komunikacijske sisteme na Institutu "Jožef Stefan". Doktoriral je leta 2002 na Fakulteti za elektrotehniko Univerze v Ljubljani. Leta 2006 je bil na Mednarodni podiplomski šoli Jožefa Stefana izvoljen v naziv docent za predmetno področje "Telekomunikacije". Tam je tudi dopolnilno zaposlen in izvaja več predmetov na 2. in 3. stopnji bolonjskega študija. Njegovo raziskovalno delo sodi na področja satelitskih, stratosferskih, brezžičnih, kognitivnih in senzorskih omrežij.

Optimalno upravljanje električnih porabnikov v inteligentnem domu

Mark Umberger, Entia d. o. o., Iztok Humar, Fakulteta za elektrotehniko, Univerza v Ljubljani

Povzetek — Članek predstavlja pilotni projekt operaterskega koncepta inteligentnega doma in prve izkušnje o delovanju sistema v pasivni hiši. Gre za avtomatsko upravljanje procesov v bivalnem okolju s ciljem povečati udobje in varnost uporabnikov, omogočiti oddaljeno upravljanje preko internet omrežja in zagotoviti učinkovito rabo energije z optimalnim upravljanjem sistema za ogrevanje, hlajenje in prezračevanje, razsvetljave in naravne svetlobe z regulacijo senčil. Operaterski koncept delovanja sistema inteligentnega doma pa omogoča tudi optimalno upravljanje električnih porabnikov s ciljem zmanjšati konice v skupni porabi, omogočiti porabo električne energije v časovno optimalnih trenutkih in povečati porabo električne energije pridobljene iz obnovljivih virov energije. Dosedanje izkušnje o delovanju sistema v pasivni hiši dajejo izhodišča za nadaljnje dopolnitve pilotne projekta.

Ključne besede — inteligentni dom, operaterski koncept, konvergenca storitev, optimalno upravljanje električnih porabnikov

Abstract — The article presents the pilot project of the server side solution of smart home system and its first operational experience in the passive house. The proposed system enables the process control in the living environments with the goal to increase users comfort and security, to provide remote control via Internet and to enable energy savings by optimal control of heating, cooling and ventilation system, lighting system and awning system for daylighting. Server side solution of smart home also enable optimal control of all electricity consumers with the goal to decrease the picks in total consumption, to enable time shifting of operation of electrical devices and to increase the consumption from renewable energy. Current operation experiences with proposed smart home system in passive house gives a good starting point for further extensions of the pilot project.

Keywords — smart home, server side solution, optimal control of electricity consumers

I. UVOD

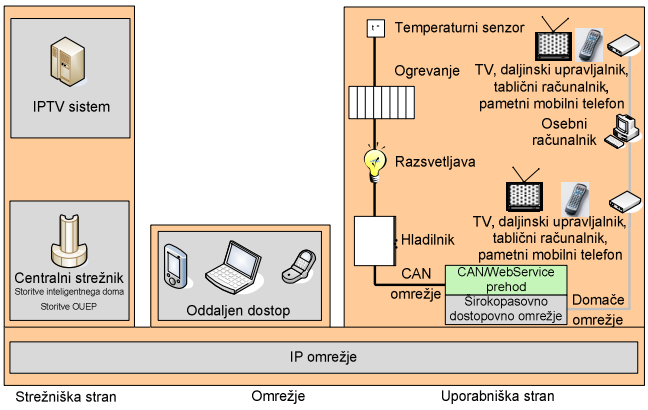
Z razvojem elektronskih elementov sistemi in storitve za upravljanje procesov v zgradbah (UPZ) počasi prehajajo iz industrijskega v uporabniški trg. Različne analize so pokazale, da bo večina bivalnih okolij v prihodnosti opremljenih s tovrstnimi sistemi [1]. Glavni nosilec njihovega razvoja je želja po povečanju udobja in varnosti uporabnikov zgradb, zagotoviti učinkovito rabo energije v zgradbah in omogočiti oddaljeno upravljanje z bivalnimi okolji preko internetnega omrežja [2]. Sistemi in storitve UPZ omogočajo povečano udobje s pomočjo optimalnega upravljanja bivalnih parametrov (npr. optimalna temperatura, osvetljenost in vlažnost v prostoru, itd.), večja varnost pa je zagotovljena s pomočjo proti požarnih in proti vlomnih sistemov. Pojem učinkovite rabe energije v zgradbah je danes izrednega pomena. Le to lahko zagotovimo s pomočjo bolj izpopolnjenih konceptov zgradb v smislu arhitekture in materialov (npr. tlorisi z majhnimi obodnimi površinami fasade, okna z majhnim faktorjem prevodnosti, večja količina izolacije itd.). V ta namen so se pojavili praktični primeri novozgrajenih zgradb, t.i. nizko energetskih oziroma pasivnih zgradb, ki po definiciji zagotavljajo porabo energije za ogrevanje in toplo vodo v višini cca. 50 kWh/m^{2}a na leto v primeru nizko energetske zgradbe oziroma cca. 15 kWh/m^{2}a na leto v primeru pasivne zgradbe [3]. Učinkovito rabo energije pa zagotavljajo tudi sistemi UPZ, ki omogočajo avtomatsko upravljanje procesov v zgradbah (npr. sistem za ogrevanje, hlajenje in prezračevanje, sistem zunanje in notranje razsvetljave, sistem senčil itd.) in so zaradi tega danes tudi sestavni del sodobne nizko energetske oziroma pasivne zgradbe [4], [5]. Poleg tega pa jih je mogoče uporabiti v novih zgradbah, kot tudi v obstoječih oziroma starejših zgradbah, kar še dodatno povečuje njihovo uporabnost. Z razvojem osebnih in tabličnih računalnikov ter pametnih mobilnih telefonov pa mora sodobno bivalno okolje omogočati tudi oddaljeno upravljanje preko internet omrežja, s čimer postane življenje v njih še bolj prijetno. Terminologija besedne zveze UPZ se je razvijala po korakih, zelo aktualna pa je tudi besedna zveza *inteligentni dom*, katero bomo tudi uporabljali v nadaljevanju.

V tem članku predstavljamo pilotni projekt operaterskega koncepta inteligentnega doma, ki omogoča avtomatsko upravljanje procesov v pasivni hiši s ciljem povečati udobje in varnost uporabnikov, omogočiti oddaljeno upravljanje preko internet omrežja in zagotoviti učinkovito rabo energije z optimalnim upravljanjem sistema za ogrevanje, hlajenje in prezračevanje, razsvetljave in naravne svetlobe z regulacijo senčil. Komunikacijska arhitektura, ki temelji na operaterskem principu delovanja, omogoča konvergenco storitev inteligentnega doma z storitvami internetne televizije [8], kot tudi konvergenco z storitvami za optimalno upravljanje električnih

porabnikov v domovih. Te storitve omogočajo zmanjšanje konic v skupni porabi, porabo električne energije v časovno optimalnih trenutkih in povečanje porabe električne energije pridobljene iz obnovljivih virov energije. V 2. poglavju članka najprej podrobno predstavimo konvergenčni arhitekturni model operaterskega koncepta inteligentnega doma ENTIAliving in v nadaljevanju izpostavimo uporabniške vmesnike, ki omogočajo interakcijo med uporabnikom in sistemom. V 3. poglavju predstavimo pilotni projekta operaterskega koncepta inteligentnega doma ENTIAliving v pasivni hiši, kjer so izpostavljene tudi praktične izkušnje z uporabo sistema.

II. KONVERGENČNI ARHITEKTURNI MODEL

Konvergenčni arhitekturni model sistema ENTIAliving, ki omogoča konvergenco storitev inteligentnega doma, internetne televizije in storitev za optimizacijo upravljanje električnih porabnikov (OUEP) prikazuje Slika 1 [6]. Sestavljen je iz strežniškega dela, omrežja in uporabniškega dela.



Slika 1: Konvergenčni arhitekturni model

Strežniški oziroma operaterski del vsebuje vso opremo, ki je potrebna za izvajanje vseh storitev, ki jih konvergenčni arhitekturni model zajema, kot sta centralni strežnik za storitve inteligentnega doma in za storitve OUEP in sistem IPTV. Centralni strežnik vsebuje spletni strežnik in podatkovno bazo. Naloga prvega je, da streže grafični uporabniški vmesnik, ter da ima implementirano celotno aplikacijsko logiko za izvajanje in nadzor storitev inteligentnega doma in storitev OUEP. Najbolj pomembna funkcija centralnega strežnika pa je, da omogoča integracijo storitev inteligentnega doma, storitev OUEP in storitev IPTV. To pa je mogoče doseči s pomočjo posebno zasnovanega in implementiranega programskega vmesnika, ki omogoča konvergenco vseh grafičnih uporabniških vmesnikov, ter z uporabo programskega vmesnika za komunikacijo s prehodom WebService/CAN, ki omogoča upravljanje in nadzor storitev inteligentnega doma na daljavo. Naloga sistema IPTV pa je, da omogoča predvajanje video - in avdio – vsebin na daljavo. Poleg tega sistem IPTV vsebuje še video kodirnik za prevajanje televizije v živo. Omrežje zagotavlja povezavo strežniškega dela z uporabniškim delom s pomočjo širokopasovnega dostopovnega omrežja. Poleg tega mora zagotavljati ustrezen nivo varnosti, zadovoljivo kakovost storitev, zaradi sistema IPTV pa mora zagotavljati tudi delovanje v načinu oddajanje večjemu številu prejemnikov (angl. multicast). Kot vidimo na Sliki 1, je konvergenčni arhitekturni model zasnovan na operaterskem pristopu izvajanja storitev, katerega glavna prednost se kaže v centralnem nadzoru in upravljanju konvergenčnega sistema in v zmožnosti dodatnih integracij različnih zunanjih storitev ter v zmožnosti različnih posodabljanj z enega, centralnega mesta s strani operaterja. Uporabniški del vključuje sistem inteligentnega doma, prehod in uporabniške vmesnike. Sistem inteligentnega doma sestavljajo različne naprave (senzorji in krmilniki), katerih funkcija je samodejno upravljanje različnih procesov (npr. ogrevanje, hlajenje, razsvetljava, senčila, itd.) in scenarijev (npr. luči 70 %, ogrevanje 23 ºC itd.). Glavna naloga prehoda je, da storitvam inteligentnega doma, ki delujejo na osnovi standarda CAN, omogoča dvosmerno komunikacijo z oddaljenim centralnim strežnikom z uporabo omrežnih tehnologij TCP/IP. Glavna naloga uporabniških vmesnikov je zagotoviti uporabniku možnost upravljanja in nadzora nad vsemi storitvami, ki jih predlagan konvergenčni arhitekturni model zagotavlja.

A. Uporabniški vmesniki

Sistem ENTIAliving uporabnikom omogoča ročno upravljanje bivalnih okolij s pomočjo različnih uporabniških vmesnikov. Le ti morajo biti čim bolj enostavni za uporabo, zato je za uporabnike najbolj pomemben parameter kakovost uporabniške izkušnje (angl. quality of experience) [7]. Zaradi tega dejstva ENTIAliving omogoča upravljanje bivalnih okolij s pomočjo uporabniških vmesnikov, ki zagotavljajo najvišji nivo kakovosti uporabniške izkušnje. Uporabniške vmesnike sistema ENTIAliving prikazuje Slika 2.

Slika 2: Uporabniški vmesniki sistema ENTIAliving

III. IMPLEMENTACIJA PILOTNEGA PROJEKTA ENTIALIVING V PASIVNI HIŠI

Pilotni projekt sistema ENTIAliving v pasivni hiši omogoča avtomatsko upravljanje sledečih procesov:

– ogrevanje, hlajenje in prezračevanje
– senčila
– razsvetljava
– varnostni sistem

Pasivna hiša, v kateri je implementiran sistem ENTIAliving, ima za potrebe ogrevanja, hlajenja in prezračevanja nameščeno toplotno črpalko tipa zrak-zrak, ki zagotavlja dovajanje in odvajanje toplega oziroma hladnega zraka v posamezne prostore. Sistem za ogrevanje, hlajenje in prezračevanje ima nameščen tudi rekuperator zraka, ki omogoča segrevanje oziramo hlajenje dovodnega svežega zraka s pomočjo odvodnega odpadnega zraka. Celotna moč toplotne črpalke znaša 1 kW. Toplotna črpalka torej v zimskem času omogoča ogrevanje prostorov, v letnem času pa omogoča hlajenje prostorov. Sistem ENTIAliving pa omogoča avtomatsko upravljanje loput, ki zagotavljajo nadzor nad pretokom zraka v posameznem dovodnem oziroma odvodnem kanalu. Na ta način je mogoče nastaviti temperaturo v vsakem prostoru posebej. Prav tako pa sistem ENTIAliving omogoča avtomatsko zapiranje posamezne lopute v primeru odprtega okna v prostoru, kar bistveno pripomore k učinkoviti rabi energije. Za potrebe ogrevanja pa ima pasivna hiša nameščena tudi dva električna radiatorja moči 700 W, ki v primeru zunanje temperature pod -15 °C omogočata zadovoljivo ogrevanje pasivne hiše. Sistem ENTIAliving tako omogoča avtomatski vklop električnih radiatorjev v primeru, ko temperatura v prostorih pade pod 19 °C. Pasivna hiša ima na južni strani velike steklene površine z namenom segrevanja prostorov v zimskem času s pomočjo sončne energije. V letnem času pa je izredno pomembno, da se pasivna hiša zaradi velikih steklenih površin ne pregreje, zato mora imeti nameščena kakovostna senčila z avtomatskim upravljanjem, kar je prikazano na Sliki 3. Sistem ENTIAliving v pasivni hiši tako omogoča avtomatsko upravljanje senčil, s čimer se senčila v letnem času v primeru sončnega sevanja avtomatsko spustijo. Ravno obratno delovanje pa je omogočeno v zimskem času, ko se senčila avtomatsko dvignejo v primeru sončnega sevanja, s čimer je omogočeno segrevanje prostorov s pomočjo sonca. S tem pa je zagotovljena tudi optimalna regulacija naravne svetlobe v posameznih prostorih, kar ima izredno pozitiven učinek na udobje bivanja. Praktična izkušnja kaže, da se v zimskem času prostori segrejejo tudi do 3 °C v 1 h, kar kaže na smiselnost velikih steklenih površin na južni strani pasivne hiše. Prav tako pa sistem ENTIAliving samodejno zazna sunke vetra, ki lahko senčila močno poškodujejo. V tem primeru se senčila avtomatsko dvignejo.

Slika 3: Senčenje pasivne hiše

Pri razsvetljavi v pasivni hiši je izredno pomembno, da deluje zgolj takrat, ko je nujno potrebna, saj ima pasivna hiša tako majhno porabo električne energije, da lahko že majhno prekomerno delovanje razsvetljave pomeni bistveno večjo porabo električne energije celotne pasivne hiše. Zaradi tega dejstva ENTIAliving omogoča avtomatsko upravljanje razsvetljave v prostorih glede na jakost zunanje in notranje svetlobe in prisotnost uporabnikov. Na ta način se luči začnejo prižigati takrat, ko notranja in zunanja razsvetljava nista več zadovoljivi, prav tako pa se luči avtomatsko ugasnejo v primeru odsotnosti uporabnikov v posameznem prostoru. S pomočjo sistema ENTIAliving je mogoče razsvetljavo upravljati zvezno in diskretno. Pri zveznem upravljanju je mogoče posamezno luč nastaviti na poljubno vrednost v razponu med 0 % in 100 %. Prav tako pa se luči v vseh prostorih avtomatsko ugasnejo, ko uporabniki zapustijo hišo. Sestavni del vsakega sodobnega bivalnega okolja pa je tudi učinkovit varnostni sistem, ki mora zagotavljati varovanje pred nezaželenimi in pa tudi veliko krat nevarnimi vlomi, kot tudi varovanje pred požarom in poplavami. Zaradi teh dejstev sistem ENTIAliving omogoča varovanje pred vlomi s pomočjo nameščenih senzorjev prisotnosti in senzorjev, ki zaznajo razbitje steklenih površin v oknih. Prav tako pa ENTIAliving s pomočjo senzorjev dima omogoča hitro zaznavanje požara in s pomočjo senzorjev za razlitje vode zaznavanje poplave. S pomočjo nadzora nad močnostnimi vtičnicami pa sistem ENTIAliving omogoča tudi nadzor nad likalnikom in pečico v bivalnem okolju. Na ta način nam ni več potrebno skrbeti ali smo ugasnili likalnik oziroma pečico, ampak lahko leto preverimo preko mobilnega telefona oziroma se leta ugasne avtomatsko.

Sistem ENTIAliving pa omogoča tudi medsebojno delovanje med različnimi procesi. V ta namen omogoča izvajanje različnih pred nastavljenih scenarijev, kjer lahko uporabnik s pritiskom na tipko sproži izvajanje različnih procesov (npr. s pritiskom na scenarij »večer« se vklopi razsvetljava v dnevni sobi na 30 %, razsvetljava na vrtu in bazenu se vklopi na 100 %, senčila se dvignejo in temperatura v dnevni sobi se

poviša na 23 °C). Uporabnik pa lahko scenarije sproži s pomočjo nameščenih sobnih upravljalnikov, ki se nahajajo v vsaki sobi posebej, s pomočjo »pametnih« mobilnih telefonov ali s pomočjo tabličnih računalnikov.

IV. ZAKLJUČEK

V članku smo podrobno predstavili pilotni projekt operaterskega koncepta pametnega doma ENTIAliving v pasivni hiše, kjer sistem omogoča avtomatsko upravljanje procesov v bivalnem okolju s ciljem povečati udobje in varnost uporabnikov, omogočiti oddaljeno upravljanje preko internet omrežja in zagotoviti učinkovito rabo energije z optimalnim upravljanjem sistema za ogrevanje, hlajenje in prezračevanje, razsvetljave in naravne svetlobe z regulacijo senčil. Praktične izkušnje so pokazale, da mora biti sistem za avtomatsko upravljanje procesov v bivalnih okoljih sestavni del vsake pasivne hiše, saj brez njega ni mogoče doseči predvidene porabe energije, kot tudi ni mogoče zagotoviti udobnega bivalnega okolja v letnem času. V prihodnosti je mogoče pričakovati [8], da bodo operaterski koncept inteligentnega doma začeli uvajati različni ponudniki internetnih storitev in storitev Internetne televizije[9]. Na ta način bodo začeli uvajati storitve inteligentnega doma, kar bo bistveno izboljšalo njihov konkurenčen položaj na trgu. Prav tako pa bodo operaterski koncept inteligentnega doma začela uvajati različna podjetja, ki se ukvarjajo z proizvodnjo ali distribucijo električne energije. Na ta način bo mogoče optimalno upravljati različne porabnike električne energije, s ciljem zmanjšati konice v skupni porabi, omogočiti porabo električne energije v časovno optimalnih trenutkih in povečati porabo električne energije, pridobljene iz obnovljivih virov energije.

LITERATURA

[1] A. Z. Alkar, U. Buhur. An internet based wireless home automation system for multifunctional devices, IEEE Consumer Electronics 4 (2005) 1169-1174.

[2] H. Merz, T. Hansemann, C. Hubner, Building automation, Communication systems with Konnex, LON and BACnet, Germany: Springer Berlin Heidelberg (2009).

[3] M. Felkner, Possibilities for Economization in Buildings Renovation Using Passive House Components, Eleventh international conference on passive houses, 2007.

[4] G. Wood, M. Newborough, Energy-use information transfer for intelligent homes: enabling energy conservation with central and local displays, Energy and Buildings, 4 (2007) 495-503.

[5] C. P. Baumeister, Building Automation in the Passive House, Eleventh international conference on passive houses, 2007.

[6] M. Umberger, Arhitekturni model in metode konvergence storitev upravljanja procesov in internetne televizije, doktorska disertacija, 2010.

[7] M. Umberger, S. Lumbar, I. Humar, Modeling the network delay on user experience in distributed home-automation networks, Information systems Frontiers, 2010.

[8] M. Umberger, I. Humar, A. Kos, J. Guna, A. Žemva, J. Bešter, The integration of home-automation and IPTV system and services, Computer Standards and Interfaces 4 (2009) 675-684.

[9] RWESmarthome, http://www.rwe-smarthome.de/web/cms/de/448330/smarthome, April 2011.

Petek, 13. maj 2011

Building the Internet of Things

Jari Arkko, Ericsson Research

Abstract — Everything that benefits from networking will eventually be connected. This is the basis for the interest in the "Internet of Things", a reason why many research projects exist, why a large number of standards bodies want to build standards for it, and why there is a lot of commercial activity. However, on some areas, the Internet of Things pushes the limits of the current Internet. The Internet will evolve to meet the demand, as it has done in previous occasions. This paper argues that this evolution is more about enabling interoperability than about developing new technology. Most of the communications technology for creating the Internet of Things already exists, and the pain points are elsewhere.

Keywords — Internet of Things, interoperability

I. INTRODUCTION

A key feature of the Internet is that different devices can work together: any browser works with any web server, almost all content is viewable by all devices, any device can plug into a home router, different networks can exchange routing information with each other, and so on. As the Internet has evolved, *interoperability* has always been a major concern, in terms of protocol design and extensibility, building products that in practice work well together with other devices, and setting standards.

In general, today's Internet builds on a key set of protocols that work extremely well between different types of devices and in varying types of networks: IP itself, TCP, DHCP, DNS, HTTP, TLS, HTML, XML, and so on. But in many cases there are still some components in the protocol stack that are proprietary, application-specific, available for limited platforms, or come from a single source. For instance, specific link layer technologies, content formats (Flash), or applications (Skype). This shows that it is important to balance the need for an interoperable Internet with the need to allow commercial innovation. Still, it is expected that over time, generally interesting components become available for all devices that need them.

This paper argues that we already have most of the technology that we need for building the Internet of Things, and that the problem is not so much about lack of technology but rather how to ensure that different pieces of equipment can work well together.

Section II discusses some of the existing technology that we believe is a key for building the Internet of Things. The rest of the paper discusses the concern of interoperability. Section III introduces the basic problem of a capability mismatch: how a small sensor may not be capable of using the same communication protocols as a full-fledged Internet host. Sections IV through VI highlight certain specific issues such as the need for interoperability at a semantic level. Finally, Section VII concludes with some recommendations on how these concerns can be alleviated.

I. TECHNOLOGY FOR THINGS

There are many research proposals, ongoing projects, and standardization efforts in this area. It is perhaps important to emphasize that this does not mean we have to wait for the completion of all this work before we can start deploying our Internet of Things networks. Some of the ongoing work addresses important requirements in specific situations, some brings interoperability where we previously had none, some develops useful optimizations, some is interesting research, and some is merely exploring new designs.

But if we just look at what is already being deployed in real-life, it becomes clear that to a large extent, the Internet of Things technology is already here. In 2004, the utility company that provides energy for my house gave me a meter that uses cellular modem to upload information to a server in real-time. This was a standard solution for all new subscribers in Finland already back then. Going beyond the personal and national anecdote, the industry by and large is already deploying this technology. Utility companies with millions of metering devices, service companies with innovative ideas, health and sport related devices (weight scales that employ wireless LAN, for instance), e-book readers, tablets, cameras, and other gadgets with network connectivity, traffic applications that employ communications and positioning technology, building and surveillance solutions that run on top of IP, gateways that link legacy networks to the Internet, and so on.

Some of the key tools in the Internet of Things toolbox include:

– IP – including IPv6. It will also be necessary use the various mappings how IP runs over particular link

layers (such as 6LOWPAN [1]). We also need the necessary tools that allow IPv6-based Things to communicate over legacy IPv4 networks (such as NAT64 [2]).
– Basic web technology: TCP, HTTP, HTML, XML. While as not optimized as some newer solutions, this is very easy to use, efficient when properly used, and guaranteed to pass through any home gateway firewall.
– Link layer technology such as cellular, wireless LAN, and ZigBee.
– User interfaces based on the web, and in some cases on SMS, e-mail, chat, or social media interfaces.

A more in-depth discussion of the available Internet protocol tools can be found in [3].

II. INTEROPERABILITY

Today's Internet is primarily characterized by applications with a human in the loop. A successful Internet application is one where the desired human experience is achieved. For instance, the desired visual effect is correctly rendered on screen. This makes interoperability a bit easier, as the humans are responsible for processing the "semantic" part of the communications. Today's Internet also consists of a relatively homogeneous set of devices. While there are differences between a smartphone, a laptop, and a high-end server, for instance, they are all still high power computing devices.

Some of the requirements and expected usage patterns in the Internet of Things will cause interoperability challenges. For instance, there is

– a capability mismatch between traditional Internet hosts and small devices,
– widely differing communication and processing bandwidths in different devices,
– needs for interoperability at a semantic level,
– different internetworking protocol choices (legacy vs. IP vs. IPv6), and
– solutions that are suitable for only some networks.

The two first items are a key problem. The desire to build large numbers of small, battery-operated, and inexpensive devices drives the need for simple solutions. Often these devices are not easily software upgradable, and their protocol and application suite is limited. Some of the typical limitations include:

– MTU limitations,
– simplified web protocols (COAP/UDP [4] instead of HTTP/TCP),
– single-stack instead of dual-stack,
– limited or no support for security that would be suitable for operation over the Internet,
– sleep schedule that does not allow for communication at all times,
– and so on.

These limitations would have no effect if the device only communicated to other similar devices, but they do have an effect when attempting to provide *Internet-wide interoperability* to such devices. For instance, clients that today employ HTTP would be unable to communicate with such a device. We believe that Internet-wide interoperability is required, as the system of connected devices usually consists of sensors, actuators, user interfaces, servers, and other components. Many of these components are expected to be devices in the traditional Internet. For instance, it is likely that computers and smartphones are used as the user interface for controlling many Internet of Things applications.

It is important to note that some of the capacity requirements would preclude direct communication to an Internet of Things device even if implemented exactly the same protocol stack as other devices in the Internet. For instance, a sensor whose value is interesting to a large audience may not be able to accommodate all requests.

III. SEMANTIC INTEROPERABILITY

Most Internet applications designed for humans often require only transport of data from one place to another, and an accurate rending of that data on the screen. It is not necessary to process or understand the data in any semantic manner.

Much of the current focus in the Internet of Things is also on the lower parts of the stack: designing the wireless networks, running IPv6 over them, getting routing to work, and using UDP/TCP and COAP/HTTP.

It is important to realize that this is **not** enough for true interoperability. For instance, it would not be enough for a light switch from one vendor to control lights from another. For true interoperability we need *semantic interoperability*, the ability of the devices to understand what the data they communicate **means**. Most often this would imply standardizing not just the protocols and data formats, but also the meaning of the data, e.g., that "1" in a particular field means that the light should be switched on. Standardizing the meanings is difficult and time consuming, however. It has to be done on a per-application basis and with application specific expertise.

There are of course different ways of achieving semantic interoperability. This does not always involve standards. Devices could accept program code that performs the required actions. For instance, a light switch might accept a program fragment from a light bulb to run the user interface necessary to control the light. This is similar to how Flash-based applications can support new video codecs without requiring support from the browser or any Internet-wide agreement about the new coding format. It remains to be seen if programmable control models become popular in the Internet of Things.

Nevertheless, there should be some way for the light switch and the light bulb to agree how the lights are turned on. This is not to say that there is no benefit from an Internet of Things without it. There will always be a need for some proprietary or leading edge, non-standard communications. And even if none of the application layer communications would interoperate with each other, we would still have a common backbone for the Internet of things, consisting of the IP layer, routing, COAP/HTTP proxies, and so on. We call this the *Internet of Things transport network*. This would be tremendously valuable. But it would not enable an Internet of Things where any light works with any switch or any energy meter works with any provider's server.

IV. AUTHORIZED INTEROPERABILITY

There are a number of security related challenges as well. Many of these fall into the capabilities category. But there is another, more fundamental issue. It is not enough that two endpoints support the same security mechanisms. The communicating parties also have to share some type of relationship that allows them to *authenticate* each other and *authorize* whatever actions are taking place. There are many ways to implement this, for instance with shared secrets, trusted third parties, or certificate infrastructures. It is relatively straightforward to set this up in small networks or within a single organization. Setting this up in a larger scale or in situations that require multiple participating organizations is going to be harder. For instance, home owners, manufacturers, and electricity utility companies might all want to control a particular home appliance.

V. NETWORK-SPECIFIC SOLUTIONS

The Internet of Things is pushing the limits of technology in many areas. As we approach those limits we need to apply optimizations and design techniques to make our technical solutions feasible. But at the same time this may make our solutions less general than we would wish. For instance, the RPL routing protocol [5] has two modes optimized for different types of networks. Those modes are necessary, because without them it is not possible to support some important applications. However, the modes are incompatible and highly optimized implementations are unlikely to support both. As a result, interoperability is not assured merely through the use of the same protocol. Note that while we use the two modes from RPL as an example, many similar issues exist elsewhere as well (different header compression types in 6LOWPAN [6], XML vs. JSON vs. binary XML for sensor data, and so on).

VI. CONCLUSIONS

Employing IP (and IPv6 in particular) for the Internet of Things is a necessary step. However, it is only the first step in ensuring a truly useful Internet of Things where different objects seamlessly communicate with each other. Some of the key areas where further work is needed include, for instance, standardization of application specific messages and semantics, and ensuring that each individual protocol specification is interoperable in all situations.

Looking back at the development of the Internet, one of the lessons that we can draw from it is to ensure that we have sufficiently general mechanisms that address most needs. Highly optimized and specialized solutions have rarely succeeded. Robustness and generality are often more important than mere performance. Based on this it is likely that most networks will actually employ pretty much standard Internet technology as we already know it today: IP, web protocols, and existing link layers. We need to be careful about spending too much effort in optimizations with narrow usability. Achieving interoperability has been a far more important success criteria for the Internet, and this is where we should spend our future efforts.

REFERENCES

[1] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler. Transmission of IPv6 Packets over IEEE 802.15.4 Networks. RFC 4944, IETF, September, 2007.

[2] F. Baker, X. Li, C. Bao, K. Yin. Framework for IPv4/IPv6 Translation. Internet Draft draft-ietf-behave-v6v4-framework (work in progress), IETF, August, 2010.

[3] F. Baker, D. Meyer. Internet Protocols for the Smart Grid. Internet Draft draft-baker-ietf-core (work in progress), IETF, March, 2011.

[4] Z. Shelby, K. Hartke, C. Bormann, B. Frank. Constrained Application Protocol (CoAP). Internet Draft draft-ietf-core-coap (work in progress), IETF, March 2011.

[5] T. Winter, P. Thubert, A. Brandt, T. Clausen, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, JP. Vasseur. RPL: IPv6 Routing Protocol for Low power and Lossy Networks. Internet Draft draft-ietf-roll-rpl (work in progress), IETF, March 2011.

[6] J. Hui, P. Thubert. Compression Format for IPv6 Datagrams in Low Power and Lossy Networks (6LoWPAN). Internet Draft draft-ietf-6lowpan-hc (work in progress), IETF, February, 2011.

Jari Arkko is a researcher with Ericsson Research in Jorvas, Finland. He serves currently also as one of the Area Directors at the Internet Engineering Task Force (IETF). His main interests include Internet Architecture, IPv6, the Internet of Things, and social media. He frequently communicates with his toaster on Facebook.

Uporabnost omrežij »Metro Wi-Fi« za »Internet stvari«

Rudolf Sušnik, Mobitel, d. d., Jure Sodja, Telekom Slovenije, d. d.

Povzetek — Tehnologija brezžičnih lokalnih omrežij po standardu IEEE 802.11 je poznana že dolgo, uveljavila se je zlasti za pokrivanje notranjosti zgradb v poslovnih in domačih okoljih. Z uvajanjem pristopa »mesh« omrežja, tehnologija v zadnjem času dobiva nov zagon zlasti s storitvami »3G offload« in »Metro Wi-Fi«, kar posledično omogoča tudi storitve interneta stvari. Da tehnologija postaja resen »igralec«, napovedujejo tudi vodilni proizvajalci z napovedmi o opremi Wi-Fi operaterskega nivoja (t. i. carrier grade).

Ključne besede — Metro Wi-Fi, mesh, IEEE 802.11, WLAN, WMAN

Abstract — Wireless technology IEEE 802.11 has been well-known for several years now. The Wi-Fi networks are mostly deployed indoor at enterprise and home users. However, introducing mesh paradigm into Wi-Fi gave new rise to the technology. Nowadays, the most known services built up with mesh outdoor equipment are "3G offload" and "Metro Wi-Fi", which in turn, together with "smart city" paradigm makes also opportunities for internet of things. In this article, we would like to introduce our findings of testing mesh Wi-Fi equipment of four prominent vendors. At the time, all equipment tested was in beta phase. However, all vendors claim their equipment is just about to be carrier grade. In some aspects we can agree to them.

Keywords — Metro Wi-Fi, mesh, IEEE 802.11, WLAN, WMAN

I. UVOD

Tehnologija brezžičnih lokalnih omrežij, združena v družini standardov IEEE 802.11 [1] in poimenovana kot WLAN (angl. Wireless Local Area Network) ali Wi-Fi (angl. Wireless Fidelity) ima že kar dolgo zgodovino. Začetki tehnologije segajo vse do leta 1985, ko je ameriški urad za komunikacije FCC (Federal Communications Commision) deklariral nelicencirano frekvenčno področje imenovano ISM pas (Industiral, Scientific and Medical radio bands). Prvi standard 802.11 je bil izdan v letu 1997. Ta standard je predvideval komunikacije v ISM pasu 2.4 GHz z uporabo 20 MHz kanalov in bitnimi hitrostmi 1 ali 2 Mbit/s.

Od začetkov pa do danes je tehnologija doživela izjemen razvoj. Kmalu po prelomu tisočletja, s standardoma 802.11a in 802.11b, so se pojavile prve poslovne pobude v smislu javnih omrežij Wi-Fi. Mobilna omrežja so v tem času namreč ponujala še precej počasen prenos podatkov, predvsem pa prenos podatkov ni bil niti slučajno poceni. Ideja javnih omrežij Wi-Fi se je razširila vse do te mere, da imamo podobno kot v mobilnih omrežjih tudi v omrežjih Wi-Fi, t.i. roaming agregatorje, in s tem z enim uporabniškim računom/identiteto možnost gostovanja v omrežjih Wi-Fi po celem svetu. Pobudi javnih omrežij Wi-Fi je sledila tudi Skupina Telekom Slovenije s prvim javnim slovenskim omrežjem Wi-Fi NeoWLAN [2], ki je bilo v sodelovanju s Fakulteto za elektrotehniko razvito na Mobitelu in SiOL-u ter predano v uporabo spomladi leta 2003.

Sočasno z razvojem javnih omrežij Wi-Fi, se je tehnologija širila v poslovnih okoljih (angl. enterprise), v zadnjih letih pa se je zaradi cenovne dostopnosti močno razširila tudi med domačimi uporabniki.

V Sloveniji sicer javna (plačljiva) omrežja Wi-Fi niso najbolj uspešno zaživela, česar pa širše, tj. vsaj v evropskem merilu, ni mogoče na splošno trditi [3]. Ne glede na vse to, se nam nakazuje »nova doba« omrežij Wi-Fi. Ta ne bodo več lokalno omejena, pač pa bo to evolucija omrežij WLAN v omrežja WMAN (Wireless Metro Area Network) [4]. Razlogov za to evolucijo je več, naštejmo le nekaj glavnih:

- poceni tehnologija je povzročila izjemen razmah naprav, opremljenih z vmesniki Wi-Fi, na trgu skoraj ni več mobilnega telefona, ki ne bi imel vgrajenega vmesnika Wi-Fi;
- razmah t. i. pametnih telefonov in socialnih omrežij, ki zahtevajo non-stop podatkovno povezljivost;
- razvoj tehnologije 802.11 in s tem njena zanesljivost sta napredovala do nivoja, ki ga lahko že razglasimo za nivo operaterske tehnologije (angl. carrier grade) [5], hkrati pa je še vedno cenejša od mobilne tehnologije (HSPA, LTE);
- na gosto naseljenih področjih je vlaganje v razširitev zmogljivosti mobilne podatkovne tehnologije lahko zelo drago;
- večja mesta vse več vlagajo tudi v brezžično komunikacijsko infrastrukturo in s tem postajajo konkurenca aktualnim operaterjem (npr. Ljubljana [6]).

Vidimo torej, da obstaja precej razlogov, da utegne tehnologija Wi-Fi postati pomemben dejavnik na področju mobilnih komunikacij, s tem pa se

neposredno dotika tudi interneta stvari o čemer se sprašujemo in iščemo odgovore v nadaljevanju tega prispevka.

II. METRO WI-FI IN »INTERNET STVARI«

Z množičnim uvajanjem omrežij Wi-Fi so se začele pojavljati tudi ideje o uporabi te tehnologije za pokrivanje zunanjih površin v mestih – Metro Wi-Fi. Ker tehnologija Wi-Fi deluje v nelicenciranem frekvenčnem spektru, z omejeno močjo in posledično omejenim dosegom pokrivanja (cca. 100 m), je šel razvoj za potrebe zunanjih postavitev v smer t .i. mesh omrežij, s čimer se gradnja omrežij tipa Metro Wi-Fi bistveno poenostavi in poceni.

V svetu najdemo kar nekaj Metro Wi-Fi postavitev, večinoma so z Wi-Fi pokriti le posamezni deli mest (npr. Maribor, Pariz, Minneapolis), ponekod celotna mesta (npr. Austin). Poznanih je tudi več primerov kjer so ugotovili, da omrežje Metro Wi-Fi ne dosega želenih ciljev, npr. Dublin, Portland, Sydney, Chicago. Vzroki neuspeha so bolj ali manj ekonomske narave, tudi tam, kjer je uradna razlaga, da je vzrok neuspeha tehnološki, je v ozadju ekonomski vzrok – zaradi slabo načrtovanega pokrivanja je kakovost storitev neustrezna, za zadostno pokritost pa bi povečan strošek investicije »podrl« finančno konstrukcijo (npr. Portland).

Eno od gonil omrežij Metro Wi-Fi je iniciativa »Smart city«, ki zagovarja in vzpodbuja idejo, da so komunikacijska in informacijska infrastruktura ter storitve velikega pomena za prihodnost [7]. V tej iniciativi najdemo stično točko z internetom stvari – storitve pametnih mest vključujejo komunikacije med ljudmi, med ljudmi in napravami ter med napravami samimi. Tako med najbolj obetavnimi storitvami pametnih mest najdemo:

- odčitavanje števcev (voda, elektrika, plin …);
- krmiljenje javne razsvetljave;
- upravljanje cestnih prometnih tokov (štetje prometa, krmiljenje semaforjev, nadzor voznikov);
- storitve za javne službe (gasilci, reševalci, policija);
- nadzor javnih površin, mirujočega prometa, črnih odlagališč;
- storitve za prebivalce (e-uprava, e-zdravje, turistične informacije …);
- itd.

Večino teh storitev sicer lahko že danes uspešno realiziramo v mobilnem omrežju, vendar tak pristop lahko prinese precejšnje stroške, zato večina pomembnejših »igralcev« vidi rešitev v tehnologiji Wi-Fi. Težava mobilnih podatkovnih omrežij je v tem trenutku vezana predvsem na gosto naseljena območja (velemesta), kjer stalno povečevanje števila pametnih telefonov dosega ali celo presega kapacitete omrežja. Težava niti ni toliko v pasovnih širinah kot v številu sočasnih povezav, širjenje kapacitet pa je drago (licence) ali celo nemogoče (lokacije in gradbena dovoljenja). Obstoječa storitev v tej smeri je t. i. storitev »3G offload« [8]. Treba je upoštevati, da z Wi-Fi signalom ne prodremo v notranjost stavb, kar pri mobilnem radijskem signalu ni težava. Seveda ni izključeno niti to, da gre pri vsej Wi-Fi pobudi zgolj za (kratkoročno) premostitev ali celo špekulacijo.

III. TESTIRANJE NAPRAV WI-FI

Vsako mobilno omrežje deluje zadovoljivo le, če zagotavlja ustrezno pokritost z radijskim signalom. Glede na to, da je radijski domet tehnologije Wi-Fi relativno majhen (cca. 100 m), je potrebno zagotoviti dokaj veliko število dostopovnih točk (angl. Access Point, AP) na enoto površine – na odprtem terenu pribl. 40/km^2, v arhitektonsko zapletenejših urbanih okoljih tudi mnogokratnik tega števila.

Pri tako velikem številu dostopovnih točk v omrežju se izvedljivost bistveno poenostavi z uporabo tehnologije »mesh« (IEEE 802.11s), kjer je vsakemu AP sicer potrebno zagotoviti električno napajanje, ne pa tudi kabla za omrežno povezljivost – ta je rešena s prenosom Wi-Fi med sosednjimi AP-ji. Vsak AP ima tako vgrajena vsaj dva radijska modula (en za uporabniški dostop, drugi za povezovanje s sosednjimi AP-ji), zato je oprema mesh dražja od ne-mesh opreme.

A. Testni parametri

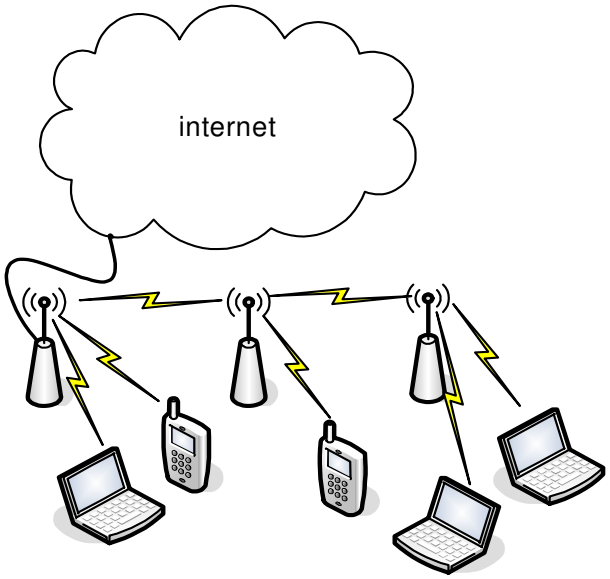
Pri testiranju opreme smo v smislu zagotavljanja mobilnosti in uporabnosti omrežja Wi-Fi za »internet stvari« iskali odgovore na več vprašanj:

- možnost gradnje omrežja mesh in število dostopovnih točk, ki jih je mogoče zaporedno povezati prek radia (t. i. »hop« število);
- bitni pretoki v omrežju mesh (uporabniški dostop in hrbtenica);
- pokritost oz. domet dostopovnih točk;
- delovanje v različnih frekvenčnih področjih (2.4 GHz oz. 5 GHz);
- zagotavljanje kvalitete storitve (QoS) v omrežju (za potrebe npr. video in VoIP-prometa);
- zagotavljanje varnosti v omrežju;
- mobilnost uporabnikov med dostopovnimi točkami istega omrežja;
- (samodejno) prilagajanje motnjam v okolici;
- nadzor in upravljanje omrežja;
- fizične in montažne karakteristike opreme.

Na testu smo imeli opremo štirih različnih proizvajalcev, opremo vsakega posameznega proizvajalca smo preizkušali ločeno.

B. *Metode in merilni pripomočki*

Za preizkušanje smo v centru Ljubljane postavili testno okolje, ki naj bi bilo čim boljši približek stanja, ki ga lahko v realnih razmerah pričakujemo za omrežje Metro Wi-Fi. Med pomembnejšimi parametri okolice je število motilnih dostopovnih točk Wi-Fi, ki smo jih na delu področja testnega poligona zaznali preko 300.



Slika 1: Prikaz zasnove testnega poligona – glavna dostopovna točka (root AP), ki je z optično povezavo povezana v internet ter dve dostopovni točki (mesh AP), ki imata dostop v internet zagotovljen z radijsko povezavo preko root AP.

Shema testnega poligona je prikazana na sliki 1. V omrežjih vrst mesh imamo opravka z dvema vrstama dostopovnih točk:

– root AP: dostopovna točka, ki je žično (optični ali kovinski vodnik) povezana v internet ter poleg svojega uporabniškega prometa nudi prehod v internet prometu mesh-točk;
– mesh AP: dostopovna točka preko katere se povezujejo uporabniki, dostop v internet pa zagotavlja z radijsko povezavo preko root AP, pri čemer je lahko vsak mesh AP »repetitor« prometa drugega mesh AP.

Testna postavitev je obsegala en root AP in dva zaporedno povezana mesh AP-ja. Razdaja med root AP in prvim mesh AP je znašala 200 m, med obema mesh AP-jema pa 150 m. Razdalja med AP-ji med katerimi vzpostavljamo hrbtenične povezave, je lahko večja kot med AP in odjemalcem (prenosnik, pametni telefon) predvsem zaradi boljših lastnosti anten. Nekatere sodobnejše antenske izvedbe omogočajo fokusiranje radijskega žarka, t.i. beam-forming, in s tem učinkovitejši prenos (zmanjšan vpliv motilnih signalov).

Za praktično uporabo omrežja je glavni podatek uporabniška izkušnja – kot uporabniške testne terminale smo uporabljali različne odjemalce Wi-Fi: Intel in Cisco Linksys na prenosnih računalnikih ter mobilnike HTC, Nokia, Sony-Ericsson in Samsung. Pri povezljivosti uporabniških klientov smo preizkušali standarda 802.11g in 802.11n. Standard IEEE 802.11n je zgrajen na antenski tehnologiji MIMO (Multiple Input, Multiple Output) [9] in zato mogoča precej višje prenosne hitrosti, kot npr. 802.11g. Standard je relativno nov, zato v vseh preizkušenih dostopovnih točkah ni vedno ustrezno deloval, je pa prav gotovo podpora temu standardu obvezna za vsako nastajajoče omrežje Metro Wi-Fi. Hitrost prenosa smo merili z aplikacijama ZAP in iPERF.

Zaradi omejenega števila testnih odjemalcev v večini primerov nismo mogli natančno izmeriti, koliko sočasnih povezav lahko hkrati servisira ena dostopovna točka, zato smo ločeno merili še zmogljivost hrbtenične radijske povezave med dvema mesh AP-jema oz. med mesh AP in root AP.

Zagotavljanje kvalitete storitve (QoS) je pomemben dejavnik, če želimo zagotoviti neko minimalno prenosno hitrost vsakemu uporabniku, ki je povezan v omrežje. Ker je tak scenarij najbolj pogost pri telefoniji in video prometu, smo funkcionalnost testirali s pretočnim videom in VoIP-telefonijo, kjer smo hkrati preizkusili še mobilnost med dostopovnimi točkami.

Poleg omenjenih ZAP in iPERF smo za potrebe video testov uporabljali odjemalca VLC, za potrebe VoIP testov pa Mobitelovo storitev Komunikator [10].

IV. REZULTATI

Zmogljivosti omrežja za uporabniški promet smo merili v okolici vsake od treh dostopovnih točk. V okolici vsake AP smo si na različnih oddaljenostih od AP (med 20 m in 150 m, neposredna vidljivost ali brez vidljivosti) izbrali med 5 in 10 merilnih mest ter merili naslednje parametre:

– hitrost prenosa TCP-prometa v smeri od omrežja proti uporabniku (download);
– hitrost prenosa TCP-prometa v smeri od uporabnika proti omrežju (upload);
– hitrost prenosa UDP-prometa v smeri od omrežja proti uporabniku (download);
– hitrost prenosa UDP-prometa v smeri od uporabnika proti omrežju (upload).

V tabelah 1 in 2 podajamo pričakovane povprečne prenosne hitrosti za uporabnika v frekvenčnem pasu 2.4 GHz oz. 5 GHz. Višje hitrosti pričakujemo v bližini dostopovnih točk in tam kjer imamo neposredno vidljivostjo, nižje hitrosti pa na bolj oddaljenih in zakritih lokacijah.

Tabela 1: Uporabniške prenosne hitrosti (Mbit/s) v frekvenčnem pasu 2.4 GHz. Vrednosti predstavljajo povprečne izmerjene hitrosti opreme vseh štirih proizvajalcev.

	tcp DL	tcp UL	udp DL	udp UL
root AP	30	23	30	25
mesh AP #1	25	20	38	30
mesh AP #2	12	15	25	25

Tabela 2: Uporabniške prenosne hitrosti (Mbit/s) v frekvenčnem pasu 5 GHz. Vrednosti predstavljajo povprečne izmerjene hitrosti vse testirane opreme.

	tcp DL	tcp UL	udp DL	udp UL
root AP	45	60	65	90
mesh AP #1	20	38	30	65
mesh AP #2	8	10	16	35

Hrbtenične prenosne hitrosti med AP-ji smo merili v frekvenčnem pasu 5 GHz. Situacija v našem okolju je pač takšna, da je frekvenčno območje 2.4 GHz večinoma zelo zasedeno (onesnaženo), pas 5 GHz pa je širši in predvsem bistveno manj zaseden. Zato se zdi smiselna postavitev hrbteničnega omrežja na 5 GHz in uporabniškega dostopa na 2.4 GHz. Tabela 3 podaja pričakovane prenosne hitrosti na hrbtenici omrežja mesh.

Tabela 3: Pričakovane prenosne hitrosti hrbtenice (Mbit/s) v frekvenčnem pasu 5 GHz. Vrednosti predstavljajo povprečne izmerjene hitrosti opreme vseh štirih proizvajalcev.

	tcp DL	tcp UL	udp DL	udp UL
root – mesh#1	62	53	60	75
root – mesh#2	25	20	38	35

Omejitve glede števila dostopovnih točk v mesh-verigi so različna in odvisna od proizvajalca. V našem testu te meje nismo nikoli presegli.

Sposobnost zagotavljanja QoS ugotavljamo tako, da določimo, koliko sočasnih VoIP klicev zadovoljive kakovosti zvoka lahko opravimo. Nadalje QoS lahko ugotavljamo tudi tako, da ob vzpostavljenem VoIP-klicu ali pretočnem videu (multicast promet) generiramo dodaten promet z nižjo prioriteto in merimo pri kolikšni količini dodatnega prometa začne kakovost VoIP-klica slabeti oz. kakovost pretočnega videa upade pod sprejemljivo (subjektivno merjeno) kakovost. Zaradi omejenega števila testnih terminalov (13) smo le pri opremi enega proizvajalca uspeli preseči maksimalno število sočasnih VoIP-klicev.

Za zagotavljanje kakovosti storitev protokoli označujejo prometne tokove in jim s tem omogočajo prioriteto pri transportu, zato nam s simulacijo običajnega (internetnega) podatkovnega prometa (aplikacija ZAP), ki smo ga generirali kot dodatno obremenitev dostopovne točke, ni uspelo degradirati VoIP oz. video vsebin, medtem ko nam je pri uporabi »invazivnejšega« postopka iPERF to uspelo.

Odpornost omrežja na motnje, tj. signale drugih (motilnih) dostopovnih točk, se je v vseh primerih izkazala za učinkovito – uporabniški odjemalci so tudi na večjih oddaljenostih ostali povezani na izbrano točko in zagotavljali prenos s primerno hitrostjo oz. so preklopili na drugo dostopovno točko istega omrežja (najhitrejši preklop smo dosegli z opremo, ki je v povprečju porabila 480 ms za preklop in pri tem izgubila zgolj 1 podatkovni paket).

Glede ostalih lastnosti, ki smo jih še vzeli pod drobnogled nismo ugotovili posebnosti, pravzaprav gre za bolj ali manj že uveljavljene funkcionalnosti, ki se sicer od proizvajalca do proizvajalca nekoliko razlikujejo, vendar v končnem omogočajo izgradnjo varnega, zanesljivega, robustnega in obvladljivega omrežja Wi-Fi.

V. ZAKLJUČEK

Sodobna oprema za gradnjo omrežij Metro Wi-Fi izkazuje dokaj dobre lastnosti, ki so v marsikaterih primerih že povsem na ravni opreme klasičnih mobilnih omrežij. Oprema, katere testiranje smo opisali v tem prispevku, je bila še v razvojni fazi (podpora standardu IEEE 802.11n za »outdoor« rešitve še ni rutina), zato v produkcijskih izdelkih pričakujemo še boljše zmogljivosti.

Zaključimo lahko z ugotovitvijo, da so tudi omrežja Wi-Fi povsem mogoča infrastruktura za »»internet stvari««, seveda le v dobro načrtovanem omrežju. Glede na zmogljivosti opreme je oprema Wi-Fi povsem mogoča alternativa, vendar pa bo za vsak konkreten primer potrebno preučiti prednosti in slabosti v primerjavi z ostalimi možnostmi brezžičnega oz. mobilnega pokrivanja.

LITERATURA

[1] IEEE 802.11 Wireless Local Area Networks, http://www.ieee802.org/11
[2] NeoWLAN, http://www.mobitel.si/storitve/neowlan.aspx
[3] O2 to fling out free Wi-Fi for all, The Register, 26. januar 2011, http://www.theregister.co.uk/2011/01/26/o2_free_wi_fi
[4] Wi-Fi CERTIFIED Hotspot Program to Ease Subscriber Connectivity in Service Provider Wi-Fi Hotspots, Wi-Fi Alliance, 22. marec 2011.
[5] Cisco, Ruckus Wireless introduce carrier-class Wi-Fi solutions for smart data offload, Fierce Broadband Wireless, 13. februar 2011, http://www.fiercebroadbandwireless.com/story/cisco-ruckus-wireless-introduce-carrier-class-Wi-Fi-solutions-smart-data-of/2011-02-13?utm_medium=nl&utm_source=internal
[6] Razpisna dokumentacija za izbiro zasebnega partnerja za javno-zasebno partnerstvo »Uvedba brezžičnega omrežja na območju Mestne občine Ljubljana«, Mestna občina Ljubljana, julij 2010.
[7] Keeling, M., Smarter Cities for Smater Growth, IBM Institute for Business Value, avgust 2010.
[8] The new data offloading industry, Fierce Broadband Wireless, 16. jul. 2009, http://www.fiercebroadbandwireless.com/story/offload/2009-07-16
[9] Tse, D., Viswanath, P., Fundamentals of Wireless Communication, Cambridge University Press, 2005.
[10] Komunikator, http://www.mobitel.si/storitve/komunikator.aspx

dr. Rudolf Sušnik je od leta 2006 zaposlen v Razvojnem oddelku paketnega omrežja podjetja Mobitel, d. d. Pred tem je bil kot mladi raziskovalec zaposlen na Fakulteti za elektrotehniko Univerze v Ljubljani, kjer se je tudi začel ukvarjati s tehnologijami brezžičnega interneta. Poleg tehnologije Wi-Fi se ukvarja še z razvojem storitev, razvojem različnih orodij za podporo omrežju in sistemom avtentikacije, avtorizacije in zaračunavanja ter z integracijo elementov AAA v Mobitelovo paketno omrežje.

Jure Sodja je leta 2008 diplomiral na Fakulteti za elektrotehniko Univerze v Ljubljani. Od tedaj je zaposlen v Razvojnem oddelku dostopovnega omrežja podjetja Telekom Slovenije, d. d. Njegove zadolžitve poleg tehnologije Wi-Fi in satelitskih sistemov pokrivajo predvsem strateški razvoj fiksnega dostopovnega omrežja in delo s fiksnimi dostopovnimi napravami (modemi, DSLAM-i, FWT …).

Uporaba vsestranskega senzorskega vozlišča za podporo okoljskim aplikacijam

Kemal Alič, Marko Kastelic, Denis Škrabl, Miha Smolnikar, Tomaž Javornik, Mihael Mohorčič
Odsek za komunikacijske sisteme, Institut »Jožef Stefan«

Povzetek — Okolje, v katerem živimo, postaja aktivni del Interneta stvari. Poleg daljinskega zaznavanja, vzorčenja s kemijsko analizo in tradicionalnih načinov spremljanja okolja, je v zadnjem času zaznati intenzivno uvajanje tehnologij na osnovi brezžičnih senzorskih omrežij, ki s podporo procesov odločanja s podatki v realnem času, omogočajo nove načine nadziranja pestrosti življenjskih habitatov ter podporo učinkovitejšemu in prijaznejšemu sobivanju z naravo. Namen tega prispevka je podati pregled okoljskih aplikacij z uporabo platforme Vsestranskega senzorskega vozlišča (VSN). Modularna zasnova platforme omogoča visoko stopnjo prilagodljivosti zahtevam aplikacije. V prispevku bodo predstavljene izkušnje pri razvoju avtonomnih sistemov za: (*i*) spremljanje temperature in vlage v hlevih za detekcijo hipertermije, (*ii*) spremljanje stanja rek za podporo športnemu ribolovu, (*iii*) nadzor stanja v čebeljih panjih ter klimatskih pogojev za medenje in (*iv*) multispektralno slikanje ter zajem senzorskih podatkov z brezpilotnim letalom.

Ključne besede — brezžična senzorska omrežja, Internet stvari, Vsestransko senzorsko vozlišče (VSN), zbiranje podatkov, opazovanje okolja

Abstract — The environment we live in is becoming an active part of the Internet of Things (IoT). Wireless Sensor Networks (WSN) represent one of its core technologies and allow putting in force process management with real-time sensor data and in this way enable the development of new principles for monitoring the diversity of living habitats. The purpose of this paper is to present WSN aided environmental applications and experiences gained in the development of autonomous systems for: (*i*) hyperthermia detection in stables, (*ii*) remote observation of sport-fishing conditions, (*iii*) inspection of beehives and local climate conditions affecting the bees, and (*iv*) multispectral imaging and data harvesting using an Unmanned Aerial Vehicle (UAV). A special attention is devoted to the use of custom designed Versatile Sensor Node (VSN) platform, characterized by modular structure. By using dedicated sensors and actuators, add-on boards, the platform allows adaptation to diverse application requirements.

Keywords — Wireless Sensor Networks (WSN), Internet of Things (IoT), Versatile Sensor Node (VSN), Data harvesting, Environmental monitoring

I. UVOD

Vsi v omrežje povezani objekti predstavljajo gradnike v paradigmi Interneta stvari (angl. Internet of Things, IoT). Delimo jih na ponore in izvore informacij. Z razmahom števila mrežnim elementov, ki smo mu priča (računalniške funkcionalnosti vgrajujemo tako rekoč povsod: v avtomobile, hladilnike, rastline, vinograde, vsebino nakupovalne košarice ...), lahko pričakujemo kvalitativen in kvantitativen preskok na različnih področjih, kot so medicina, transport, zabava, gospodinjstvo ... [1].

Brezžična senzorska omrežja (angl. Wireless Sensor Networks, WSN) in radio-frekvenčna identifikacija (angl. Radio-Frequency IDentification, RFID) sta tehnologiji, ki v tem trenutku predstavljata jedro IoT [2]. Glavna razloga sta relativna zrelost obeh tehnologij in dobro pogojen spekter uporabe na najrazličnejših področjih. Tehnologiji lahko interpretiramo tudi kot virtualno plast med informacijami o fizičnih lastnostih sveta in uporabniškimi aplikacijami [3].

Doprinos IoT nista zgolj oddaljeno opazovanje in nadzor, pač pa je to predvsem povezovanje heterogenih sistemov v skupne informacijske storitve [4]. Udejanjanje v resničnem svetu opazujemo med drugim tudi projektih večjih korporacij, kakršna sta npr. 'Smart Planet' podjetja IBM ali 'CeNSE' podjetja HP. Nadalje, skupnost s področja daljinskega zaznavanja, ki informacije v največji meri pridobiva iz fotografij (satelitski in letalski posnetki), pričakuje, da bo svoje podatke lahko obogatila s senzorskimi meritvami. Slednje pomeni, da moramo danes pripraviti pot, ki bo omogočila konvergenco heterogenih sistemov, pri čemer SOAP (angl. Simple Object Access Protocol) in REST (angl. Representational State Transfer) predstavljata primera dobre prakse za povezovanje podatkov pridobljenih iz WSN in spletnih storitev [5].

Z veliko gotovostjo lahko trdimo, da bodo WSN postala del našega vsakdana. Vprašanje je le, na katerem področju se bodo aplikacije prej uveljavile. Opazovanje okolja zaradi vse večje ozaveščenosti javnosti gotovo predstavlja eno od smeri, ki bo požela veliko pozornosti [6]. Potresi, cunamiji in izginjajoči ledeniki so nedvoumen dokaz, da se naše okolje spreminja. Trenutno znanje pa nam ne zadošča, da bi

spremembe pojasnili. Tradicionalne načine zbiranja informacij o okolju je zato potrebno spremeniti oz. dopolniti z novimi, temeljitejšimi metodami, pri čemer WSN predstavljajo cenovno ugodno in zadosti kakovostno alternativo [7].

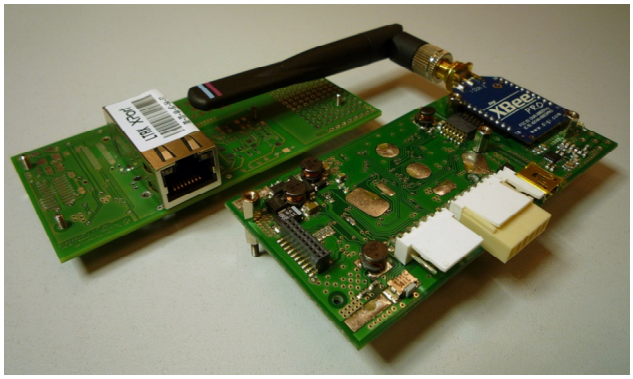
WSN so bila v zadnjem desetletju deležna velike akademske pozornosti. Žal so rezultati pridobljeni v zaprtih okoljih v večini primerov teoretične narave in v najboljših primerih nakazujejo možnosti praktične uporabe. Pomanjkanje praktičnih izkušenj zato kljub relativni zrelosti tehnologije, upočasnjuje prodor aplikacij do končnih uporabnikov. Dokončen preskok iz teorije v prakso zato ni odvisen zgolj od padca cen senzorskih vozlišč, temveč je potrebno tudi znanje pridobljeno iz dolgo trajajočih pilotskih projektov v naravnem okolju [8]. Za okoljske aplikacije, primerne za posvojitev tehnologije WSN dodatno veljajo zahteve, da morajo komponente delovati zanesljivo v pogosto neprijaznem okolju ter da se za obratovanje pričakuje dolga doba avtonomnosti [9].

V članku se posvetimo posebnostim opazovanja okolja skozi prakso pridobljeno v različnih aplikacijah. Ker vse aplikacije temeljijo na uporabi senzorske platforme VSN, jo najprej predstavimo v poglavju II. V poglavju III podamo izkušnje z uporabe platforme VSN za nekaj primerov aplikacij opazovanja okolja. Poglavje IV povzema glavne ugotovitve in podaja smernice za nadaljnji razvoj.

II. VSESTRANSKO SENZORSKO VOZLIŠČE

Senzorsko vozlišče, ki nudi podporo različnim aplikacijam, mora biti prilagodljivo v smislu podpore različnih vrst tipal, aktuatorjev, komunikacijskih vmesnikov in uporabe različnih energijskih virov. Vsestransko senzorsko vozlišče (angl. Versatile Sensor Node, VSN), ki je bilo razvito v sodelovanju med Institutom »Jožef Stefan« in podjetjem ISOTEL d. o. o., ustreza zapisanim zahtevam in obenem ponuja visoko zmogljivost procesiranja. Primer izdelanih komponent vozlišča ponazarja Slika 1.

Vsestranskost platforme zagotavlja modularna zasnova, ki omogoča uporabo zgolj tistih modulov, ki jih določena aplikacija potrebuje oz. dovoljuje razvoj poljubnih namenskih modulov. Jedrni modul (VSC) bazira na visokozmogljivem mikrokrmilniku z jedrom ARM Cortex-M3, ki ga lahko napajamo preko baterij, sončnih panelov ali direktno iz električnega omrežja. Preko vmesnikov kot so UART, I^2C, SPI, ADC in DAC, vozlišče omogoča priklop digitalnih in analognih senzorjev ter aktuatorjev. Le ti se navadno realizirajo kot del z aplikacijo pogojenega razširitvenega modula (VSE). Podpora perifernim napravam trenutno zajema senzorje za temperaturo, vlago, svetilnost, barvo, odboj svetlobe, zračni in mehanski tlak, prisotnost oz. gibanje, sliko (kamera), lokacijo (GPS), zvok, pospešek, različne pline in razdaljo, ter aktuatorje kot so motor, rele, servo in alarm.



Slika 1: Vsestransko senzorsko vozlišče

Različni radijski vmesniki, ki se nahajajo v enem od frekvenčnih pasov med 350 MHz in 2.4 GHz namenjenih industrijski, znanstveni in medicinski rabi (angl. Industrial, Scientific and Medical, ISM), so na voljo na več različicah radijskega modula (VSR). Podpiranje standarda IEEE 802.15.4 omogoča uporabo protokolnih skladov kot sta ZigBee in 6LoWPAN, poleg tega pa je podprta tudi tehnologija Wireless M-BUS ter nekaj nestandardiziranih rešitev. Za komunikacijo izven senzorskega omrežja oz. za oddaljen dostop, lahko v okviru posebnega razširitvenega modula VSE na vozlišču izvedemo prehod v druga podatkovna omrežja, vključno z GSM/GPRS, HSPA, Ethernet, Wi-Fi in Bluetooth.

Napajalni del za VSC, VSR in nekatere VSE, ki obsega stikalni napajalnik za priključitev zunanjega vira ali solarne celice ter polnilnik baterij, je izveden na modulu VSC. Poleg tega pa platforma za periferijo, ki ima višje zahteve glede porabe moči, preko modula VSP omogoča priključitev in krmiljenje dodatnih napajalnikov in virov energije.

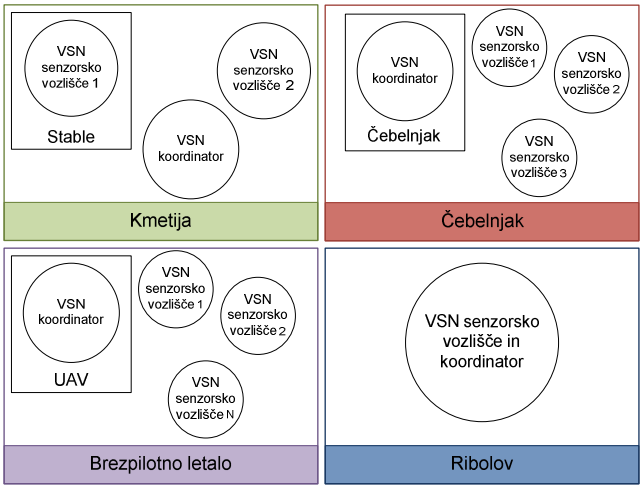
S stališča programske opreme za razvoj rešitev na podlagi VSN je na voljo širok spekter razvojnih orodij. Set odprtokodnih orodij obsega integrirano razvojno okolje (angl. Integrated Development Environment, IDE) Eclipse, orodno verigo Sourcery G++ ter OpenOCD JTAG vmesnik za razhroščevanje. Platforma podpira vrsto odprtokodnih knjižnic[1] in med drugim tudi operacijska sistema Contiki in NuttX.

III. RAZVITE APLIKACIJE

Vse v nadaljevanju predstavljene aplikacije temeljijo na uporabi vozlišča VSN. Deli rešitev posamičnih aplikacij so med seboj prenosljivi, zato se pri posamičnih aplikacijah osredotočimo zgolj na njihove posebnosti. Skozi opise poudarimo raznolikost, ki jo mora podpirati vozlišče VSN, tako s stališča topologije, podpore tipalom, energijskim podpornim

[1] http://sensorlab.ijs.si/

sistemom in komunikacijskim vmesnikom. Razlike in podobnosti med posamičnimi aplikacijami so ponazorjene tudi na slikah 2 in 3.



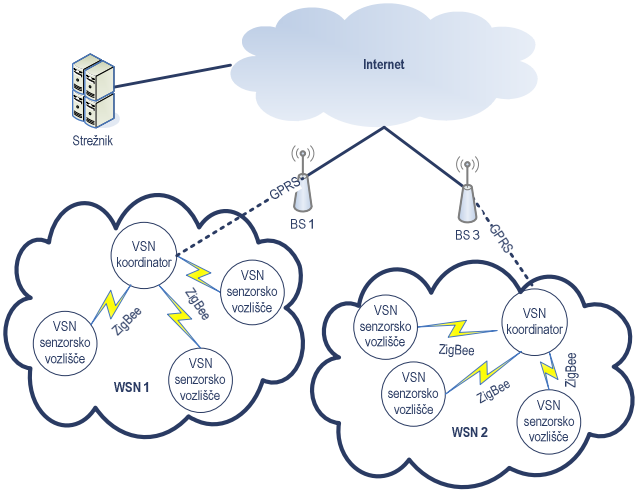
Slika 2: Topologija WSN za različne aplikacije

A. *Detekcija hipertermije v hlevih*

Obstaja sum, da krave, ki prvič telijo v vročih in vlažnih pogojih, skozi celotno življenjsko obdobje proizvajajo manj mleka, kot krave, ki niso podvržene takšnemu stresu. Da bi potrdili ali zavrgli to hipotezo je potrebno na več lokacijah v in zunaj hleva meriti temperaturo in vlažnost s frekvenco vzorčenja ene ure. Za oblikovanje reprezentativnega vzorca pričakujemo, da bo zbiranje podatkov trajalo več let. Podatki morajo imeti časovni žig, zbirati pa se morajo na enem mestu, t.j. v podatkovni bazi na strežniku. Zbiranje podatkov o kravah, njihovih teletih in količini proizvedenega mleka, ne spada v področje senzorskih mrež, zato te podatke zbiramo ročno in jih dodamo v spletno bazo.

Za detekcijo hipertermije na farmah potrebujemo tri senzorska vozlišča. Dve vozlišči sta zadolženi za merjenje temperature in vlage znotraj in zunaj hleva. Tretje vozlišče ima vlogo upravitelja mreže (koordinatorja) in določa kdaj se veličine merijo, opazuje stanje baterije, zbira meritve iz obeh vozlišč ter jih posreduje na oddaljen strežnik. Lokalno senzorsko omrežje je osnovano na protokolu ZigBee, komunikacija z oddaljenim strežnikom pa je preko koordinatorskega vozlišča zagotovljena z uporabo omrežja mobilne telefonije ter tehnologije GPRS.

Merilni senzorji so nameščeni 2 metra nad tlemi in so zavarovani pred umazanijo. Merilni senzorji se avtomatsko zbujajo vsako uro, opravijo meritve, jih posredujejo koordinatorju in se postavijo nazaj v stanje spanja. Stene v hlevih, posebej starejših, so relativno debele, kar predstavlja komunikacijsko oviro. Spričo tega smo pri izvedbi lokalnega senzorskega omrežja uporabili antene z višjim dobitkom, ki omogočajo tudi nekaj prihranka pri energiji.

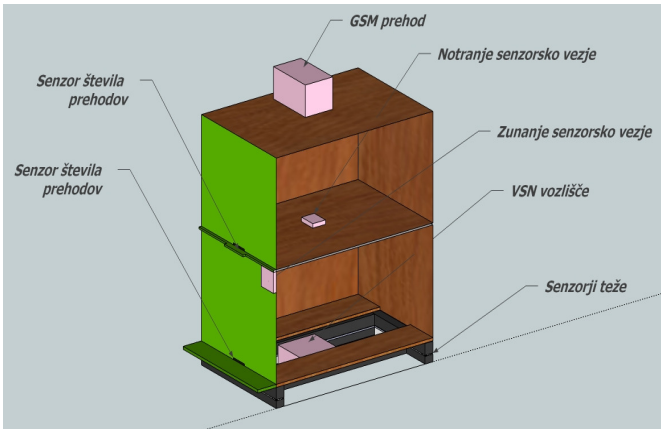


Slika 3: Komunikacijski sloj izvedbe za predstavljene WSN

Električno napajanje v hlevih predstavlja naslednjo v seriji prilagoditev. Le to je redko prisotno na mestu, kjer želimo opraviti meritve, uporaba podaljškov pa ni zaželena. V notranjosti so tudi možnosti izrabe alternativnih virov kot je sonce ali veter nemogoče, zato smo se odločili za uporabo baterije z večjo zmogljivostjo (3700 mAh), ki shranijo zadosti energije za nemotene obratovanje vozlišča za tri mesece. Za detekcijo nizke vrednosti zaloge energije na merilnih vozliščih je zadolžen koordinator, ki po potrebi v nadzorni center pošlje alarm za vzdrževanje. Ker lokacije koordinatorja ne pogojuje sama aplikacija in ker je zaradi stalnega obratovanja potrebuje konstanten vir energije, je lokacija njegove namestitve odvisna od razpoložljivosti električnega omrežja.

B. *Opazovanje športno-ribolovnih pogojev*

Slovenija je svetovno poznana muharska destilacija. Predvsem zaradi geografskega položaje je le nekaj dni v letu, ko muharjenje na rekah na celotnem območju Slovenije ni mogoče. V času prehodnih vremenskih pojavov (npr. krajših obdobij padavin) se alpske reke odzivajo drugače od kraških. Tuji ter domači muharji, odločitev o lokaciji muharjenja zato pogosto sprejmejo v zadnjem možnem trenutku, kjer poizkušajo upoštevati trenutne vremenske razmere. Specifične informacije o pogojih pa so težko dostopne oz. bolje rečeno ne obstajajo. Zaradi tega se ribiči zanašajo drug na drugega in se informirajo po telefonih, forumih in drugih podobnih medijih. Definicija ugodnih ribolovnih pogojev presega okvir tega prispevka, zagotovo pa bi bila večina ribičev-muharjev zadovoljna z vodostajem reke, temperaturo reke in zraka. Vse dodatne informacije o vremenu ter v obliki fotografije razmer pa bi bile zelo dobrodošle. Želeno je, da je frekvenca vzorčenja ena ura, kar zadostuje tudi za razpoznavo delovanja hidroelektrarn, ki močno vplivajo na vodostaj.



Slika 4: Slovenski panj 'žnidaršič' opremljen s senzorji in senzorskimi vozlišči

Za opazovanje ribolovnih pogojev zadošča že eno samo senzorsko vozlišče, ki upravlja z VGA kamero, senzorji za merjenje temperature, pritiska in vlažnosti zraka ter senzorji za merjenje temperature in vodostaja vode. Vozlišče v večini primerov namestimo na most, tako da iz lokacije zajamemo fotografijo vode, hkrati pa lahko namestimo senzorje v vodo. V primerih, ko vsem zahtevam ne moremo ugoditi z enim vozliščem, lahko podobno kot v prejšnji aplikaciji, dodamo merilno vozlišče.

Senzorje, ki merijo izbrane lastnosti vode na vozlišče priklopimo preko vodila, ki je lahko dolgo do 15 metrov. Zaradi tega razloga je za komunikacijo med tipalom in senzorskim vozliščem predvidena komunikacija z nižjimi prenosnimi hitrostmi. Senzor za temperaturo vode in tlak namestimo na rečno dno v vodotesno ohišje.

Merjenje vodostaja je realizirano z diferencialnim senzorjem tlaka, kjer je en senzorski vhod za referenco meri tlak zraka, drugi konec pa se preko silikonske cevi nahaja v vodi. Tak sistem omogoča merjenje vodostaja med 0 in 10 metri z natančnostjo ±1 cm.

S kamero lahko zajemamo slike resolucije v velikosti 640×480 slikovnih točk ter v 24-bitni resoluciji barv. Format slik je JPEG, zato jih na oddaljen strežnik pošljemo brez dodatne obdelave.

Energijo za delovanje vozlišča črpamo iz baterije, ki se polni preko solarnega modula. Vozlišče zbrane meritve na oddaljen strežnik posreduje vsako uro, večino preostalega časa pa je v stanju spanja. Tako kot v prejšnjem primeru, podatke posredujemo na oddaljen strežnik preko GPRS modula.

C. Lokalne klimatske posebnosti v okolici čebelnjaka

Čebelarstvo, kot ena najstarejših ruralnih dejavnosti, ima v Sloveniji dolgoletno tradicijo in predstavlja pomembno gospodarsko dejavnost. Poleg znanih pozitivnih učinkov čebel, kot so pridelava medu in voska, čebele lahko obravnavamo tudi kot odlične bio-indikatorje za odkrivanje kemičnega onesnaževanja (npr. pretirano rabo fitofarmacevtskih sredstev). Na čebele negativno vpliva nepravilna raba fitofarmacevtskih sredstev kjerkoli v radiju treh kilometrov okrog čebelnjaka. Rezultati kemičnega onesnaženja pa so za čebele običajno pogubni, saj veliko čebel pogine preden se vrnejo v panj. Zmanjšano število čebel v panju pa vpliva na znižanje temperature v panju, kar je pogubno tudi za preostale čebele [10].

Poleg čebelarjev, ki so od čebel tudi ekonomsko odvisni ter jih zanima kakovost paše v okolici čebelnjaka in zdravstveno stanje panja, kažejo vedno več zanimanja za spremljanje stanja čebeljih družin tudi okoljske agencije.

Slovenska čebelarska zveza[2] vzdržuje in opazuje mrežo čebeljih družin ter preko njih spremlja in napoveduje kakovost paše na izbranih področjih. Podatki o teži panja, zunanji temperaturi in vlagi, v nekaterih primerih pa tudi smeri in hitrosti vetra se zbirajo na območju celotne Slovenije[3].

Meritve se odvisno od kraja zbirajo bodisi avtomatično ali ročno, podatki pa se shranjujejo v centralni podatkovni bazi, kjer čakajo na kasnejšo obdelavo. Glavne pomanjkljivosti obstoječih sistemov so (*i*) visoka poraba energije merilnih postaj, ki posledično zahtevajo menjavanje baterij na mesečni ravni, (*ii*) delno ročno pobiranje podatkov, zaradi pomanjkljive komunikacijske infrastrukture na področju meritev, (*iii*) pomanjkljive informacije o klimatskih pogojih znotraj panjev ter (*iv*) neobstoj sistema, ki bi zaznal nenaden upad števila čebel v panju (t.j. tistih, ki se zvečer niso vrnile s paše), kar lahko nakazuje na zastrupitev s pesticidi.

Za opazovanje lokalnih klimatskih pogojev kot podporo pri napovedovanju paše in opazovanje blagostanja čebeljih družin smo sestavili senzorsko omrežje sestavljeno iz najmanj štirih vozlišč, ki se nahajajo v panju, ob njem in v bližini čebelnjaka.

Koordinatorsko vozlišče je odgovorno za zbiranje podatkov s pripadajočih merilnih vozlišč ter za nadzor zunanjih klimatskih pogojev (temperatura in vlaga). Zbrani podatki se na oddaljen strežnik posredujejo preko GPRS modula. V začetni fazi projekta vozlišča na in ob panju merijo težo panja ter temperaturo in vlago v panju. V drugem delu projekta bomo dodali vozlišča in podporne senzorje zadolžene za merjenje števila čebel, ki v vstopajo in izstopajo iz panja ter snemalnike zvoka. Predvidevamo, da bomo s pomočjo zbranih podatkov našli odvisnost med blagostanjem čebel in onesnaženjem okolice. Senzor za določanje smeri in jakosti vetra bo pomagal pri določanju in

[2] http://www.czs.si
[3] http://www.czs.si/Napoved/napoved_medenja.php

napovedi čebelje paše. Eksperimentalno postavitev senzorjev na panj prikazuje Slika 4.

D. Multispektralno slikanje in zbiranje podatkov s brezpilotnim letalom

Satelitsko multispektralno in hiperspektralno slikanje omejuje predvsem nizka prostorska ločljivost, medtem ko je časovna ločljivost pri satelitskem opazovanju za večino aplikacij zadostna. Obratna situacija pa velja za letalsko slikanje zemlje, kjer imamo višjo prostorsko ločljivost, vendar nizko časovno ločljivost. Poleg teh posebnosti in pomanjkljivosti je težava tudi, da so posnetki pridobljeni s pomočjo satelitov ali letal relativno dragi, kar še posebej drži, ko imamo opravka z manjšo površino zemlje, kar je značilno v Sloveniji.

Majhna in nizko-cenovna brezpilotna letala (angl. Unmanned Aerial Vehicle, UAV) lahko predstavljajo ugodno alternativo za vrsto uporabniških aplikacij, posebno na področjih, kjer imamo opravka z manjšimi koščki zemlje, razkropljenimi po večjem območju. Na področju preciznega kmetijstva lahko npr. slike pridobljene iz UAV uporabimo za določanje vsebnosti vode v rastlinah, stresa rastlin, težav s škodljivci, pomanjkljivosti pri gnojenju, itn.

Območja s pomanjkljivo komunikacijsko infrastrukturo so pogosto zanimiva za opazovanje s senzorskimi mrežami. Pobiranje podatkov na takih območjih običajno poteka ročno, alternativo pa nam predstavlja UAV, ki lahko dostopa tudi do odročnih predelov, kamor smo namestili senzorje. Z namestitvijo senzorskega vozlišča s funkcijo ponora podatkov na UAV, lahko s takim sistemom poberemo podatke s senzorskih vozlišč.

Za pobiranje podatkov na oddaljenih lokacijah s pomanjkljivo komunikacijsko infrastrukturo smo razvili manjše brezpilotno letalo (UAV) na katerem se nahaja tudi koordinatorsko vozlišče. Za navigiranje letala smo uporabili odprtokodno platformo ArduPilot [11], ki pri določanju lokacije letala uporablja GPS sprejemnik, IR senzorje, s katerimi določamo nagib letala in ga uravnavamo, ter tlačni senzorj, preko katerega določamo hitrost in višino letala.

UAV pošljemo po poti opisani z GPS koordinatami ob v naprej določenem času. V tem obdobju se senzorska vozlišča, ki se nahajajo na tleh, zbujajo iz spanca vsako minuto in poizkušajo vzpostaviti povezavo s koordinatorskim vozliščem na letalu. Če povezave ne vzpostavimo takoj, letalo nekaj časa kroži nad senzorjem in poizkuša ponovno. Po uspešni vzpostavitvi zveze med vozliščema, se zbrani podatki prenesejo na koordinatorsko vozlišče. Če povezava ni uspešno vzpostavljena, letalo nadaljuje svojo pot. Podatke iz koordinatorskega vozlišča zberemo šele po pristanku letala.

Prav to letalo pa uporabljamo tudi za multispektralno slikanje. Fotoaparat proži koordinatorsko vozlišče na letalu. Na točki zanimanja se letalo izravna in vzpostavi primerno hitrost. S kamero Tetracam ADC, ki ima CMOS senzor z resolucijo 2048×1536 slikovnih točk, smo najboljše fotografije posneli na višini med 50 in 100 metri.

IV. Zaključek in pogled naprej

V prispevku smo skozi praktične primere okoljskih aplikacij pokazali potrebo po vsestranskosti senzorskih vozlišč. Aplikacije, ki so si v sami osnovi močno podobne zahtevajo prilagajanje s stališča podpore tipalom, komunikacijskim protokolom in energijskemu napajanju. Veliko dela in prostora smo namenili tudi prilagajanju na okolje v katerem omrežja delujejo.

Tehnologija senzorskih mrež je predvsem zaradi nizkih cen in zadovoljive natančnosti omogočila, da smo uporabniške primere spravili v življenje. Kljub temu, da del aplikacij že teče, pa se naše delo še vedno nadaljuje. Za same aplikacije moramo razviti še specifična tipala (npr. svetilnost v detekciji športno-ribolovnih pogojev, da bi lahko določali motnost vode; čebelnjake bomo opremili s števcem čebel). Glede tipal so zahteve jasne, v primeru IoT, ki je pravzaprav šele na začetku razvojne poti, pa je v tem trenutku težko pripraviti generično rešitev, ki ne bi potrebovala večjih posegov v srednjeročnem časovnem razdobju. Podobno kot z IoT, pa bo senzorske podatke potrebno na primeren način opisati tudi za potrebe skupnosti opazovalcev zemlje. Spregledati pa ne gre niti izkušenj in znanj, ki jih bomo pridobili po daljšem obdobju delovanja WSN v, za elektronske komponente, neprijaznem okolju, na katerih bomo lahko gradili naprej.

Zahvala

Delo predstavljeno v prispevku je delno podprla Evropska skupnost skozi projekt 7. okvirnega programa AgroSense (FP7-204472). Avtorji članka se zahvaljujejo tudi ekipi SensorLab za podporo in prispevke.

LITERATURA

[1] [1] C. Alcaraz, P. Najera, J. Lopez *et al.*, "Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?," in 1er International Workshop on the Security of The Internet of Things (SecIoT 2010), Tokyo (Japan), 2010.

[2] [2] R. Rodrigo, A. Cristina, L. Javier *et al.*, "Key management systems for sensor networks in the context of the Internet of Things," *Computers & Electrical Engineering,* to be published, 2011.

[3] [3] R. Roman, J. Lopez, and C. Alcaraz, "Do Wireless Sensor Networks Need to be Completely Integrated into the Internet?," in Future Internet of People, Things and Services (IoPTS) eco-Systems, Brussels, 2009.

[4] [4] M. A. Moisescu, I. Ş. Sacală, and A. M. Stănescu, "Towards the development of internet of things oriented intelligent systems," *UPB Scientific Bulletin, Series C: Electrical Engineering,* Vol. 72, No. 4, pp. 115-124, 2010.

[5] [5] Q. Zhu, R. Wang, Q. Chen *et al.*, "IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things," in IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Hong Kong, China, 2010.

[6] [6] C. Alippi, R. Camplani, C. Galperti *et al.*, "A Robust, Adaptive, Solar-Powered WSN Framework for Aquatic Environmental Monitoring," *IEEE Sensors Journal,* Vol. 11, No. 1, pp. 45-55, January, 2011.

[7] [7] S. Hu, H. Wang, C. She *et al.*, "AgOnt: Ontology for agriculture internet of things," in 4th IFIP International Conference on Computer and Computing Technologies in Agriculture and the 4th Symposium on Development of Rural Information, CCTA 2010, Nanchang, China, 2010, pp. 131-137.

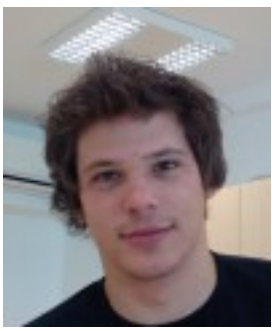
[8] [8] G. Barrenetxea, F. Ingelrest, G. Schaefer *et al.*, "Wireless Sensor Networks for Environmental Monitoring: The SensorScope Experience."

[9] [9] K. Q. Wang, and K. Cai, "Farmland information gathering and monitoring system based on IOT," in 2nd Pacific-Asia Conference on Circuits, Communications and System, PACCS 2010, Beijing, China, 2010, pp. 253-256.

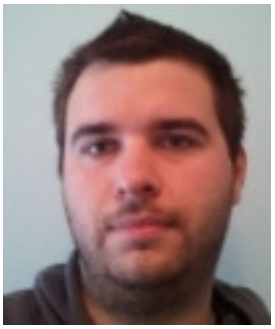
[10] [10] C. Porrini, A. G. Sabatini, S. Girotti *et al.*, "The death of honey bees and environmental pollution by pesticides: the honey bees as biological indicators," *Bulletin of Insectology,* Vol. 56, No. 1, pp. 147-152, 2003.

[11] [11] C. Anderson. "ArduPilot home page," March, 2011; http://diydrones.com/profiles/blog/show?id=705844%3ABlogPost%3A44814.

Kemal Alič je na Odseku za komunikacijske sisteme Instituta »Jožef Stefan« zaposlen od leta 2008. Njegovo področje delovanja je simuliranje komunikacijskih omrežijh s posebnim poudarkom na mrežnem nivoju.



Mare Kastelic je absolvent na Fakulteti za elektrotehniko v Ljubljani. Na Odseku za Komunikacijske sisteme Instituta »Jožef Stefan« je zasposlen kot študent od Junija 2010. Njegovo glavno delo je razvoj mikrokrmilniških vezij.



Denis Škrabl je absolvent na Fakulteti za elektrotehniko v Ljubljani. Kot študent dela na Institutu »Jožef Stefan«, na odseku za Komunikacijske sisteme, od septembra 2008 na področju razvoja mikrokrmilnikov in brezpilotnih letal.

Tomaž Javornik je na Odseku Za komunikacijske sisteme Instituta »Jožef Stefan« zaposlen od leta 1987, v zadnjem obdobju na mestu višjega raziskovalnega sodelavca. Njegovo področje delovanja je razvoj in analiza fiksnih in mobilnih brezžičnih telekomunikacijskih sistemov in senzorskih sistemov, s posebnim poudarkom na fizičnem nivoju.

Miha Smolnikar je diplomiral leta 2005 na Fakulteti za elektrotehniko Univerze v Ljubljani in se zaposlil kot mladi raziskovalec na Odseku za komunikacijske sisteme Instituta »Jožef Stefan«. Trenutno zaključuje doktorski študij elektrotehnike na Fakulteti za elektrotehniko Univerze v Ljubljani. V okviru raziskovalnega dela se ukvarja z medplastnim načrtovanjem protokolnega sklada, kognitivnim radijem, adaptivnimi brezžičnimi komunikacijskimi sistemi in senzorskimi omrežji.

Mihael Mohorčič je višji znanstveni sodelavec in vodja Odseka za komunikacijske sisteme na Institutu »Jožef Stefan«. Doktoriral je leta 2002 na Fakulteti za elektrotehniko Univerze v Ljubljani. Leta 2006 je bil na Mednarodni podiplomski šoli Jožefa Stefana izvoljen v naziv docent za predmetno področje "Telekomunikacije". Tam je tudi dopolnilno zaposlen in izvaja več predmetov na 2. in 3. stopnji bolonjskega študija. Njegovo raziskovalno delo sodi na področja satelitskih, stratosferskih, brezžičnih, kognitivnih in senzorskih omrežij.

Approaches to sustainable telcos: global action and local intelligence

Fedor Gabrovšek, Simeon Lisec, Radovan Sernec, Telekom Slovenije d. d.

Povzetek — Upoštevanje trajnostnega razvoja telekomunikacijskih operaterjev je nujno za izpolnjevanje EU2020 ciljev. To je dosegljivo z uporabo obnovljivih virov energije, zmanjšanjem porabe energentov in IoT inteligentnih tehnologij za sklenitev regulacijskega kroga v realnem času. Vendar apliciranje IoT na geografsko porazdeljenih postrojenjih prinaša velike izzive informacijske varnosti.

Ključne besede — IoT, informacijska varnost, IPv6, agenda EU2020, fotonapetostni moduli, trajnostni razvoj

Abstract — Telecom operators must embrace sustainable operations in order to achieve EU2020 goals. This is achievable by using renewable energy sources, efficient energy use and IoT intelligent technologies to perform real time closed loop regulation. IoT is putting forward information security challenges.

Keywords — Sustainability, IoT, information security, IPv6, EU2020, photovoltaics

I. INTRODUCTION

In this paper we focus on environmental issues and improvements telcos can contribute in the long term to society and especially to exceed EU2020 energy goals, enabling low carbon economy and how can IoT local intelligence contribute to achieve the automatic closed cycle global integration. EU must cut CO2 emissions by 30 % by 2020, up from previously envisioned 20 %. EU Intelligent Energy programme aims to foster new state of the art developments in many industry sectors.

10 trends in future technology identified ICT as the major CO2 emission contributor (14 %), but also possible biggest saver (5× of its use) via implementation of smart IoT technologies and solutions. Telecoms in particular are big energy consumers and statistics worldwide show steady increase of electricity consumption by 4 % - 10 %/y. This is attributed not only to larger customer base, but primarily to endless network and IT equipment refurbishing cycles to keep pace with growing demands on data traffic and implementation of new services. It is true that new equipment tends to be more energy efficient in general and provide more performance, but at the same time each replacement demands more energy, largely due to Moore's law.

A major worldwide telco operator can consume several 1000s GWh/y, whereas a local smaller one several 10s GWh/y. Note, that this represents yearly output of a power plant of 10-100 MW scale in itself. Energy consumption inevitably results also in CO2 emissions attributing to global warming.

Crucial to integration of local IoT intelligence and global society impact is definition of new key performance indicators (KPI), especially environmental ones, measure them in real time across the organisation and close the control loop to improve upon the required predefined metrics of telco operations, e.g. lower CO2 foot print, electricity consumption, reduce or reuse waste heat. KPI are defined from telco internal human experts, standards, EU directives, etc.

Dematerialization technologies can reap the benefits from adoption of telecom services that directly lower CO2 footprint, as large scale videoconferencing, work from home (subtracts any commuting CO2 emissions) requires significant personal and enterprise cultural shifts. However such applications directly attribute also to energy efficiency among different industry sectors, in this case at least: transport-telecommunication-ICT equipment vendors.

In the past few years IT has done a lot in energy efficiency via virtualization, load balancing and highly efficient data centers, with record braking PUE < 1 developed in Finland. Much of these experiences can be readily reused in telco environment.

II. SUSTAINABILITY

Sustainability is very broad term and encompasses company relation to economic, society and environmental positive influences.

Sustainability approach forces society and enterprises into different thinking mode: can we grow, but at the same time lower the environmental impact, use other energy sources, lower CO2 foot print and improve life for society at large. Sustainability was indeed identified as one of the 6 possible ways of achieving growth. This will benefit telco directly via lowered Opex in general and indirectly after governments issue so called eco tax, CO2 coupons or require efficient building code across industries.

Telekom Slovenije is aware of sustainability importance and has issued related documents to its shareholders and integrated it into its strategy. This is in the same vein as with other major telcos and their

association ETNO in EU: Telecom Italia, Vodafone and even some telco equipment vendors: Ericsson.

Sustainability in telecoms usually takes into account internal (human resources, shareholders) and external stakeholders (customers, suppliers, competitors, community, environment) that when governed in positive way result in performance indicator improvements (image, brand, reputation, profit, lower energy consumption, lower CO2 footprint) across the whole organisation. It is worth noting that sustainability is already accepted on major stock exchanges worldwide with indexes like: DJSI STOXX, DJSI WORLD (NY), FTSE Environmental leaders Europe (London), etc. We must emphasise that new sustainability practices in the longer term inevitably result in improved quality of operations in general and service to customers in particular.

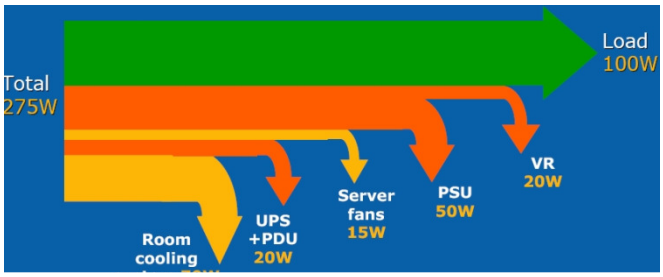
III. ENERGY EFFICIENT TELCO APPROACHES

We are proposing the holistic approach to green telco. Therefore it is crucial to work on several fronts in parallel to achieve fast returns and maintain long term effects:

– Energy savings from operations and IT and network in particular
– Cash flow from renewable energy sources, especially photovoltaics (PV) and wind farms
– Research to explore beyond state of the art in renewable energy sources, like thermoelectric Rankine cycle generators and increasing efficiency of PV. Telcos can become suitable development and pilot test vehicles when cooperating with laboratories and manufacturers of new solutions.

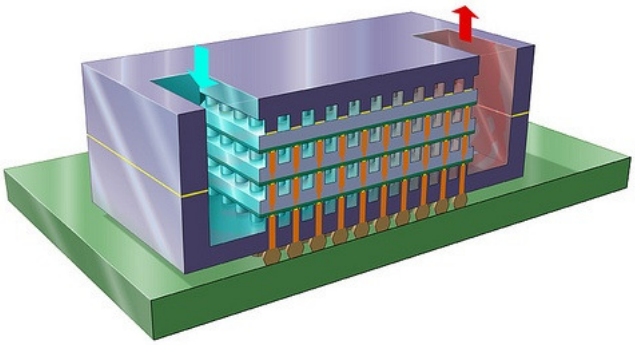
End-to-end energy consumption within telco to transport single bit of information over broadband interface reads like a very inefficient tale. A large proportion of electrical losses are due to AC/DC conversions, and again DC/DC to finally power chips. Telco had traditionally preferred -48 VDC for its equipment and this DC wave is coming back in form of new IEC standard for 400 VDC used to power state of the art ICT systems, thus completely eliminating one conversion step and increasing efficiency at least by 5 %. One must note safety measures required due to default arcing if not handled properly.

To substantially lower energy bill in IT operations one can go for aggressive IT consolidation with recent multicore, multithread, water cooled system servers, like IBM zEnterprise196, that can replace up to 4000 equivalent x86 cores of pre 2010 vintage, especially taking into account much higher sustainable CPU utilizations attainable on such systems. As a by-product a lot of physical space is freed and can thus be used to host private/hybrid cloud solutions making telco a viable large scale cloud provider.



Picture 1: Energy conversion losses to servers (Intel).

Of the myriad recent developments in efficient cooling techniques, direct, hot water, 3D chip scale solution comes out on top. Solution employs a layer of small specialized 50 µm micro channels directly integrated within chip itself in which cooling water is circulated. It is interesting that cooling is done with hot water at ~ 60 °C contributing to much lower chilling requirements in general.



Picture 2: 3D packaging with water cooling (IBM).

Among the less obvious possibilities of efficient energy use is also the application of passive building code for retrofitting older telco buildings. Drastic heat (administration) and cooling (technical) energy reductions can be expected, by several factors (3-5), as evidenced already in private housing sector.

What would it take to make a telco operation, with 200 K broadband users electrically self sustainable. To simplify the assumptions we will do calculation only for the PV use (micro amorphous or mono crystalline), disregarding any other forms of renewable sources.

Input assumptions:

– SE EU region of solarisation: 1050 kWh per kWp of installed PV
– 8 m2 PV area per kWp
– PV 1 kWp at 1500 € for large installations in 2012
– Telco electricity consumption of 50 GWh/y
– Results and requirements:
– 47 MWp PV power plant
– 376.000 m2 for PV power plant
– 70,5 M € Capex of PV power plant self sustainable telco solution

Implications of this mind exercise are far reaching taking into account also current developments in hybrid and electric vehicles and Smart, distributed energy generation GRID. The whole PV generation within such telco is going to be distributed, mainly installed on buildings (roof and walls) and integrated within national energy grid. Due to government subsidies for electricity PV generation telco can expect to get x3 amount of money back into operations as positive cash flow, compared to M € of Opex for electricity bills nowadays. ROI is expected to be < 6 years due to large installation capacity done as a single investment with special contract with 2-3 PV module manufacturers, since this represents a good portion of their yearly output. The most important implication is the notion on environment integration with distributed local "electricity pumps" for future electric vehicles that are telco branded. Note also that vehicle integrated batteries act as energy buffer to smooth uneven PV electricity generation during 24 h cycle. Even telco own car fleet for field installations of several 100 hybrid cars, each carrying 30 kWh battery already form suitable closed ecosystem with PV.

Indeed, telco can become a viable player in the energy generation field. We must add to this wind generation capabilities in the same vein. The cycle is thus closed: intelligent IoT enabled distributed renewable energy generation put to disposal to local society to gain the self sustainable energetically telco operations.

Proposal for a set of improved telco focused environmental sustainable KPIs:

- kWh per broadband fixed or mobile subscriber (from complete operations); takes into account also IT efficiency, customer field support
- kWh per broadband fixed or mobile subscriber (from network operations only); measures power consumption and efficiency of network equipment and its wise use
- kWh (or %) from renewable sources (for complete operations); takes into account use of photovoltaics, cogeneration, wind, biomass, free cooling, heat pumps for electricity of heat requirements.
- PUE (power usage effectiveness) for IT data and network equipment centers operations
- Joule per transported bit within network
- CO2 per broadband fixed or mobile subscriber (for complete operations); takes into account also IT efficiency, customer field support
- CO2 per broadband fixed or mobile subscriber (from network operations only)

For all the mentioned approaches to act as an integrated, intelligent, closed loop ecosystem we must employ IoT and M2M technologies.

IV. IoT Vision

The central element of this vision is the existence of a network of interconnected objects (from e-procedures to sustainable sources of energy, even food will be included) that will be able not only to obtain information from their surroundings and interact with the physical world, but also to use Internet standards to provide services inside corporate networks and in global internet. IoT represents an evolution that is heaving or will have a great impact on our corporate environments and our lives. The vision of the Internet of Things (IoT Vision) is widely adopted nowadays and supported by industrial companies and most of the governments all over the world.

Security is extremely important for achieving this goal. In this networks of interconnected objects can be exploited anywhere by anyone and anytime. The necessity to enhance it with strong security foundations must have a high priority. In fact, in order to adequately protect the IoT, there are plenty of factors that must be taken into account.

Let's look a little bit deeper at next use case. The protection of the different building blocks, the creation of interoperable security mechanisms, the development of new services that allow multiple entities (machines, objects and animals and humans) to cooperate with each other, and the management of all the information produced by those interactions. We are focusing in machines and objects in the scope of IoT. While analyzing sustainability of IoT enterprise, in our case telco company should cover next important topics:

- Identifying, authenticating, and authorizing entities.
- Connecting heterogeneous technologies.
- Development of trust frameworks for secure collaboration.
- New security problems in the context of the IoT.
- Privacy risks and data management problems.
- Resilience to external and internal attacks.
- New cryptographic primitives for constrained "things".
- Legal Challenges and Governance Issues.
- Context-Aware security.
- Providing protection to an IP-connected IoT.
- Distributed policy enforcement and rights management.
- Usability of Security and Privacy Technologies in the context of the IoT.

V. Security considerations

An old fashioned grid may be inefficient, but it may be easier to secure than a "smart grid". Much of the benefits of a smart grid come from internet connectivity, and that connectivity opens the door to attacks.

"If I want to cut off the power to the house now, I'd find electricity cabinet somewhere outside, and turn it

off manually. Everything's physical. Once we have a smart grid in place anyone could do that any place."

"The sheer volume of interactive devices on two-way networks is the biggest risk. By the end of 2015 we will have several million new hackable points on the grid in each EU county. Nobody around here is equipped to deal with that today."

And of course, there is worse case scenario. We elaborated several different ones and the most important triplet is:

The one everyone thinks about is the neighbour or someone in another continent turning off the power to the telco premises in the middle of night. While no one wants that to happen, it'll be detected pretty quickly, so it's really not a big issue.

Second, if you can cause rapid problems in the sustained grid ecosystem to occur in the right place at right time, you could destabilize the corporate grid, black out whole ecosystem and cause massive damage to the corporation. Sometimes this happens accidentally, but it could also happen from malicious means. Some of the devices are very expensive and therefore, there are few spares. For example, self sustainable plants aren't even made in this country anymore and sometimes it can take a long time to get replaceable one.

The third potential problem has to do with voltage control. If you want to optimize the amount of power the self sustainable company has, you want to engage in voltage control, where you have devices along the way inline from the source. You can adjust the voltage, every device gets the right voltage, and everyone's appliances are running more efficiently. Putting in those devices is expensive. Those become hackable points now, because if you can control them, then someone else can also do it. So if our power is out, that would be highly inconvenient. But what if they ran the voltage up and down in-house, the voltage-sensitive equipment like computers, sensors, security devices, routers etc. would still be working?

Nevertheless, the points raised are largely valid. Virtually every large piece of software (Windows, Linux, OS X, Internet Explorer, Safari, Firefox, Adobe Flash, etc.) created has had vulnerabilities that have been found and exploited. It's unlikely to think that the software that governs the SmartGrid will be free of similar vulnerabilities.

Google Grid and Microsoft Hohm are web based connected grids and sounds great on paper, but it introduces a pressing need for security, as people from all over the world can now try to attack the power infrastructure remotely. A typical cyber attack introduces brokenness for accessing to defined website, an attack on the corporate grid could literally prove deadly.

VI. IPv6 INFLUENCE

Introducing IoT services within enterprise environment means blinding the machine to machine (M2M) services with artificial intelligence. Best practise for green field services in line with IoT is to use IPv6 as a default IP protocol for running code applications on remote devices and local server farms. Piggyback on the Internet of Things based on IPv6 consists of technical solutions in several different areas including obstacles and constraints:

– End2end security,
– QoS,
– Management, SNMP and non-SNMP based,
– Adaptation to dynamic topology changes,
– Inherent routing,
– Leverage medium access layer on random access,
– Adoption for resource-limited networks (6LowPAN), see also G3-PLC,
– Avoidance of data aggregation,
– Usage of open, non-propriety standards.

VII. CONCLUSIONS

Telcos must embrace innovative IoT solutions for their sustainable growth. This will link methods of efficient energy use and renewable energy generation into a coherent real-time ecosystem. Path is likely to be long, but first step was already done within by putting sustainability charter within telco's strategy agendas.

REFERENCES

[1] http://www.securethecloud.com
[2] http://www.microsoft-hohm.com
[3] http://smartgrid.ieee.org/public-policy/european-union
[4] http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf
[5] Sustainability report, Vodafone, 2010.
[6] Sustainability and corporate responsibility report, Ericsson, 2009.
[7] Measuring and managing sustainability, MCE, 2011.
[8] Making it sustainable, ETNO, 2010.
[9] Smart2020 Report, 2010.
[10] Energy efficient networks, Topic issue, IEEE Network magazine, March 2011.
[11] IBM to use water cooling for future 3D IC processors, IBM, 2011.

Integracija mobilnih in brezžičnih senzorskih omrežij

Marko Pesko, Luka Vidmar, dr. Mitja Štular, Mobitel, d. d.

Povzetek — Naraščajoče število senzorjev povezanih v različna omrežja preko novih tehnologij si vse bolj utirajo pot tudi v svet mobilnih omrežij. Integracija brezžičnih senzorskih omrežij (angl. Wireless Sensor Networks, WSN) z mobilnimi omrežji je le eden izmed potencialnih pristopov mobilnih operaterjev k naprednejšim aplikacijam in praktični podpori komunikacije med napravami (angl. Machine-To-Machine, M2M) v smeri "medomrežja stvari" (angl. Internet of Things). Prispevek obravnava tehnologije mobilnih in senzorskih omrežij, njune skupne točke, prednosti njunega združevanja v primerjavi z integracijo senzorskih omrežij z ostalimi tipi omrežij ter vplive integracije na mobilna omrežja.

Ključne besede — mobilno omrežje, brezžična senzorska omrežja, integracija, M2M, medmrežje stvari

Abstract — An increasing number of sensors deployed in variety of networks across new technologies are gaining importance also in the field of the mobile networks. Integration of the Wireless Sensor Networks (WSN) with the mobile networks is thus only one of the potential approaches for the mobile operators to realize enhanced future services and Machine-to-Machine (M2M) communication in the direction of the Internet of Things. This paper discusses the mobile networks and the sensor networks technologies, their common integration points, advantages in comparison to the integration with other network types and impacts of the integration on the mobile networks.

Keywords —mobile network, Wireless Sensor Networks, integration, M2M, Internet of Things

I. UVOD

Koncept »Medmrežja stvari« (angl. Internet of Things, IoT) je postal ena izmed najbolj vročih raziskovalnih in tudi industrijskih tem, ki se je oblikoval in dopolnjeval na osnovi vidikov različnih področij. Avtorji v [1] ga predstavljajo kot presek pogledov s področja naprav oz. stvari, medmrežja ter semantike. Pri njegovi praktični realizaciji bo ključna predvsem vloga mobilnih in fiksnih operaterjev zaradi edinstvene omrežne infrastrukture, ki je že danes nepogrešljiva osnova komuniciranja večine modernih naprav povezanih v medmrežje.

Ericsson predvideva, da bo do leta 2020 obstajalo že 50 milijard komunikacijsko povezanih naprav [2]. Posledično bi morali operaterji in proizvajalci komunikacijske opreme že danes razvijati, načrtovati in posodabljati omrežno infrastrukturo, da bo pripravljena za prihodnje potrebe. Po ocenah sodeč naj bi od 50 milijard naprav le 3 milijarde predstavljali uporabniški terminali, ostalo naj bi bile komunicirajoče naprave oziroma »stvari« [3].

Zaradi tega upravičeno obstaja nevarnost, da bodo mobilna omrežja postala zgolj podporno komunikacijsko orodje za prenos informacij medmrežja stvari, kar ne bo nujno prinašalo primernega dobička. Za preprečitev omenjene situacije bodo mobilna omrežja v podporo poslovnim konceptom prihodnosti morala v medmrežju stvari imeti čim aktivnejšo vlogo. Slednjo jim lahko omogoči integracija z omrežji WSN in tako odpre vrata novim vrstam storitev zasnovanih na informacijah, za katere bodo uporabniki pripravljeni dodatno plačevati.

II. TEHNOLOGIJA MOBILNIH IN BREZŽIČNIH SENZORSKIH OMREŽIJ

A. Mobilna omrežja

Mobilno omrežje je sestavljeno iz stacionarnih omrežnih elementov in mobilne uporabniške terminalne opreme, ki je povezana v tokokrogovno in paketno omrežje. Tokokrogovni del je namenjen govornim storitvam, a pri Mobitelu že od leta 1999 podpira tudi klicni dostop s tehnologijama vodovno komutiranih podatkov CSD in hitro vodovno komutiranih podatkov HSCSD s hitrostma 9,6 kbit/s ter 43,2 kbit/s. Mobitelov paketni del omrežja obstaja od uvedbe GPRS leta 2001 in z EDGE podpira prenosne hitrosti do 236,8 kbit/s. Mobilno omrežje tretje generacije se nadgrajuje s hitrim paketnim dostopom na navzdolnji povezavi HSDPA s 7,2 Mbit/s ter hitrim paketnim prenosom od uporabnika HSUPA z 1,4 Mbit/s. Od leta 2010 se uvaja tudi dostop z visoko hitrostjo HSPA+ s še višjimi prenosnimi hitrostmi.

Pomembni gradniki stacionarnega mobilnega omrežja so bazne postaje v sistemu GSM ter NodeB v sistemu UMTS, ki brezžično komunicirajo z uporabniškimi terminali. So konstantno napajane in oddajajo z močmi reda nekaj 10 W. Ločimo jih na makro postaje z daljšim dosegom (300 m - 2000 m), mikro postaje z nekoliko manjšim dosegom (300 m - 1000 m) in piko ter femto postaje z najmanjšim dosegom (< 100 m). Uporabniška terminalna oprema na drugi strani so bili vrsto let mobilni telefoni, a

prevladujoči uporabniki paketnega prenosa postajajo računalniki z modemi ali za usmerjevalniki s karticami SIM in nizkocenovni komunikacijski moduli, ki se lahko priklopijo na različne naprave.

B. Brezžična senzorska omrežja

Za razliko od mobilnih omrežij so omrežja WSN omrežja malih, medsebojno komunicirajočih fiksno-mobilnih avtonomnih naprav t.i. senzorskih vozlišč. Ta so namenjena postavitvi po določenem interesnem območju, na katerem želimo zaznavati različne fizikalne veličine in vplivati na okolico ali naprave.

Senzorska vozlišča naj bi bila komunikacijsko kompatibilna z različnimi standardi in tehnologijami, kot so IEEE 802.15.4, ZigBee, WirelessHART, ISA 100.11a, 6LoWPAN, ANT+, a so velikokrat realizirana z lastniškimi (angl. proprietary) rešitvami, zaradi katerih so dokaj nepoznana in posledično komercialno neraziršjena. Senzorska vozlišča lahko v literaturi zasledimo pod različnimi imeni, kot npr. koordinatorje, omrežne naprave, usmerjevalnike, končna vozlišča, dostopovne točke. Njihovo poimenovanje je odvisno predvsem od kompatibilnosti z določenim standardom oziroma tehnologijo. V splošnem pa se jih deli med (1) namenske vgrajene (angl. embedded) naprave sestavljene po komponentah, (2) prilagojene splošno uporabne računalnike (angl. adapted-general purpose computers), kot so mobilni terminali, in (3) sisteme v enem čipu (angl. System on Chip, SoC).

Komunikacija med senzorskimi vozlišči je v primerjavi z mobilnimi omrežji zasnovana na energijsko učinkovitih brezžičnih povezavah moči reda nekaj 10 mW, ki podpirajo prenosne hitrostmi od nekaj 10 bit/s do tipično 250 kbit/s. Senzorska vozlišča komunicirajo na frekvencah ISM 2,4 GHz, 868 MHz in 433 MHz. Njihove specifične oddajne moči po posameznih frekvencah ureja Pravilnik o radijskih frekvencah, ki se smejo uporabljati brez odločbe o dodelitvi radijskih frekvenc [4]. Kljub zakonskim omejitvam lahko premagujejo razdalje med nekaj 100 m v zaprtih prostorih do nekaj km na prostem in v vidnem polju.

Paketni prenos za izmenjavo in posredovanje senzorskih izmerkov, nastavitev, programskih popravkov in drugih informacij med senzorskimi vozlišči poteka v različnih omrežnih topologijah, kot so zvezdna, drevesna, mešana, točka-točka in druge. Senzorski izmerki se lahko shranjujejo bodisi na senzorskih vozliščih ali v primernih pomnilnikih na nivoju celotnega omrežja. Potreba po njihovi hitri dostavi pa se kaže na vse več področjih. Zato postaja povezovanje senzorskih vozlišč v zunanja fiksna in mobilna omrežja za posredovanje izmerkov do končnega uporabnika, aplikacije ali podatkovne baze vse bolj razširjeno.

III. INTEGRACIJA OMREŽIJ

Potencialne možnosti združevanja mobilnih omrežij in omrežij WSN se kažejo tako na stacionarnem delu mobilnega omrežja kot na strani uporabniške terminalne opreme.

Na stacionarnem delu omrežja se lokacije, strojno opremo in povezanost postaj proti jedrnem omrežju z nadgradnjami WSN lahko uporabi kot izvore različnih virov uporabnih informacij. Primer japonskega NTT Docomo prikazuje, da je senzorje na postajah mogoče uporabljati za spremljanje raznolikih okoljskih parametrov, npr. vremenskih razmer, koncentracije svetnega prahu, onesnaženja, itd. [5]. Postaje s primerno senzoriko pa so primerne tudi za obveščanje pred nevarnostmi vse pogostejših naravnih nesreč, kot so poplave, neurja ali radioaktivna onesnaženja. Ravno geografska razporejenost postaj po celotni državi takšnim aplikacijam lahko zagotovi potrebno natančnost na mikro nivoju. Kot prikazuje Tabela 1 so Mobitelove postaje blizu druga drugi. Tako bi njihova potencialna integracija z omrežji WSN lahko ponudila precejšnjo natančnost zaznavanja na področju celotne Slovenije.

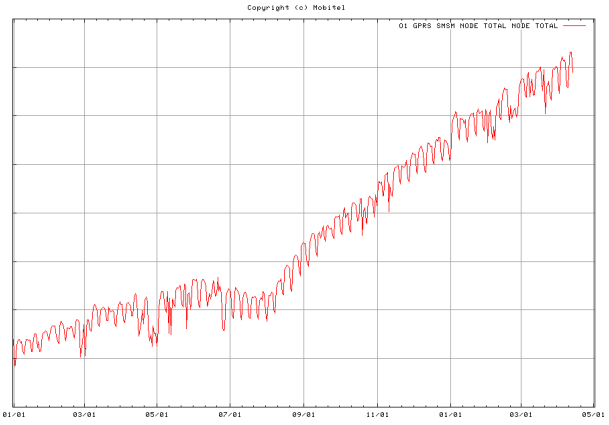
Na strani uporabniške terminalne opreme se kaže potencial v združevanu vse naprednejše terminalne opreme z raznolikimi senzorji in možnostjo brezžičnega povezovanja na kratke razdalje s kompatibilnimi komunikacijskimi vmesniki WSN s podporo Bluetooth 4.0, ANTz, NFC, RFID itd. Takšne naprave so predvsem pametni telefoni in tablični računalniki, ki lahko tvorijo mobilna senzorska omrežja (angl. Mobile Sensor Networks) preko javanskih aplikacij ali neposredno preko izvirnih aplikacij platform Android, iOS, Symbian, Windows Mobile, BlackBerry in drugih. Zelo razširjene so tudi naprave in vgrajene naprave s komunikacijskimi vmesniki GPRS, EDGE, UMTS in HSPA, v katere se vstavi kartica SIM. Z novimi vgrajenimi karticami SIM (angl. embedded SIM cards) [6] se bo začelo korenito spreminjanje povezovanja senzorskih naprav v mobilna omrežja. Vgrajene kartice SIM se bo integriralo v senzorska vozlišča ter druge naprave, ki bodo lahko

Tabela 1: Povprečna razdalja povprečnih razdalj posamezne bazne postaje in postaje NodeBe do prvih treh sosed glede na področja postavitve.

Področja postavitve baznih in NodeB postaj	**Približna povprečna razdalja povprečnih razdalj posamezne postaje do prvih 3 sosed**
Ljubljana, Maribor	560 m
Naselja z več kot 10000 prebivalci	780 m
Naselja z manj kot 10000 prebivalci	2600 m
Hribovita področja nad 1000 m.n.v	2630 m

aktivirane in vključene v omrežja na daljavo. To bo dodatno povzročilo povečanje števila aktivnih kontekstnih povezav v paketnem delu mobilnega omrežja, katerih porast je opazna že zadnjih nekaj let in za obdobje zadnjega leta prikazana na Slika 1.

Uporabniško terminalno opremo s senzorji, ki podpira komunikacijske vmesnike WSN, se lahko uporabi kot senzorska vozlišča ali za prehode (angl. gateways) proti hrbteničnemu omrežju. Kot je bilo predstavljeno, so tipične prenosne hitrosti v omrežjih WSN reda 250 kbit/s. Za občasno pošiljanje in sprejemanje manjšega števila senzorskih izmerkov v praksi pa zadostuje že okoli 200 kbit/s, kadar ne prenašamo večpredstavnostnih vsebin. Torej so s stališča mobilnih tehnologij za povezovanje senzorskih vozlišč proti hrbtenici primerne tehnologija EDGE in vse zvrsti tretje generacije mobilnih komunikacij.



Slika 1: Rast števila aktivnih kontekstnih povezav.

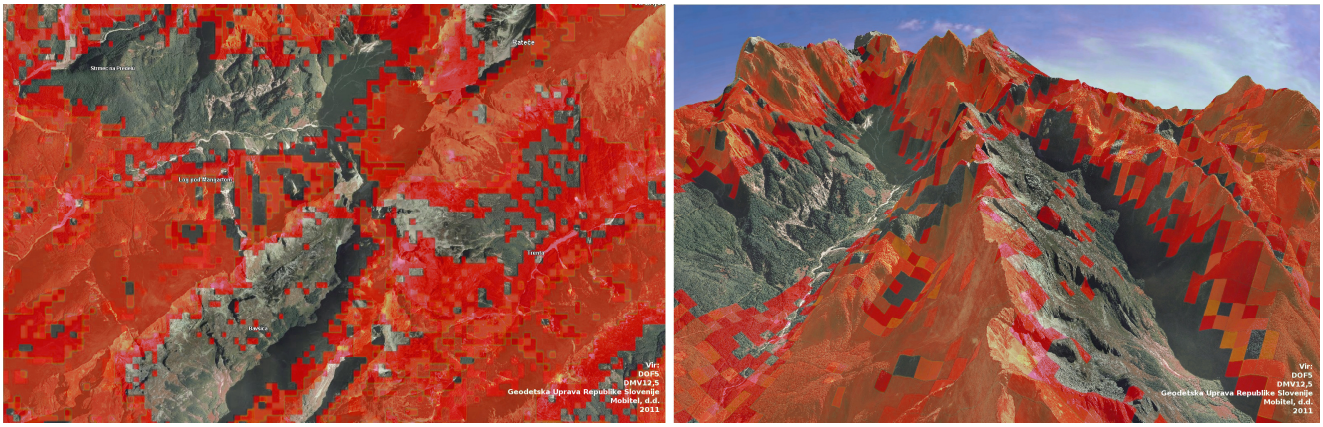
IV. PREDNOSTI IN VPLIVI INTEGRACIJE MOBILNEGA OMREŽJA Z OMREŽJI WSN

Zaradi uporabe izmerkov senzorskih vozlišč in podpore širokega nabora raznolikih aplikacij je zaželeno, da je zajemanje na določenem interesnem področju čim gostejše in čim cenejše. Fiksno postavljena omrežja WSN se lahko povezujejo z različnimi fiksnimi in fiksnimi brezžičnimi omrežji, ki so dokaj dostopne, a največkrat omejene na strnjeno poseljena območja. Zunaj naseljenih območij je potrebna njihova nadgradnja, kar je časovno in cenovno potratna rešitev, zato predstavlja uporaba obstoječih, že prisotnih in dostopnih omrežij boljšo rešitev.

Za razliko od fiksnih rešitev lahko Mobitelovo mobilno omrežje podpre vse fiksne kot tudi mobilne scenarije omrežij WSN na področju celotne Slovenije. Največjo pokritost s signalom nudi EDGE, ki pa vendar ne pokriva celotne površine Slovenije. Največja z EDGE nepokrita področja so npr. okolica Koprivne, Snežnika, Haloz, Mislinje, Stegovnika, Glažute in Loga pod Mangartom (glej Slika 2), ki so velika nekaj kvadratnih kilometrov. V primeru potrebe po postavitvi omrežja WSN ravno na enega izmed takšnih področij se lahko z enim ali več komunikacijskimi skoki med senzorskimi vozlišči, ki dosegajo tudi kilometrske povezave, vzpostavi povezavo do roba pokritosti s signalom EDGE, tam pa se uporabi prehod v mobilno omrežje. Tako lahko Mobitel komunikacijsko podpre postavitve senzorskih omrežij kjerkoli v državi in jim omogoči hiter ter cenovno ugoden dostop do hrbtenice. Takšno podporo omrežjem WSN s svojo infrastrukturo cenovno ugodno težko zagotovi katerakoli druga alternativna rešitev.

Združevanje omrežij WSN z mobilnimi omrežij lahko po drugi strani pripelje do ogromnega, v skrajnem primeru celo neobvladljivega števila podatkovnih povezav. Senzorska vozlišča se bodo vse pogosteje povezovala v mobilno omrežje in najverjetneje ustvarjala majhne količine podatkovnega prometa z veliko količino sinhronizacijske režije. Posledično bo v namen preprečitve zasičenosti potrebno uvesti primerne ukrepe, ki bodo to odpravljali.

Mobilni operaterji imajo dolgoletne izkušnje na področju uporabniškega prometa, saj so bila mobilna omrežja najprej zasnovana za komunikacijo med ljudmi (angl. Human-To-Human, H2H). Večanje podatkovnega prometa velikega števila senzorskih vozlišč bo zato korak v neznano, saj so vsa mobilna



Slika 2: Primer okvirne pokritosti oziroma nepokritosti s signalom EDGE v okolici Loga pod Mangartom cca. 2 × 25 km^2.

omrežja dimenzionirana za določeno zmogljivost. Za uspešno podporo omrežij WSN bodo mobilni operaterji morali izvesti temeljite analize svojih omrežij in trga ter z mnogo poskušanja in prilagajanja sproti odpravljati zaplete, ki bodo nastajali z vsakodnevnim večanjem senzorskega prometa. Promet senzorskih vozlišč za razliko od uporabnikov zahteva večjo pasovno širino na navzgornji kot na navzdoljni povezavi, zato bi bila s strani operaterjev smiselna uvedba priporočil za pisanje programske opreme povezovanja senzorskih vozlišč ter ostalih naprav v mobilna omrežja prihodnosti. Za razliko od uporabnikov se naprave ne morejo odzvati operaterju prijazno v primeru težav z omrežjem ali pokritostjo s signalom, zato bo potrebna detekcija in uvedba mehanizmov za odpravljanje nastalih težav na strani mobilnega omrežja. Potrebna bo tudi zamenjava in nadgradnja kritičnih infrastrukturnih elementov mobilnega omrežja ter določena standardizacija na področju ločevanja podatkovnega prometa, saj npr. komunikacija med napravami časovno kritičnih aplikacij zahteva višjo kvaliteto storitev kot komunikacija časovno nekritičnih aplikacij.

V. ZAKLJUČEK

V članku smo izpostavili naraščanje komunikacije med napravami in predstavili mogočo aktivno vlogo mobilnih omrežij pri integraciji z omrežji WSN. Predstavljeni sta bili tehnologiji mobilnih omrežij in omrežij WSN ter ključne točke njunega združevanja na stacionarnem delu mobilnega omrežja in na strani uporabniške terminalne opreme. Pokritost s signalom EDGE in ostalimi zvrstmi tretje generacije mobilnih komunikacij so glavna prednost pred ostalimi tipi fiksnih omrežij in zadoščajo potrebam tako fiksnih kot tudi mobilnih scenarijev omrežij WSN. V primeru potreb po postavitvi omrežij WSN na s signalom nepokritih področjih pa se lahko uporabi več skokov med senzorskimi vozlišči za dosego primernega prehoda v mobilno omrežje. Tako fiksni kot mobilni operaterji pa se morajo na integracijo z omrežji naprav vseh vrst temeljito pripravljati že danes.

ZAHVALE

Posebna zahvala gre Evropski uniji, ki iz Evropskega sklada za regionalni razvoj/Evropskega socialnega sklada/Kohezijskega sklada delno financira program usposabljanja mladega raziskovalca ter vsem sodelavcem za izkazano pomoč.

LITERATURA

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks: The International Journal of Computer and Telecommunications Networking,* Vol. 54, pp. 2787-2805, 2010.

[2] Ericsson. (2010, 14.3.2011). *Ericsson discussion paper: Towards 50 billion connected devices*. Available: http://www.ericsson.com/au/res/region_RASO/docs/2010/ericsson_50_billion_paper.pdf

[3] Ericsson. (2011, 14.3.2011). *Ericsson white paper: More than 50 billion connected devices*. Available: http://www1.ericsson.com/res/docs/whitepapers/wp-50-billions.pdf

[4] (2011, April 4). *Pravilnik o radijskih frekvencah, ki se smejo uporabljati brez odločbe o dodelitvi radijskih frekvenc*. Available: http://zakonodaja.gov.si/rpsi/r06/predpis_PRAV6466.html

[5] (2009, April 14). *DOCOMO to Launch Environmental Sensor Network Business*. Available: http://www.nttdocomo.com/pr/2009/001461.html

[6] (2011, April 14). *Sierra Wireless Embedded SIM*. Available: http://www.sierrawireless.com/en/productsandservices/AirPrime/Wireless_Modules/Embedded_SIM.aspx

Marko Pesko je diplomiral na Fakulteti za elektrotehniko na Univerzi v Ljubljani leta 2009. Zaposlen je v podjetju Mobitel, telekomunikacijske storitve, d. d. in kot mladi raziskovalec iz gospodarstva sodeluje z Odsekom za komunikacijske sisteme na Institutu Jožef Stefan. Njegova raziskovalna dejavnost so brezžična senzorska omrežja in njihovo povezovanje z mobilnimi omrežji naslednje generacije.

Luka Vidmar je diplomiral na Univerzi v Ljubljani leta 2008. Trenutno dela v podjetju Mobitel, telekomunikacijske storitve, d.d. in v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko Univerze v Ljubljani kot mladi raziskovalec iz gospodarstva. Njegova raziskovalna dejavnost med drugim vključuje tudi optimizacijo omrežij žičnega in brezžičnega širokopasovnega dostopa s poudarkom na metodah za premoščanje digitalnih vrzeli v Evropi.

Mitja Štular je diplomiral na Fakulteti za elektrotehniko in računalništvo na Univerzi v Ljubljani leta 1994. Istega leta je dobil prestižno slovensko študentsko nagrado za svoje raziskovalno delo na področju mobilnih komunikacij. Leta 1997 je uspešno zagovarjal svojo magistrsko nalogo in tri leta kasneje še doktorsko disertacijo, obe s področja telekomunikacij. Svojo kariero je v Mobitelu začel 2001. leta kot svetovalec izvršnega direktorja in vodja UMTS-projekta. Vključen je bil v številne raziskovalne in razvojne projekte tako doma kot tudi v tujini. 2006 je postal tehnični direktor podjetja, odgovoren za omrežja, storitve in IT ter 2009 višji strateški svetovalec izvršnega direktorja.

Predlog uvedbe davčno zanesljivih fiskalnih blagajn

Domen Baškovec, odgovoren za razvoj inovativnih poslovnih rešitev v podjetju Si.mobil d. d.

Povzetek — Davčne utaje ogrožajo javno finančne vire in slabijo konkurenčnost podjetij, ki poslujejo v skladu s predpisi. Si.mobil predstavlja učinkovito in preizkušeno rešitev davčno zanesljivih fiskalnih naprav na vseh gotovinskih plačilnih mestih v Republiki Sloveniji, in je kot tak tehnološki odgovor na enega izmed davčnih problemov. Predlog temelji na mobilnih komunikacijah in izkorišča prednosti, ki nam jih omogoča sodobna tehnologija.

Ključne besede — utaja DDV, fiskalne naprave, GPRS prenos podatkov, mobilne komunikacije

Abstract — Tax evasions are threatening public financial sources and weakening competitiveness of companies, which do business in compliance with regulations. Si.mobil is presenting efficient and tested solution of tax reliable fiscal devices on all cash POS in Republic of Slovenia, and as that, represents a technological answer on one of the tax-related problems. Proposal is based on mobile communications and is exploiting benefits of modern technologies.

Keywords — VAT evasion, fiscal devices, GPRS data transmission, mobile communications

I. UVOD

Ukrepi za preprečevanje davčnih utaj in z njimi povezani prestopki so v času finančne krize še bolj pomembni. Medtem ko mnoga podjetja vlagajo skrajne napore v obstoj na trgu in ohranjanje minimalnega nivoja konkurenčnosti, pa prenekateri gospodarski subjekti svojih davčnih obveznosti ne poravnavajo. Na ta način pa predstavljajo resno grožnjo pošteni konkurenci, zaradi zmanjšanega toka plačevanja davčnih obveznosti pa povzročajo tudi neposredno škodo državi.

Po oceni policije je v Sloveniji v letu 2009 skupna škoda iz naslova gospodarskih kaznivih dejanj presegla 190 milijonov evrov, od tega naj bi bilo med 100 in 130 milijonov evrov neposredno vezanih na utajo davka na dodano vrednost (DDV). Levji delež teh zlorab izhaja iz neposrednega gotovinskega poslovanja davčnih zavezancev, saj je stopnja nadzora pristojnih državnih služb in uradov (DURS, CURS, UPPD, MF, MZG, in drugi) nad posameznimi transakcijami v teh primerih nizka, možnosti zlorabe pa raznolike.

Zlorabe obračunavanja davka na dodano vrednost najpogosteje vključujejo prirejanje podatkov o gotovinskih denarnih tokovih davčnih zavezancev, med drugim ne-izdajanje računov davčnih zavezancev, naknadno brisanje že izstavljenih računov oziroma brisanje posamezni postavk računov in podobno, obenem pa zavezanci poskrbijo tudi za uničenje s tem povezane tiskane dokumentacije (računov). Tovrstne utaje zelo pogosto vključujejo tudi dobavitelje oziroma vzdrževalce davčnih blagajn in povezane programske opreme, ki omogočajo zgoraj opisane manipulacije podatkov o gotovinskem poslovanju. V skladu s Kazenskim zakonikom Republike Slovenije (KZ-1) se dobavitelje in vzdrževalce tako prirejenih davčnih blagajn oziroma programske opreme obravnava enako, kakor da bi kaznivo dejanje utaje davkov storili sami, pri čemer sme biti kazen bolj mila.

Vsem naštetim davčnim utajam je skupno, da jih je pri naknadnem davčnem nadzoru zelo težko odkriti in dokazati, oziroma je potrebna v dokaznih postopkih dobra povezava med različnimi državnimi uradi (npr. med DURS in UPPD) in dobro razdelane pravne omejitve in zakoni, kot nas učijo številni primeri dobre prakse v tujini (Švedska, Italija, Grčija idr.).

Vlada Republike Slovenije je na 104. seji, dne 21. 10. 2010, obravnavala poročilo posebej sestavljene "Medresorske delovne skupine za pripravo ukrepov za preprečevanje davčnih utaj pri poslovanju z gotovino" in sprejela sklep, da omenjena medresorska skupina do 30. 11. 2011 pripravi predloge sprememb in dopolnitev davčne zakonodaje, s ciljem zmanjševanja davčnih utaj in izboljšav možnosti pregona davčnih zavezancev.

Predlogi ukrepov vključujejo:

- predloge zakona za odvzem in obdavčitve na kakršen koli nezakonit ali protipraven način pridobljenega premoženja,
- predloge krepitve sodelovanja med DURS, CURS in UPPD,
- predloge ureditev gotovinskega poslovanja in omejitve gotovinskih transakcij nad določenim zneskom,
- predloge za pregon nedobrovernih dobaviteljev davčnih blagajn in povezane programske opreme, in
- izhodišča za razvoj davčne kulture v Sloveniji in promocijo predlaganih sprememb.

Večina zgoraj omenjenih predlogov je povsem v pristojnosti Vlade Republike Slovenije in povezanih strokovnih služb in uradov, mi pa bomo v nadaljevanju pogledali, kako lahko napore Vlade za zmanjševanje obsega utaj davkov in gospodarskega kriminala podpremo tehnološko – to pa je ureditev vprašanja nadzora nad davčnimi blagajnami in povezano programsko opremo.

II. DAVČNO ZANESLJIV BLAGAJNIŠKI SISTEM

V izogib manipuliranjem z davčnimi podatki v davčnih blagajnah v prihodnosti, predlagamo uvedbo fiskalnih naprav (davčne blagajne in davčni tiskalniki – zahteve za izdajo računov so pri obeh napravah enake) z novo, moderno arhitekturo, in sprejetje standardov, ki jih morajo izpolnjevati vse fiskalne naprave, ki jih uporabljajo davčni zavezanci, oziroma poslovni subjekti v Republiki Sloveniji. Na ta način bi nadzor nad fiskalnimi napravami sistematizirali in v veliki meri onemogočili manipuliranje z davčnimi podatki, kot je to, sicer v nasprotju z davčnimi predpisi, mogoče v trenutni ureditvi.

Fiskalne naprave bi v skladu z novo, moderno arhitekturo vključevale dva ločena sklopa komponent, in sicer moderni davčni terminal in zapečatena SD pomnilniška kartica. Vse opisane komponente so brez izjeme vgrajene in zaplombirane v ohišju fiskalnih naprav in kot take varne pred nepooblaščenimi posegi.

A. Davčni terminal

Moderni davčni terminal vsebuje naslednje komponente:
- procesor,
- ura s koledarjem in časom,
- obstojni pomnilnik in
- GPRS modem s pripadajočo SIM kartico.

Obstojni pomnilnik je sestavljen iz dveh ločenih modulov, ki imata tudi ločeno namembnost.

Prvi modul je namenjen shranjevanju poročila X fiskalne naprave, ki se osveži ob vsaki izdaji računa stranki, in je, prav tako kot sam obstojni pomnilnik, sestavljen iz dveh delov s podatki:
- prvi del je bil do sedaj namenjen zgolj poslovodjem trgovin in vsebuje podatke o številu strank, popustov, doplačil, prejemkov in izplačil, gotovinskem in kartičnem poslovanju itd., torej vrsto parametrov, pomembnih za preverjanje dela POS terminala,
- drugi del je namenjen beleženju podatkov o prometu po razredih DDV, ki jih davčna uprava uporablja za izračun DDV.

Drugi modul obstojnega pomnilnika se uporablja kot fiskalni pomnilnik, ki shranjuje vsakodnevno fiskalno poročilo Z, poleg tega pa vključuje poseben oddelek za shranjevanje identifikacijskih številk in drugih posebnih parametrov. Podobno kot poročilo X je tudi poročilo Z sestavljeno iz dveh delov s podatki:
- prvi del je namenjen poslovodstvu trgovin,
- drugi del pa shranjevanju podatkov o prometu po razredih DDV.

Poročilo Z se zapiše v fiskalni pomnilnik ob izdaji ukaza za tiskanje dnevnega poročila Z; takrat se podatki iz poročila X na prvem modulu v obliki dnevnega fiskalnega poročila Z shranijo na fiskalni pomnilnik naprave. Kapaciteta modula fiskalnega pomnilnika mora zadostovati za vsaj 1825 dnevnih poročil Z, oziroma 5 let rednega delovanja.

GPRS modem s pripadajočo SIM kartico omogoča dvosmerno komunikacijo med posameznimi fiskalnimi napravami in centralno lokacijo DURS, in pozna dva osnovna načina delovanja:
- prvi je privzeti način delovanja, ki se uporablja za prenos poročil Z iz fiskalnega pomnilnika na strežnik DURS v vnaprej določenih intervalih, običajno vsakih 14 dni,
- drugi je sekundarni način delovanja, ki se uporablja za prenos poročila X iz prvega pomnilniškega modula na strežnik DURS. Ta način delovanja se vklopi na zahtevo strežnika DURS, ki fiskalni napravi pošlje aktivacijsko SMS sporočilom, vključno s časom v katerem mora fiskalna naprava poslati sporočilo X na DURS (po vsaki izdaji računa, ali v poljubnih intervalih, izraženih v minutah)

Sekundarni način delovanja omogoča davčni upravi spletni nadzor izbranih fiskalnih naprav v realnem času, in se uporablja v primerih, ko obstaja sum, da fiskalna naprava ne zapiše vseh prodaj. Prav to pa je najbolj pogosta prevara v vseh državah – prodaja se ne zavede, posledično se ne vnese vsota DDV, in podjetje se izogne plačilu davka.

Na podlagi podatkov iz držav, ki so podobne sisteme že vpeljale (Srbija, Bolgarija, Albanija, BiH idr.), deluje cca. 90 % fiskalnih naprav v privzetem načinu delovanja, 10 % pa v načinu spletnega nadzora. Pomembno je dejstvo, da lahko oba načina delovanja na fiskalnih napravah preklapljamo s pošiljanjem SMS sporočil, posledica tega pa je, da je predlagan sistem izredno prilagodljiv. Opisan sistem omogoča davčnim inšpektorjem nadzor nad fiskalnimi napravami kar iz njihovih pisarn, obiske na terenu bi bilo potrebno opraviti samo v primerih utemeljenih sumov goljufanja glede DDV na prodajnem mestu.

B. SD pomnilniška kartica

SD pomnilniška kartica je nameščena pod pečatom fiskalne naprave, in je tako zaščitena pred nepooblaščenimi posegi, zamenja jo lahko samo uradni serviser. Uporablja se za zapisovanje vseh dokumentov, ki jih v dnevnik zapiše fiskalna naprava, in na ta način omogoča preverjanje podatkov o preteklih transakcij v primeru, ko obstaja sum zlorabe. Vsebina dokumentov je zaščitena pred spremembami in brisanjem s kontrolnima vsotama SHA1 in MDP5 za vsak dokument posebej, in s skupno kontrolno vsoto za dnevniški zapis. Pri vsakem dnevnem zapisu se ta skupna kontrolna vsota zapiše v poročilo Z, prek njega pa v fiskalni pomnilnik. Pomnilniška kartica SD mora

vsebovati dovolj pomnilnika za shranjevanje elektronskega dnevnika za eno leto, ob predpostavki intenzivnega delovanja fiskalne naprave.

III. Integracija sistema z Davčno Upravo Republike Slovenije

Davčna Uprava Republike Slovenije bi morala, po vzoru tujih držav, sama poskrbeti za pripravo centralnega strežnika DURS, kamor bi fiskalne naprave pošiljale informacije o poslovanju posameznega POS. Nacionalne davčne uprave zelo poredko predajo izdelavo tako pomembnega sistema v druge roke, in navadno so taki centralni davčni strežniki razviti in vzdrževani interno. Možen je tudi razvoj takega sistema v zasebnem podjetju, v tem primeru ocenjujemo stroške razvoja na okrog 100.000 EUR.

Komunikacija med posamezno fiskalno napravo in centralnim strežnikom DURS bi potekala izključno po zavarovanih in nadzorovanih komunikacijskih kanalih. Od fiskalne naprave do Si.mobila poteka komunikacija prek GPRS omrežja mobilnega operaterja, dodatno varnost bi zagotavljalo navidezno zasebno omrežje (VPN). Tok podatkov se nemudoma posreduje naprej, neposredno na DURS, z uporabo direktne optične ali mikrovalovne povezave, ki je ločena od javnega omrežja, in je vzpostavljena neposredno na relaciji Si.mobil – DURS. Komunikacijski kanali zagotavljajo visoko stopnjo zaščite in nadzora nad njimi.

IV. Vpeljava fiskalnih naprav na gotovinska plačilna mesta

Opisan pristop vključuje fiskalne naprave proizvajalca DATECS, ki je največji evropski proizvajalec fiskalnih naprav, s prek 20 letnimi izkušnjami in prek 1.400.000 prodanimi napravami.

Predlog predvideva možnost nadgradnje POS terminalov z zunanjo TAX enoto (v ločenem, zaplombiranem ohišju) v primerih, ko je to mogoče.

V večini primerov bo sicer potrebno stare elektronske blagajne (npr. v manjših trgovinah) zamenjati z novimi, fiskalnimi elektronskimi blagajnami. Na delovnih postajah je potrebno zamenjati standardne tiskalnike POS zamenjati s fiskalnimi tiskalniki. Starih elektronskih blagajn raznih proizvajalcev v večini primerov ni moč nadgraditi, predvsem zaradi:

- odsotnosti komunikacijskih priključkov,
- obstoječih zaščitnih sistemov, oziroma
- bi potrebovali za vsak poseg v davčno blagajno posebno dovoljenje in sodelovanje proizvajalca.

Ocenjujemo, da bi bilo razumno obdobje za zamenjavo, oziroma nadgradnjo vseh naprav v fiskalne naprave eno do dve leti. Dobavo fiskalnih naprav (v vrednosti med 200 in 500 EUR / napravo) bi zagotovil Si.mobil, skupaj s partnerskim podjetjem DATECS, partnerja bi skupaj odgovarjala tudi za integriteto opisanega sistema, ko bi bil ta vzpostavljen.

V. Varnostni vidiki predlagane rešitve

Predlagana rešitev upošteva sodobne varnostne smernice in tehnologije, in po uvedbi onemogoča manipulacijo davčnih blagajn in tiskalnikov kot se to dogaja sedaj. Popolnoma zavarovane so tudi komunikacijske poti na relaciji POS > Si.mobil > DURS in v obratno smer.

Predlagane fiskalne naprave so plombirane, vse komponente pa zapečatene in tako varne pred posegi. Poleg tega vsebujejo vse fiskalne naprave mikrokontrolerja in strojno programsko opremo, ki vsebuje postopke in procese samo-preverjanja med zagonom naprave in med pridobivanjem operativnega statusa naprave. V primeru ugotavljanja odstopanj, se naprava sama zaklene, kar dodatno preprečuje nepooblaščene posege v vdelano strojno opremo. Za nameček je programska strojna oprema (BIOS) zapisana v obstojen, enkratno zapisljiv pomnilnik, kar preprečuje nepooblaščene posege v vdelano programsko opremo.

Tudi fiskalni pomnilnik je obstojen pomnilnik. Sestavljen je iz običajnega pomnilnika Flash in varnega mikrokontrolerja, s katerim sta skupaj združena v en modul. Strojna in programska oprema sta zasnovana na način, da fiskalnega pomnilnika po zapisu podatkov ni mogoče na kakršenkoli način spreminjati. S tem se zagotovi istovetnost podatkov, ki ostanejo od nespremenjeni od izvorne transakcije.

Proizvodnja in upravljanje papirnih dokumentov se ob vpeljavi predlagane rešitve ne spremeni, fiskalne naprave še naprej tiskajo papirne dokumente za končne stranke in blagajnika. Dodatno se vsi papirni dokumenti shranijo v elektronski dnevnik, ki ga ponovno ni mogoče naknadno spreminjati, lahko pa ga v vsakem trenutku preverja Davčna uprava.

Predlagan sistem ne vsebuje dodatnega šifriranja podatkov ob prenosu, oziroma uporabe e-podpisa v komunikaciji. Ta dva ukrepa bi stroške sistema kar konkretno povečali:

- programiranje vsake fiskalne naprave z namenskim ključem in sistem certificiranja,
- vzpostavitev sistema ključev na DURS-u,
- močnejši procesorji v fiskalnih napravah in
- e-podpis poveča ceno fiskalne naprave.

Ob tem pa se pojavlja dvom o doprinosu k varnosti predlaganega sistema. GPRS komunikacija je zaščitena in kodirana že v osnovi, direktna povezava med Si.mobilom in DURS-om je prav tako kodirana in uporablja SSL-7 kodiran prenos podatkov. Na koncu pa, če pride do manipulacije s podatki v fiskalnih napravah, dodatno kodiranje povezave ne pomaga.

VI. DRUGE PREDNOSTI OPISANEGA SISTEMA

Opisani sistem nadzora fiskalnih naprav in z njimi povezanih transakcij, oziroma omejevanja davčnih utaj ima za Slovenski prostor mnoge prednosti:

– je v skladu z vsemi obstoječimi računovodskimi standardi,
– je v skladu z obstoječo davčno zakonodajo,
– omogoča hitro integracijo – cca. 6 mesecev od dneva pričetka projekta,
– omogoča dvosmerni nadzor nad fiskalnimi napravami, in preklapljanje načinov delovanja,
– uporablja dobro razvejene in poceni mobilne komunikacijske kanale.

Prav uporaba GPRS prenosa podatkov, oziroma mobilnih komunikacijskih kanalov je največja prednost opisanega sistema. Alternativna možnost je zgolj uporaba standardne internetne povezave, kjer pa obstaja kar nekaj varnostnih pomanjkljivosti, oziroma so funkcionalnosti sistema v tem primeru omejene.

V primeru uporabe internetne povezave bi morale biti komunikacije dodatno šifrirane, saj obstaja precej potencialnih varnostnih tveganj, če poteka komunikacija prek javnega omrežja in lahko kdorkoli poskuša vdreti v sistem. Prav tako prek internetne povezave ni mogoče uvesti načina spletnega nadzora nad fiskalnimi napravami, saj poteka komunikacija prek omrežij različnih internetnih ponudnikov, ki poleg tega uporabljajo mrežno opremo (npr. usmerjevalniki, stikala itd.) različnih proizvajalcev. Fiskalne naprave bi zato lahko delovale samo v primarnem načinu. Uporaba internetnih povezav prinaša še eno težavo, in sicer večje število internetnih ponudnikov, ki morajo sistem podpreti. Za mobilno rešitev lahko hitro poskrbijo trije pomembni mobilni operaterji.

Po drugi strani ima mobilni operater celovit nadzor nad svojim mobilnim omrežjem in uporabljeno mrežno opremo, komunikacija fiskalnih naprav in DURS-a pa mobilnega omrežja nikoli ne zapusti, ozirom prenos podatkov v nobeni točki ne poteka prek javno dostopnega omrežja.

Podatki so v GPRS prenosu že šifrirani in dodatno šifriranje ni potrebno; omrežje je ločeno od javnega; omogočena sta oba načina delovanja fiskalnih naprav; ne nazadnje pa bi morali sistem podpreti zgolj trije mobilni operaterji, ki so to sposobni narediti zelo hitro.

Kot dodana vrednost opisanemu sistemu je možna tudi izdelava namenske in ekskluzivne mobilne aplikacije za pametne telefone, namenjene uporabi za davčne inšpektorje. Aplikacija bi se prvenstveno uporabljala za izvajanje davčnih inšpekcij na terenu, saj bi bila povezana neposredno na DURS-ove sisteme, vsem inšpektorjem pa bi omogočala preverjanje pravilnosti izkazanih podatkov v realnem času. Aplikacija bi, tako kot celoten sistem, izpolnjevala varnostne kriterije.

VII. KRATKA PREDSTAVITEV PODJETJA DATECS IN PRAKSE V TUJINI

DATECS je zasebno Bolgarsko podjetje, in je največji proizvajalec fiskalnih naprav v Evropi. V več kot 20-letni zgodovini je podjetje prodalo že prek 1.400.000 fiskalnih enot v več kot 25 državah. DATECS ima vodilni tržni delež v vseh državah, ki uporabljajo fiskalne naprave z brezžično povezavo do strežnikov nacionalnih davčnih uprav in več kot 6-letne temeljite izkušnje s tega področja. Trenutno se ti sistemi uporabljajo v naslednjih državah: Srbija (prva država, ki je uvedla opisan sistem, leta 2005), Republika Srbska, Etiopija, Albanija, Kosovo, Tanzanija, Zimbabve, BiH in Bolgarija. Podatka o prihrankih iz naslova uvedbe podobnih sistemov v navedenih državah žal nimamo, saj državne davčne uprave običajno ne razkrivajo teh informacij.

Bolgarija uporablja fiskalne naprave DATECS-a od leta 1993 naprej, letos pa načrtujejo temeljito prenovo in posodobitev sistema z uvedbo brezžične povezave s strežnikom davčne uprave. Načrt prenove predvideva zamenjavo ali nadgradnjo blagajn v Bolgariji do 30. Marca 2012.

VIII. ZAKLJUČEK

Sistemi se od države do države rahlo razlikujejo, v našem predlogu pa smo uporabili DATECS-ove dolgoletne izkušnje iz drugih držav in najnovejša dognanja iz s področja mobilnih komunikacij in naprednih tehnologij.

Predlog ponuja logičen, zmogljiv in preprosto uporaben sistem boja proti utajevanju DDV-ja, ki izkorišča že razvita komercialna mobilna omrežja in je zato s stališča tehnologije cenovno dostopen in preprost za implementacijo, hkrati pa zadošča varnostnim in funkcionalnim kriterijem.

LITERATURA

[1] Poročilo medresorske delovne skupine za pripravo ukrepov za preprečevanje davčnih utaj pri poslovanju z gotovino – predlog za obravnavo, objavljeno dne 28. 2. 2011. http://www2.gov.si/upv/vladnagradiva-08.nsf/WEB2?OpenView

[2] Interni dokumenti družbe Si.mobil d. d.

Domen Baškovec je zaposlen na Si.mobilu, kjer deluje v Segmentu poslovnih uporabnikov, znotraj oddelka Marketing. Odgovoren je za razvoj in implementacije modernih, inovativnih poslovnih storitev in rešitev.

Internet stvari in mobilna omrežja

Primož Jenko, Iztok Saje, Mobitel, d. d.

Povzetek — Internet stvari (angleško Internet of Things) je termin, ki ga srečujemo v vsakdanjem življenju vse bolj pogosto, čeprav z njim živimo, sicer v zelo okrnjeni obliki, že nekaj časa, predvsem v obliki komunikacije med napravami (tudi M2M). Prenos podatkov med napravami uporablja mobilna omrežja že vrsto let. Do sedaj je bilo tovrstnega podatkovnega prometa razmeroma malo v primerjavi z uporabniškim prometom, ima pa ta promet izjemen potencial za rast, na kar se moramo mobilni operaterji ustrezno pripraviti. Prispevek obravnava vpliv Interneta stvari na mobilna omrežja, podaja dosedanje izkušnje s tega področja in nudi osnovne napotke snovalcem aplikacij za ustrezno in učinkovito rabo mobilnih omrežij.

Ključne besede — Internet stvari, M2M, mobilno paketno omrežje, UTRAN, HSPA+, EDGE, LTE/EPC, IPv6.

Abstract — Machine to machine communication (M2M), as one of the many eneablers of the grand Internet of Things, has been with us for some time now. Mobile networks in their many flavours have been used by M2M applications almost since the beginning of their evolution, from the first NMT modems to the sophisitcated HSPA and LTE terminals of today. By comparison to ordinary user traffic, the M2M traffic volume might seem small, but given its huge potential for growth and its different traffic caracteristics, mobile network operators should be prepared accordingly. The paper deals with the impact of the Internet of Things on mobile networks and offers, based on the experience to date, some basic guidelines to the interested application developers.

Keywords — Internet of Things, M2M, mobile packet-switched networks, UTRAN, HSPA+, EDGE, LTE/EPC, IPv6

I. Uvod

Tehnološki razvoj že danes teoretično omogoča medsebojno povezanost vseh naprav. Ericsson, denimo, napoveduje 50 milijard naprav povezanih preko mobilnih omrežji v roku desetih let [1] in podobne napovedi slišimo tudi drugod. V Mobitelu smo pred desetimi leti govorili o šestih milijonih terminalov v Sloveniji, kar je takrat izzvalo smeh; danes pa to počasi postaja resničnost. Mobilna omrežja so praviloma v prvi vrsti načrtovana za govorne storitve in v zadnjem času tudi kot nadomestek za fiksni dostop do medmrežja, za kar so značilne velike količine prenesenih podatkov in razmeroma nizke stopnje mobilnosti. Zaradi pričakovanega bistvenega povečanja števila naprav v omrežju, ki so signalizacijsko dejavnejša (Pametni telefoni, M2M), smo se odločili, da preverimo in ocenimo, kako so naša omrežja pripravljena na verjetne spremembe v prihodnosti. Ugotovili smo, da večina omrežij ima rezervo, obenem pa smo operaterji pripravili in izvedli ustrezne širitve kapacitete omrežij, kar pomeni, da smo na pričakovane spremembe pripravljeni. Trenutne količine prometa M2M so, kljub njegovi relativni razširjenosti, glede na celoten obseg prometa še vedno skoraj zanemarljive.

II. Vloga mobilnih radijskih omrežij v Internetu stvari

Ne glede na to, na katero definicijo Interneta stvari se naslonimo je jasno, da morajo biti stvari med seboj tako ali drugače povezane in ena od od možnosti je mobilni podatkovni prenos. Ta možnost je posebej privlačna, ker nudi mobilnost in je prisotna skoraj povsod, tudi tam, kjer ni obstoječe fiksne infrastrukture. Mobilni operaterji imajo pri tem možnost prevzeti aktivno vlogo kot ponudniki celovitih storitev, lahko pa zgolj zagotavljajo nosilne storitve v obliki prenosa podatkov, kar je predmet tega prispevka.

A. Prenos podatkov v mobilnih radijskih omrežjih

Marsikdo je že pred 20 leti prenašal podatke po omrežju NMT, omrežje GSM pa že od samega začetka ponuja storitev CSD (vodovno komutirani prenos podatkov). Obe sta primerljivi z modemskim dostopom po telefonski parici. Zaradi nizke prepustnosti je CSD primeren le za zelo specifične aplikacije in se danes le redko uporablja.

Prvi pravi paketni prenos se je pojavil v GSM s prihodom GPRS (splošna paketna radijska storitev), ki je bil kasneje nadgrajen še v EDGE. EDGE, v primerjavi z osnovnim GPRS nudi kompleksnejše kodne sheme in s tem višje prenosne hitrosti ter druge izboljšave.

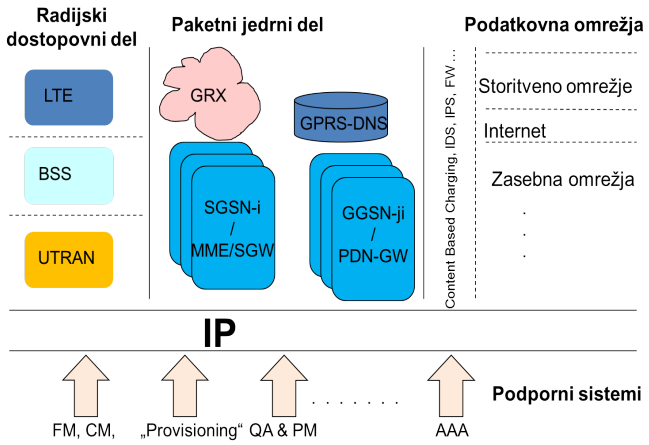
Za marsikatero storitev tudi danes še povsem zadošča tudi storitev kratkih sporočil (SMS), ki za prenos sporočil izkorišča izključno signalizacijske zmogljivosti.

Za doseganje višjih prenosnih hitrosti in boljše izrabe radijskega spektra smo uvedli tehnologijo HSPA+ (hitri paketni dostop), ki ponuja veliko višje vršne hitrosti in večjemu številu uporabnikov ponuja storitve, ki so že primerljive s tehnologijo ADSL. Tehnološki razvoj je omogočil prihajajoče sisteme LTE/LTEa, ki so/bodo še bolj učinkoviti in uporabnikom omogočajo hitrosti,ki so trenutno dosegljive le v optičnih dostopovnih omrežjih. V nadaljevanju se bomo osredotočili na mobilni paketni prenos podatkov

B. *Pregled arhitekture mobilnega paketnega omrežja*

Poesnostavljeno arhitekturo mobilnega paketnega omrežja delimo na štiri dele:

- Radijski dostopovni del
- Jedrni del
- Ciljna podatkovna omrežja
- Podporni sistemi



Slika 1: Mobilno paketno omrežje - poenostavljeno

Radijski del skrbi za dostop, jedrni pa za usmerjanje paketov, upravljanje sej, povezavo s ciljnimi omrežji, zaračunavanje ter upravljanje mobilnosti, vključno z mednarodnim gostovanjem. Ciljno omrežje (bodisi javni Internet, bodisi zasebno omrežje) se določi na podlagi zahtevane dostopne točke APN (angleško Access Point Name), ki je v obliki domenskega imena (primer: internet.mnc041.mcc293.gprs) in se razreši v posebej za to namenjenem strežniku DNS. Ta DNS je hkrati tudi del zasebne hierarhije DNS v okviru GSMA (GSM Association) in GRX (GPRS Roaming Exchange). GRX je zasebno podatkovno omrežje pod okriljem GSMA v katero se povezujejo mobilni operaterji za potrebe mednarodnega podatkovnega gostovanja. SGSN/MME/SGW se vedno nahajajo v obiskanem omrežju, GGSN/PD NGW pa v večini primerov v domačem omrežju.

C. *Prometne značilnosti različnih vrst rabe mobilnega omrežja*

Različne vrste rabe mobilnega omrežja za prenos podatkov izkazujejo različne prometne vzorce. Z vpeljavo za uporabnike zanimivih paketov z neomejenimi količinami podatkov se izrazito poveča volumen količine prenesenih podatkov, ki pa ga generira razmeroma majhen delež vseh uporabnikov. S prihodom pametnih telefonov je ta trend manj izrazit, obenem pa se signalizacijske obremenitve omrežja povečujejo.

Na tem mestu naj omenimo le osnovne vrste mobilnega prenosa podatkov:

- Mobilni dostop do Interneta/intraneta
- Zamenjava za fiksni dostop do Interneta
- Aplikacije M2M (sledenje vozil, upravljanje voznega parka, odbiranje števcev na daljavo, transakcije)
- Pametni telefoni

Tabela 1: Osnovne značilnosti različnih vrst rabe

Raba	sig	podatki	mobilnost
mobilni	srednje	srednje	da
WWW	malo	veliko	nizka
cest	malo*	malo	da/ne*
FM	veliko	malo	visoka
MPAY	veliko	malo	nizka
SPH	veliko	veliko	visoka
števci	malo*	malo	ne
Video	malo	veliko	ne*

V gornji preglednici (Tabela 1) je podan pregled osnovnih značilnosti posameznih vrst uporabe. Zvezdica pomeni, da se lastnost lahko razlikuje, glede na namen. Pri mobilnem dostopu je poglavitna lastnost mobilnost, kjer je lahko količina prenesenih podatkov različna, gre pa bodisi za dostop da storitev znotraj storitvenega omrežja operaterja in/ali Interneta, oziroma za neposreden dostop do zasebnega lokalnega omrežja/intraneta z uporabo posebne, zasebne dostopovne točke APN (angleško Access Point Name). Slednje je predvsem uporabno za agente in kurirje na terenu. Ta vrsta uporabe omrežja ne obremenjuje pretirano, ne v signalizacijskem pogledu ne po količini podatkovnega prometa.

Za substitucijsko storitev (zamenjava za fiksni dostop - WWW) so značilne nizka signalizacijska obremenitev, izjemno velike količine prenesenih podatkov in zelo nizka, včasih celo nična, stopnja mobilnosti. še posebej je zanimiva povsod tam, kjer ni razpoložljive fiksne infrastrukture.

Aplikacije M2M (števci, MPAY, FM upravljanje flote, cestninjenje, video nadzor) so po svojem prometnem odtisu lahko med seboj zelo različne v smislu mobilnosti, signalizacijske obremenitve za omrežje in količine prenesenih podatkov. Bistvena lastnost teh aplikacij je zmožnost koordiniranega delovanja kar pomeni potencialno grožnjo za samo storitev in omrežje kot celoto. Aplikacije M2M NE SMEJO biti sprožene, nastavljene na oddajanje, poizvedovati NAENKRAT za vse terminale. Zaželena je popolna naključnost, kar je treba upoštevati pri načrtovanju aplikacije.

V vseh omrežjih po svetu se pojavlja vse več pametnih telefonov (SPH), ki pomembno prispevajo k višji obremenitvi mobilnih omrežij, tako po količini prenesenih podatkov, kot signalizacijsko. Dodatno signalizacijsko obremenitev povzroča hitro prekinjanje povezave (Fast Dormancy), ki jo uporablja vse več novih terminalov z namenom zmanjševanja porabe energije bater-

ije. Pametni telefoni so pomembni s stališča Interneta stvari zaradi množice vgrajenih senzorjev (pozicija, temperatura, jakost signala itd).

D. Izzivi, ki jih pred operaterje postavlja Internet stvari

Glavni, in za operaterje najpomembnejši, izziv, ki ga pred operaterje postavlja Internet stvari je možnost, da število medsebojno povezanih naprav lahko nekajkrat preseže velikost populacije. To je za mobilne operaterje velika priložnost, in hkrati izziv na katerega se je treba ustrezno pripraviti.
Predvsem je pomembno to, da se snovalci aplikacij M2M zavedajo omejitev, ki so specifične za mobilno radijsko okolje in da zrak ni kabel ter da zmogljivosti radijskega vmesnika niso skoraj neomejene. Kot smo uvodoma spoznali, imajo različne aplikacije različne značilnosti in zahteve. Omrežja je možno optimirati za različne prometne profile, pri čemer pa vemo, da imamo vedno opravka z mešanico različnih storitev z različnimi prometnimi profili.

Mobilna omrežja, denimo, lahko optimiramo glede na:
- čim večjo prepustnost prometa ali PPS
- število aktivnih uporabnikov
- čim višjo signalizacijsko zmogljivost
- drugo (zakasnitve, vršne hitrosti, mehanizme kakovosti storitve ...)
- kombinacijo navedenega

V kontekstu komunikacije med napravami je pričakovati predvsem porast števila aktivnih uporabnikov ter povečanje signalizacijskega prometa. S povečanjem števila uporabnikov naraste tudi potreba po naslovnem prostoru, kar v okolju mobilnih operaterjev pomeni identitete kot so IMSI in MSISDN ter naslovi IP. Naslovi IP verzije 4 hitro pohajajo, zato je za uporabo v aplikacijah M2M protokol IPv6 odlična izbira: Poleg tega, da nudi zadosti velik naslovni prostor tudi ni predvidevati velikih potreb po pretvorbi med verzijami (NAT64), čemur smo sicer priča pri uporabniškem dostopu do Interneta zaradi pomanjkanja vsebin, dostopnih po IPv6. V kolikor za potrebe komunikacij med napravami uporabimo paketno omrežje za neposreden dostop do zasebnega omrežja je seveda možna uporaba zasebnih IP-naslovov. Za aplikacije M2M je značilno tudi to, da je ponor informacij na obeh koncih naprava in ne človek. Ta pa se ne zna odzvati na razna obvestila po SMS-ih oziroma ne zna sama ročno izbrati/zamenjati omrežja v tujini, v kolikor se v danem tujem omrežju pojavijo težave.

E. Odziv mobilnih operaterjev in proizvajalcev telekomunikacijske opreme na pričakovane spremembe

Mobilni operaterj se pripravljajo na pričakovano rast števila povezanih naprav in uporabnikov predvsem s širitvijo signalizacijskih in podatkovnih kapacitet in vpeljavo različnih mehanizmov kakovosti storitev, predvsem glede na pričakovano vrsto rabe mobilnega omrežja. Pri tem se morajo seveda zanesti tudi na proizvajalce opreme. Ti v veliki meri sledijo pričakovanim trendom, pa tudi standardizacija nam stoji ob strani.
Pri tem gre predvsem:
- Za povečevanje procesorske in usmerjevalniške zmogljivosti za en velikostni razred ob nespremenjenem volumnu opreme
- zmanjševanje števila fizičnih omrežnih elementov v podatkovni ravnini (3GDT, LTE/EPC)
- možnost spreminjanja razmerja preklopne in signaizacijske zmogljivosti
- možnost zavračanja signalizacijskega prometa napačno skonfiguriranih terminalov

III. Primeri aplikacij M2M

Ena od možnih delitev aplikacij M2M glede na namen uporabe [2] je:
- spremljanje in sledenje (npr. upravljanje voznega parka)
- monitoring (npr. odbiranje števcev)
- transakcije (npr. POS, mobilno plačevanje)
- nadzor naprav (npr. prodajni avtomati)

Večina sedanjih aplikacij je razvitih za uporabno na fiksnem Internetu, kjer so mobilna omrežja le nadomestek fiksnim. Poglavitna lastnost mobilnih omrežij pa je prav mobilnost, ki omogoča internetni dostop tudi tam, kjer fiksni ni možen. Posebej privlačna so mobilna omrežja v povezavi z GPS in določanjem pozicije terminala. Poleg aplikacij za pametne telefone, je tudi vse več naprav, ki imajo vgrajen mobilni terminal. Uporabnik pogosto niti ne ve, da uporablja mobilna omrežja, saj ga zanima le storitev ne pa tudi tehnologija. Slednje pa v kontekstu interneta stvari ne sme veljati za snovalce aplikacij.

A. Ponujanje vsebin

Amazon.com ima v svoj elektronski bralnik Kindle vgrajen terminal 3G. Ob nakupu nove knjige se slednja prenese v bralnik brez uporabnikovega posredovanja.

B. Spremljanje vozil

Povezava vozil z mobilnimi omrežji je že davno presegla zgolj zaščitno oziroma varnostno funkcijo. Danes imajo tovornjaki, taksi vozila, kurirji in drugi stalno povezavo s svojim podjetjem, kar omogoča ne le spremljanja vozil temveč tudi učinkovito načrtovanje poti, razporejanje zmogljivosti ter samodejno posredovanje dokumentov, če naštejemo le nekaj prednosti. Tudi prihajajoči sistemi cestninjenja bodo predvidoma temeljili na napravah, vgrajenih v vsako vozilo na slovenskih avtocestah, ki bodo brezžično posredovali podatke in velik

del tega prometa bo predvidoma opravljen preko mobilnih omrežij.

C. Daljinsko odčitavanje števcev

Danes želimo čim hitreje in pogosto odčitavati stanja najrazličnejših števcev, od električne energije, do vode plina in podobnega. Posebej zanimivi so sistemi, ki združujejo večje število števcev skozi eno podatkovno povezavo.

D. Telemetrija

Poleg spremljanja vozil in odčitavanja števcev obstaja še cela vrsta manjših sistemov, na primer spremljanje gibanja živali, varnostni sistemi v zgradbah, daljinski nadzor naprav in podobno. Tu uporabnik sam postavi in medsebojno poveže naprave pri čemer lahko uporabii mobilni prenos podatkov.

E. Diferencialni GPS

Ena prvih storitev je bila diferencialni GPS, ki izboljšuje točnost odčitane lokacije, kar je nujno za geodetske meritve. Pri DGPS je uporaba CSD in HSCSD povezav pogosta, saj se s tem poveča zanesljivost povezave ter zmanjša trepetanje obhodnega časa.

IV. EDGE, da ali ne?

Kljub temu, da gradimo omrežja HSPA+ in LTE, večina terminalov M2M uporablja le EDGE. EDGE ponuja povsem zadovoljivo uporabniško izkušnjo in poleg tega so terminali HSPA+ opazno dražji, kar ni zanemarljivo pri izvedbah, ki terjajo velike količine terminalov. Za operaterja je EDGE zanimiv le dokler podatkovni promet izrablja proste kapacitete omrežja GSM. Ko se podatkovni promet na tehnologiji EDGE poveča in zahteva širitev celic GSM z dodatnimi oddajniki in sprejemniki, postane cena za prenos podatkov lahko tudi nesprejemljivo visoka, v vsakem primeru pa višja, kot pri HSPA+ in LTE. Zato mora v kratkem priti do znižanja cen naprav HSPA+ in LTE, operaterji pa morajo spodbujati prehod storitev M2M na omrežja tretje generacije (UMTS, HSPA).

V. Izkušnje in priporočila

A. M2M in izkušnje operaterjev

V primerjavi s fiksnim dostopom izkazujejo mobilna paketna omrežja naslednje lastnosti:

- Omogočajo mobilnost
- Razmere so veliko bolj dinamične, radijski signal je zaradi mobilnosti in presiha spremenljiv in nepredvidljiv
- Zakasnitve so spremenljive in višje*
- Prenosne hitrosti so nižje*
- Celotne zmogljivosti si deli večje število uporabnikov
- Zaračunava se količina prenesenih podatkov*

*To danes ne velja več nujno

Večino težav, ki so izhajale predvsem iz specifičnosti mobilnih omrežij so razvijalci aplikacij M2M večinoma odpravili že v prvih dveh letih po prihodu mobilnih paketnih omrežij. Začetne težave so bile predvsem:

- Nesposobnost samodejnega restarta terminalov
- Nezanesljivost nekaterih različic terminalov
- Neprilagojenost aplikacij na drugačne lastnosti povezave
- Prevelik MTU ob uporabi tunelskih tehnologij za nekatere aplikacije
- Preveliko število aktivacij za malo podatkov; problematično v tujini zaradi velikih obračunskih enot

Še vedno pa so potencialno prisotne:

- Nezmožnost ročne izbire omrežja v tujini
- Nezmožnost odziva na opozorila/nastavitve po SMS
- Restart usmerjevalnika z vgrajenim terminalom ne restarta samega terminala

B. Priporočila snovalcem in razvijalcem aplikacij

Veliko slovenskih razvijalcev storitev M2M, ki imajo izkušnje z mobilnim omrežjem, se danes že dobro zaveda razlik med fiksnimi povezavami in mobilnimi omrežji. Prihajajo pa tudi novi, ki se s tovrstno problematiko srečujejo prvič. če se testiranja izvajajo na stalnih in hitrih povezavah po ethernet-u, ne zajemajo specifičnosti mobilnih omrežij. Poznavanje delovanja mobilnih omrežij pa vodi v učinkovito uporabo radijskih zmogljivosti in tako napisane aplikacije delujejo veliko zanesljiveje in so sprejemljive za končnega uporabnika.

C. Učinkovita raba omrežij

Poleg dejanskega prometa, omrežje pogosto obremenjuje tudi signalizacija. Pogosto vzpostavljanje kratkih sej in neregularne prekinitve le teh (denimo, z izklopom napajanja terminala) obremenjujejo omrežja z nepotrebno signalizacijo, na samo delovanje storitve pa nimajo bistvenega vpliva. Neprimerna so tudi za gostovanje, kjer se lahko zgodi, da tuji operaterji uporabijo velike začetne obračunske količine (denimo prvih 100kB, naprej pa na kB)

D. Robustnost aplikacij

Radijski sistemi z velikim številom uporabnikov ne morejo delovati brez krajših prekinitev povezave, po navadi zaradi prehajanja med celicami ali med elementi jedrnega omrežja (SGSN). Aplikacije morajo preživeti izpade dolge tudi nekaj sekund in več. Najenostavnejši preizkus je, da, v kolikor testiramo preko ethernet-a, iztaknemo kabel iz naprave in počakamo 20 sekund. S tem preverimo, ali je aplikacija napisana dovolj robustno.

E. Mednarodno gostovanje

Večina terminalov se vedno najprej prijavi v vodovno komutirani del omrežja (CS), šele kasneje v paketno komutirani del (PS). Mehanizmi samodejne izbire omrežja v gostovanju so pretežno optimirani za vodovno komutirane storitve, zato se lahko zgodi, da se terminal prijavi v omrežje, v katerem paketne storitve delujejo bistveno slabše kot v domačem omrežju ali pa sploh ni vzpostavljenega gostovanja za PS. V tem primeru bi bila dobrodošla samoiniciativna ročna izbira omrežja, brez posredovanja uporabnika, ki največkrat te možnosti tudi nima. (Denimo, izpis omrežij, ki so na voljo in nato izbira prvega naslednjega z ukazom at+cops, pri terminalih, ki to podpirajo).

F. Samodejni restart terminala z odvzemom napajanja

Vsi terminali niso enako zanesljivi in, tako kot telefoni, potrebujejo občasen restart z odvzemom napajanja, ko je terminal določen čas neodziven. Vsi ki to upoštevajo jim je prihranjen marsikak obisk oddaljenih lokacij. To seveda sodi tudi k povečanju robustnosti rešitve.

G. Testiranje v različnih radijskih in prometnih pogojih

Lahko se zgodi, da napravo/aplikacijo testiramo na mizi v laboratoriju, kjer vladajo ugodni radijski in prometni pogoji, ko pa jo postavimo v avtomobil ali na oddaljeno lokacijo, se delovanje spremeni. Pri tem je pomembna izbira ustreznega terminala in testiranje v različnih pogojih in v čim več različnih omrežjih.

H. Izbira ustreznega terminala

Tudi mobilni podatkovni terminali se razlikujejo po kakovosti, stabilnosti, skladnosti in so različno odporni na zunanje motnje, zato je predhodno testiranje in izbira ustreznega terminala upravičena, še posebej v rešitvah ki vključujejo veliko število mobilnih terminalov.

I. Zasebna dostopna točka APN

Kadar gre za rešitve z večjim številom terminalov je smiselno razmisliti o uporabi zasebne dostopne točke APN, preko katere se je možno povezati v poljubo zasebno omrežje, bodisi po najeti povezavi, bodisi po IPSecu

J. HSPA+ in LTE

čeprav danes EDGE zadošča za večino potreb M2M, so za njih veliko primernejša omrežja tretje in četrte generacije, saj so ta omrežja načrtovana za veliko število terminalov in omogočajo bistveno višje vršne hitrosti, ki se med njih deli. Naprave, ki podpirajo le GPRS in EDGE, bodo kmalu zastarele in jih bo treba zamenjati z novimi.

VI. Zaključek

Današnji razvoj mobilnih komunikacij gre predvsem v smeri doseganja čim višjih prenosnih hitrosti, pri čemer pa je trenutni trend rast števila pametnih telefonov in aplikacij M2M. Oba segmenta pomembno prispevata k povečanju razmerja med signalizacijo in dejansko opravljenim prometom. Ob doseganju čim višjih vršnih prenosnih kapacitet je enako pomembno tudi čim bolj učinkovito dodeljevanje le teh velikemu številu različnih uporabnikov, kar nove tehnologije zagotavljajo s povečevanjem granulacije virov, ki jih dodeljujejo. Zmogljivosti radijskega vmesnika niso neomejene, zato sta zasnova in primerno načrtovanje aplikacij odločilnega pomena za uspeh aplikacij M2M v mobilnih okoljih. Veliko primerov dobrih praks iz preteklosti potrjuje, da je to možno in izjemno učinkovito v kolikor upoštevamo vse značilnosti mobilnega okolja. Mobilna omrežja so pripravljena za napovedano hitro rast števila naprav in prometa. Proizvajalci terminalov morajo odpraviti pretirano razliko v ceni modulov za vgradnjo, ki marsikaterega razvijalca odvrne od HSPA+. Naloga operaterjev je vzpodbuditi uporabo omrežij tretje in četrte generacije ter razvijalcem posredovati znanja s stališča omrežja, ki so nujna za razvoj učinkovitih in robustnih storitev.

Literatura

[1] Ericsson, *http://www.ericsson.com/news/110214_more_than_50_billion_244188811_c*. Feb 14, 2011

[2] ETSI TS 102 689, *Machine-to-Machine communications (M2M); M2M service requirements*. V1.1.1 (2010-08)

[3] ETSI TR 102 691, *Machine-to-Machine communications (M2M); Smart Metering Use Cases*. V1.1.1 (2010-05)

[4] 3GPP TS 22.368, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Machine-Type Communications (MTC); Stage 1 (Release 10)*. V10.4.0 (2011-03)

Primož Jenko univ. dipl. ing. elektrotehnike, je zaposlen v družbi Mobitel, v Sektorju za paketna omrežja. Ukvarja se z razvojem, načrtovanjem in testiranjem jedrnega dela mobilnega paketnega omrežja.

Iztok Saje univ. dipl. ing. elektrotehnike, vodi Sektor za radijska omrežja v družbi Mobitel, kjer od leta 1992 sodeluje pri načrtovanju, izgradnji in optimizaciji radijskih dostopovnih omrežij. Iztok Saje predava na Višji strokovni šoli za telekomunikacije v Ljubljani.

Security and Data Protection in the Internet of Things

Petr Pavlu, Cisco Systems, Emerging Markets, East

Abstract — This article highlights some of the key considerations related to the security and data protection in the Internet of Things. It looks at some of the security aspects that are specific to dense network of devices, sensors and objects, and it also relates them to security challenges in more traditional (i.e. current) networks. Ensuring proper Security in IoT environments requires current networks to be prepared for a mass of connected devices, and apply security techniques that can accommodate the diversity, scale and ubiquity that characterize IoT.

Keywords — Security, protection, threats

I. INTRODUCTION

There are multiple definitions of the concept of IoT (Internet of Things), brought by various works, often depending on the specific view and level of detail being observed (e.g. [1], [2], [3]).

Looking at IoT from the networking perspective, it can generally be characterized as a pervasive and ubiquitous network, which enables multiple functions – like monitoring and control of our physical environment – by collecting, processing, and analyzing the data generated by smart objects.

While connecting rather specific class of devices (smart objects, sensors, etc.), and using some specific technologies and protocols, IoT is eventually a data network, or in fact an extension to the existing networking environment.

The natural demand for scale, simplicity, end-to-end capabilities and integration to existing network environments makes IP a very suitable and effective paradigm for IoT. And similarly many parts of security and data protection can be extended from the existing IP networks to the networks of smart objects, on top of the specific considerations.

IoT will eventually become another domain of networking environment. This means that most of the aspects of IoT (including security and data protection) should be discussed and considered in the context of current networking practices. And it also means that the current networks should be designed and deployed in a manner that will enable a smooth and seamless integration of IoT when it becomes due.

II. SECURITY IN IOT

There are several variants of the structure of networking stack in smart objects. The stack of the smart object is designed to work on several types of media technologies, like IEEE 802.15.4, IEEE 1901, IEEE 802.11, and IEEE 802.3. Thus, all of the functions required to communicate with other objects through the networks are basically integrated into the network layers. That applies to Security protocols as well.

This integration takes the path of adapting many known techniques, technologies and protocols to the conditions and capabilities of smart objects and devices (e.g., IEEE 802.15.4, IETF *6lowpan*[1] Working Group, IETF *roll*[2] Working Group). In many instances, known and proven protocols and technologies are used and considered to ensure security (e.g., IPSec, TLS, DTLS).

Multiple IETF drafts (especially under the 6lowpan working group) are dealing specifically with security aspects of the IoT - *draft-daniel-6lowpan-security-analysis*, *draft-qiu-6lowpan-secure-router*, *draft-sarikaya-6lowpan-cgand* and others.

While the networking aspects of security in these networks can be and are handled as an evolution and development of known security technologies and practices, there are some additional considerations that should be taken in relation to security of IoT.

For example, the smart object phenomenon is bringing network intelligence to devices and systems that have traditionally been produced with little or no awareness of communication security (e.g. medical devices, consumer electronics products, utility metering devices, etc.). This new aspect of integration might initially bring specific security risks due to unexpected ways of usage, lack of experience, etc. However, this area is beyond the scope of networking security discussion.

III. GETTING IOT CONNECTED

There are important aspects that make the IoT networks specific communication and networking environment. The endpoints have limited computing

[1] IPv6 over Lowe power WPAN
[2] Routing over Low power and Lossy networks

power and intelligence, they need to have limited power consumption, they are supposed to act unattended, etc. Still, the main value will come from having IoT connected to the »traditional« networks.

Therefore it is appropriate to ask what might be the impact to the existing networks when the massive networks of objects connect to them, what can/should be done even today to get the networks prepared for it, and examine that from Security perspective.

To large extent, one may view the future proliferation of IoT as a continuation and acceleration of the trend that we are already observing now and living through it.

There is an ongoing expansion of »regular« networking devices that are connecting to the network: smart phones, tablets, digital cameras, they are all joining the networks in huge quantities (magnitude of billions per year), creating multiple challenges for the traditional ways of designing, operating and securing network infrastructures.

Under these circumstances there is a strong urgency to take a fresh look at the architecture of networks and their security today. And this urgency is only increased by the outlook of IoT coming.

IV. Delivering on Diverse Needs

Looking at some of the requirements and expectations, they seem to indicate and force some decisions to be made in an »either-or« way. Scale or simplicity? Openess or security? Dynamic or Controlled?

While these questions are legitimate to ask, the author believes that successful architectures must not fall into the trap of »either-or« view. Instead, they need to strive for finding new ways (technologies, design practices, tools, protocols) to satisfy such requirements and expectations in a »both« fashion.

A. Scale and Simplicity

The scale of the networks is mostly measured by their performance, capacity, number of connected devices and other metrics. The default view is that when the scale of network grows, the complexity increases. And hence there is a natural limit for the network scale.

Avoiding such limits requires a change of paradigm. In this context, it requires the combination of intelligence built into the network with management and control mechanisms that will be much more than before based on rules and policies.

Network architectures (cf. [4]) that follow the principles of built-in intelligence and policy control will have more room to scale while keeping the complexity (and associated costs) at manageable level. It will require new approaches and techniques to be applied – e.g. endorsing new dimensions and parameters into policy definitions (not only who, but also what device, from what location, what time of day – cf. [5]), »teaching« the network elements to automatically enforce the policy across the infrastructure at the time of connection and follow through changes as necessary, etc.

B. Open and Secure

The network as an interconnection environment should be able to connect anyone, anything, from any place, at any time. However, this needs to be done in a very secure manner.

Delivering on both expectations requires again new techniques and mechanisms. It is not feasible any more to rely on selected places in the network that will enforce the security rules and policies. With users and devices connecting dynamically (especially in mobile environment and wireless networks) and with the simplicity mandate in mind, the whole network needs to become a grid of security enforcement and control.

There is a need to build new security mechanisms into the network so that it is possible not only to authenticate and authorize a user or a device, but also to apply security measures to this user's or device's communication anywhere in the network (in the access, at the aggregation point, at the datacenter, etc.).

One attempt to build such Security paradigm is the *Secure Group Tagging* mechanism (cf. [6]) within Cisco *TrustSec* service. It enables to tag individual data packets by security marks based on the user/device identity, to carry this security »stamp« across the whole network, and consequently to enforce security measures at any network element.

C. Dynamic and Controlled

Networks need to be able to react dynamically to the changes, to connected endpoints and to other situations that may appear (failures, changes in performance/capacity, etc.). In principle, any static information, e.g., a manual action of the administrator, needed for the network to adapt to new/changed situation (within the scope of regular operation) decreases network availability and reliability. At the same time, there must be enough power in the administrator's hand to control the network, implement updates and optimize the operation.

This leads to a need for a high level of automation in the network itself and in the management and control tools. Again the built-in network intelligence is the key factor that can enable this capability, together with network administration tools that support relevant operational workflows and that are closely integrated with the policy definitions and enforcement points.

V. CONCLUSION

The Internet of Things is a concept that defines massive sets of devices, which are going to be interconnected by a networking environment. Security is one of the critical aspects of this interconnection, especially given the scale and variety of endpoints that IoT deals with.

However, while specific in many aspects, it can be recognized that IoT is actually a continuation of trends and developments that are already ongoing.

Therefore the best way to prepare for IoT and for their attachment to existing networks is to design and enhance the current network and security architectures in a way that allows them to scale by simplicity, enable widest connectivity in a secure manner, and provide dynamic environments without compromising on control mechanisms.

REFERENCES

[1] The Internet of Things, ITU report (summary), November 2005.
[2] Vision and Challenges for Realising the Internet of Things, IERC report, March 2010.
[3] "The Internet of Things: Anywhere, Anytime, Anything", GigaOM report, July 2010.
[4] Cisco Borderless Network Architecture – An Overview
[5] Cisco SecureX Architecture – An Overview
[6] Cisco TrustSec Security Group Access – Solution Configuration Guide

Petr Pavlu has been working in Cisco Systems since 1998 in various international teams, supporting channel partners and customers in different regions, primarily Central and Eastern Europe. He has been responsible for technical sales support, consulting and systems engineering team management. He currently leads the Cisco Borderless Networks Architecture team that covers region of Emerging Markets, East.

Low-Latency in Wireless Communication

Navid NIKAEIN[1], Raymond KNOPP[1,] Antonio Maria CIPRIANO[2]
Srdjan KRCO[3], Igor TOMIC[3], Philipp SVOBODA[4], Markus LANER[4], Eric LARSSON[5], Yi WU[5], Manuel GARCIA FUERTES[6], Janie BAÑOS[6], Nenad ZELJKOVIC[7], Djordje MAROVIC[7], Divna VUCKOVIC[3]
[1]Eurecom, 06504 Sophia Antipolis, France
[2]Thales Communications, Colombes, 92704, France
[3]Ericsson d.o.o, Novi Beograd, 11070, Serbia
[4]Technical University of Vienna, Vienna, Austria
[4]Linköping University, Linköping, Sweden
[6]AT4WIRELES, Malaga, 29590 Spain
[7]Telekom Srbija a.d., Beograd, 11070 Serbia

Abstract — This paper focus is on access-layer technologies targeting low-latency robust and spectrally-efficient transmission in a set of emerging application scenarios. Two basic types of wireless networks are considered, namely long-term LTE-Advanced cellular networks and medium-range rapidly deployable mesh networks. In cellular networks, research is focused on transmission technologies in support of gaming services which will undoubtedly prove to be a strategic revenue area for operators in the years to come. We also consider machine-to-machine (M2M) applications in mobile environments using sensors connected to public infrastructure (in train, buses, stations, etc.).

Keywords — Latency, LTE, LTE-A, M2M Communication Scenario, Interactive Gaming, Real-Time Application, System Architecture

I. INTRODUCTION

Latency is a major factor influencing the experience of user, machine, and any form of communicating from the application used. The majority of applications will not benefit much from lower latency than that offered by LTE, or at least users would likely not be willing to accept increased subscription rates for this feature. Important exceptions to this, however, are interactive multi-player gaming applications which, from an operator's perspective, represent a very strategic application area with respect to revenue potential. In addition, for realtime machine-to-machine (M2M) applications in the area of intelligent transport system, remote monitoring and health will be also requiring very low latency and are become the main focus of many mobile and IT operators and vendors as a new revenue opportunity.

In the following subsections, first, we provide the basic notion of latency followed by a set of low latency application scenarios for both M2M and gaming. Then, the M2M and gaming traffic characteristics are analyzed. Finally, a set of measurement is carried out to study the delay and traffic for online gaming scenario, and some techniques are presented to reduce the latency at the access layer.

II. NOTIONS OF LATENCY

One of the important design objectives of LTE/LTE-A (and to some extent HSPA) has been to reduce the network latency. Network latency consists of both c-plane and u-plane latency.

In the 3GPP Literature [4], the c-plane latency can be defined as the time taken by the first packet to successfully reach the receiver reference point. In LTE/LTE-A, the c-plane latency is defined as a transition time between two states, IDLE or DRX to ACTIVE. Typically, in LTE/LTE-A the transition time from IDLE to ACTIVE state should be less than 100ms, and from DRX to ACTIVE state depends on the DRX cycle. The user plane latency, also known as transport delay, is defined as the one-way transit time between a packet being available at the IP layer of the sender and the availability of this packet at the IP layer of the receiver. In LTE/LTE-A, this latency is defined between the UE and EPC edge nodes. LTE/LTE-A specifications target the user-plane latency of less than 5ms in unloaded condition (single user with single data stream) for a small IP packet with no payload.

However, latency can also be interpreted in terms of the efficiency of very low-layer procedures allowing for time/frequency synchronization, identification/authentication, channel setup time, channel interleaving, channel code block length, etc. These are all fundamentally related to signaling

overhead and channel-code complexity (i.e. block-length) in the access stratum. The majority of wireless systems, including LTE, are designed for a continuous flow of information, at least in terms of the time-scales needed to send several IP packets (often large for user-plane data) containing information and such overhead is manageable. In some evolving M2M application scenarios (e.g. remote "smart" metering) packets are short and small in number and extremely low duty-cycle, which from a system throughput perspective represents a vanishing data rate. In such low spectral-efficiency applications (seen by the application not the aggregate spectral efficiency), the signaling overhead latency translates directly into energy-loss, due to the fact that the whole embedded system is the sensing device is powered-up during the synchronization/training procedure prior to sending/receiving a short packet. While for a particular M2M or sensing node this energy-loss can be negligible, the aggregate cost due to the unbounded number of nodes could prove to be significant from a network standpoint. This clearly calls for a more detailed definition of latency in the presence of M2M traffic with conventional user traffic, and coupled with the potential of a rapid increase in the number of machines connected to cellular infrastructure in the coming decades.

III. Low Latency Application Scenarios

In this section, we focus on two types of applications: real-time machine to machine communication and interactive gaming [7].

A. Realtime Machine-to-Machine Communication

Although a large variety of M2M application scenarios with heterogeneous requirements and features exists, they can be classified into two main M2M communication scenarios as defined in [5], communication of M2M devices with M2M servers/users and communication between the M2M devices.

At the present time, the most interesting applications from the commercial point of view are related to smart electricity, automatic water and gas meters reading. However, the M2M application space is vast and includes security, health monitoring, remote management and control, tracking and tracing, intelligent transport systems, distributed/mobile computing and gaming, industrial wireless automation, and ambient assisted living.

i. AutoPilot

This scenario includes both vehicle collision detection and avoidance (especially on highways) and how urgency actions are taken in case of an accident. It is based on a M2M device equipped with sensors embedded in cars and surrounding environment and used in automatic driving systems. These M2M devices (cars, road sign units, highway cameras) send information to a backend collision avoidance system used. The backend system distributes notifications to all vehicles in the vicinity of the location of the collision, together with information required for potential actuation of relevant controls in the affected cars. In all the receiving cars the automatic driving systems based on the received information take over the control fully or partially (brakes activated, driving direction changed, seating belts tightened, passengers alerted etc). If there is no such system in a car, the driver is notified and instructed. Also, depending on the proximity of the accident, cars receive different commands, i.e. the cars which are closer to the place of the possible collision are getting immediate commands for the actuators, while the cars which are further away from this place get driver notifications only.

ii. Virtual Race

One example of the many possible M2M games is the virtual race (e.g. virtual bicycle race using real bicycles). The opponents are on different locations, possibly many kilometers away. At the beginning, the corresponding length of a race is agreed (i.e. 10 km or 20 min) between the peers. The measurements are taken by sensors (GPS, temperature, humidity, speed, terrain configuration etc.) and are exchanged between the opponents. They are used by the application to calculate the equivalent positions of the participants and to show them the corresponding state of the race (e.g. "you are leading by 10 m"). The number of competitors may be more than two, and all competitors must mutually exchange information, and the applications must present all participants the state of other competitors. For a large number of competitors (hundreds or more), a corresponding application server must be used. During the race they are informed about the place and the distances from each other (e.g. "you are the 3rd behind the 2nd by 10 m and leading before the 4th by 15 m").

iii. Sensor-based Alarm or Event Detection

Many categories of applications exist or will be reasonably implemented in the future. In some applications, sensors infrequently deliver a small amount of data: e.g. high risk transportation, meteorological alerts, stability of buildings, critical parameters in plants, etc. Of course the type of power supply (if the sensor is always on or not), density and other parameters depend on the application. Another type of application is event detection requiring fast reaction. An example is the detection of pressure drop

through the pipelines (gas/oil); this critical information should be sent immediately to the control centre in order to prevent potential accidents. In the field of surveillance and security, discrete sensors which should stay undetected can enable interesting applications too. Examples of this type of applications can be intrusion detection sensors, or automated network of surveillance camera (with or without motion or pattern detection, mounted or not on robots, for instance), which send periodic reports to and interact with the control center, possibly in a completely automated way, until a critical event requiring the human intervention is detected. Depending on the type of applications, certain cases may require the deployment of proprietary networks, or they may be run on top of a standard LTE/LTE-A network or of a mesh network deployed for a specific need. Only the operational context may decide of the exact network architecture.

iv. Team Tracking

Team Tracking (TT) applications aim at monitoring the position of several nodes in a given environment for situation awareness and consequent action scheduling. One typical application of the TT scenario is the monitoring of firemen or policemen in a given area (e.g. building, stadium) during an operation. In this context, it is crucial to have an up-to-date picture of the situation, to allow reactivity and manage the team considering the positions and the associated risks. A constant monitoring is usually obtained thanks to a positioning system and the connectivity among the nodes and the control center. This kind of application is typically run on ad hoc mesh networks deployed for specific needs, hence the control center may physically collocated in one of the node of the network or it may be physically far away. In the latter case, one node of the network offers connectivity to an IP backbone in order to reach the control center.

B. Gaming

At present time the evolution of processing power at the end terminal has lead to a point where even complex online games can be played anywhere even by highly mobile users, e.g., in public transport units. Even if this step can be considered as normal evolution, it is important to note that it introduces a new class of real-time applications into the world of mobile cellular wireless networks.

The core aspect of any gaming scenario is the fast inter-active nature of the application: users interact with other users. The nature of this interaction can be of different kind, like cooperative or challenging. The gaming applications span a wide range from racing simulations, over real-time strategy to first person-shooters. In general the classic applications challenge the reaction time of the users and therefore rely on low-delay access technologies. The logical network architecture is not necessarily limited to any specific setup like fully meshed nodes or server-client setups.

In contrast to most other applications, gaming traffic patterns strongly correlate with user interaction at the terminal side. A traffic stream from such a source is a function of participating users, their properties and so on. This is more than some data packets exchanged between two nodes.

i. Online Gaming

Online gaming is an application that evolved from multiplayer games. In multiplayer games two or more players enter the same game either in competition or in cooperation mode. The early realizations were realized at the same machine; later the players took part on separate computers connected via a network. In general the communication between the nodes in the game can be established over different networks and in different manners. In [6] the authors show that the games most sensitive to delay are the First Person Shooters (FPS) and sport games, e.g., car racing.

The "Online Gaming" setup is a classical multiplayer game in which two or more persons compete for a given time. Each game has a defined start and end. At the end all the scores are calculated and presented to all the participants. A high delay will impact the gaming experience of the user on one hand and the resulting score on the other hand [6]. These applications will typically take place in cellular mobile networks.

New on-line games will move latency requirements dramatically down. Low latency is especially critical for an avatar model of Online Games with high precision weapons (massively multi-user on-line first-person shooter).

ii. Gaming on Sport Events

At present online gaming application take purely place in fictional and created worlds. However with increasing number of high performance handsets one could think of online games as a part of the real world. This is targeted by this scenario we call "Gaming on Sport Events" in this paper. Now imagine instead of competing on a virtual score the participants are in the audience of a big and exciting sport event. The goal of the game is the prediction of the next major event, like:

- Tennis: who will win the next point, will the next serve be an ace?
- Basketball: will next free-throw attempt be successful?
- Soccer: will the goal be scored from a free-kick?

It is very clear that low latency is critical due to real time context. In such scenario a high number of users in the same location (few radio cells) are expected.

Furthermore, the same game can be played by TV audience. Then, the number of players can be much higher. In that case the application server has to process many more users. In any case, the traffic load can lead to increased delays. Such a setup can run either on top of LTE or LTE/A networks or as a self organizing meshed network in case of limiting the participants to the audience only.

IV. TRAFFIC ANALYSIS

In this section, we analyze the traffic characteristics for machine-to-machine communication as well as for gaming application [7].

A. *Machine-to-Machine Communication*

Today, mobile networks are dimensioned using standard mobile wireless network traffic models, which are based on a typical subscriber behaviour expressed in typical time spent using speech service, number of sent/received messages (SMS, MMS) and the amount of data subscriber is downloading. These traffic models do not take into account traffic generated by M2M devices, hence a new traffic model is required.

When modeling M2M traffic, two different patterns are expected. Most of the sensors will be in sleep mode, sending small amounts of traffic from time to time in order to notify the rest of the network that they are still alive. Some other M2M devices will generate traffic in bursts, so this type of traffic can be modeled with ON/OFF traffic model. Important parameters of traffic model that have to be considered are:

– potential number of devices and applications, density of devices
– periods of activity/sleep
– amount of useful data that is sent/received, for different type of applications
– overhead due to different types of signaling
– frequency and size of packets

The main expected differences in M2M traffic characteristics, comparing regular mobile network traffic patterns, are:

– M2M traffic will significantly increase number of parallel ongoing connections (“50 billion connected devices” by 2010 expected by Ericsson)
– M2M traffic will be more uplink consuming then downlink consuming, as it is expected that M2M devices in general have more information to send than to receive (confirmed in traffic model described in [3])

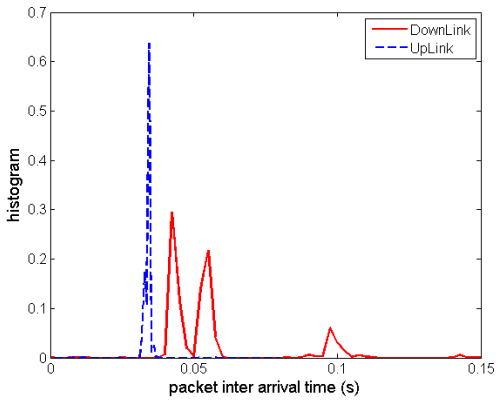
From a traffic analysis point of view it is interesting to note that some M2M device communicate using the TCP protocol. Therefore measurements will include some kind of interaction between the transport protocol and the actual access network under test. Any derived model has therefore be tested and analyzed for a possible presence of such an interdependency.

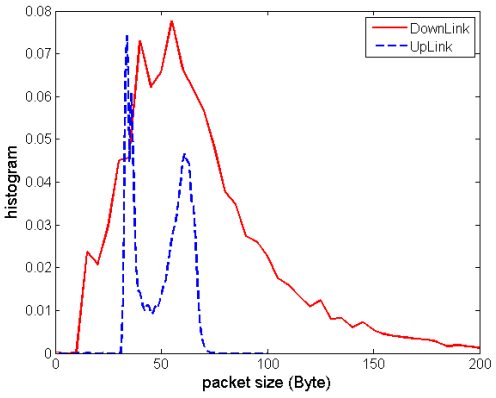
B. *Gaming*

The online gaming applications that are most prone to end to end delays are FPS and racing games [6]. Therefore we selected well-known representative for these types of online games, namely: Team Fortress 2, DiRT2. In addition to this we selected also the FPS game open arena.

When analyzing online gaming traffic patterns, we expect the use of use the User Datagram Protocol (UDP) as transport protocol on top of IP. This protocol features no advanced flow control like e.g. the Transport Control Protocol (TCP) and therefore we can directly analyze the payload values of UDP which are the packet size and inter arrival time.

In a standard client/server setup the traffic patterns for different online games are similar. This comes from the fact that data exchanged between server and client follows a given pattern. The downlink direction carries all the information about other players participating in the game. It is broadcasted by the server in a regular pattern to update the different users about the current status of the game. The traffic in downlink direction is a function of the number of real players participating in the game. A higher number of participants leads to more information that has to be transferred from the server to the clients. The packet size in downlink direction is therefore relative variable. In the uplink direction the client reports the actions of the local user to the server. As the single user can only execute a very limited number of actions in a timeslot, the uplink traffic consists of packets with a small spread in payload size, e.g., ranging from 40 to 70 Byte. The following two figures depict the packet size and the packet inter-arrival time for the open source game OpenArena. The game is based on the Quake 3 engine. The results follow the values expected for a FPS game as in [6].





The modeling of online gaming traffic can be done straight forward using packet size and inter arrival time as the underlying protocol is UDP. Therefore there is no interaction at the protocol layer. However, there is a correlation between the two values.

V. Delay and Traffic Measurement for Online Gaming

Delay measurements of Online Gaming were conducted in the existing network of Mobile Telekom Serbia (MTS) in order to get reference and idea of delay and traffic patterns in real network. The measurement campaigns recorded the different delay patterns found in the access networks. As shown in the figure below, the technologies tested in this measurement are:

– ADSL Asymmetric Digital Subscriber Line,
– FTTB Fiber To The Building,
– WLAN Wireless Local Area Network,
– UMTS / 3G Universal Mobile Telecommunications System.

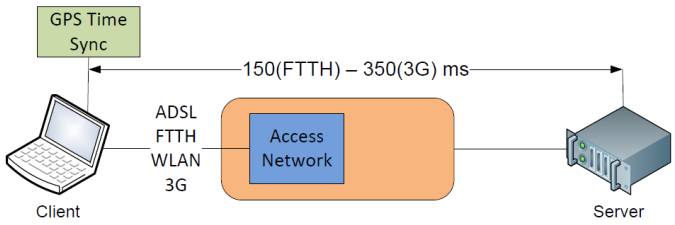


Figure 1: Measurement Setup for ADSL, FTTB, WLAN and 3G

The values obtained for the different technologies show a delay ranging from 150 ms for the fast access types like FTTB to 350 ms for 3G. The ping command via ICMP is used to measure the E2E delay. The server under test is the game server for the applications HalfLife and Colin Mc Rea Rally (two type of Online Gaming). The packet size is around 80 Byte and nearly constant, while the inter packet time has a peak around 45 ms between consecutive packets and a subsequent peak at 60ms. In contrast to this the uplink packet size histogram has three discrete spikes at 60, 75 and 90 Byte, with an update rate of 30 ms.

VI. Latency Improvement in Access Layer

In this section, we present some possible access layer adaptation to lower the latency of the system for the considered applications. They include adaptive modulation and coding (AMC), scheduling, and hybrid analog/digital transmission [7].

A. *AMC design*

The current implementation of LTE has achieved a good flexibility and low latency in the management of HARQ and AMC when dealing with standard applications like VoIP or multimedia communications in a context of an unloaded network. However, the raise of M2M applications will probably highlight once again the old issue of resource management in presence of a high density of users (humans and, now, machines) possibly in conditions of high loaded. Moreover, the development of M2M application will probably set new challenges to HARQ and AMC, linked to the sparcity of the traffic, the presence of relay or multiple hops among devices, etc.

i. Policies for Sparse Traffic

Sparse traffic in some M2M applications raise challenges not only on the access and scheduling, but also on the choice of the best way to carry out information. Can spatial correlation be taken into account? What is the impact of having limited or null channel information? The influence of long sleep times may in fact be important in the choice of the right AMC and HARQ.

Certain applications (for example alarms) may need to send a limited number of information bits but with a very high reliability and in a strictly limited number of transmissions, due to strong latency constraints or battery life optimization. In such cases, the most correct metric for measuring the delay introduced by HARQ could be the maximum peak delay values and not the average ones.

ii. Policies for multihop network

The presence of multiple hops inside a cell of a future LTE-A network (or evolution) or on a rapidly deployable mesh network may have a strong impact on the definition of the most correct AMC and HARQ algorithms and procedures. For example, cooperative techniques may be considered: the expected gain is the increased robustness of the communication.

However, signalling and exact HARQ strategies need to be designed with the aim of minimizing latency. The impact on improved reliability on the throughput must also be controlled, and can make

sense for certain M2M applications needing low user bit rates.

Finally, issues related to the time-frequency synchronization of the nodes and channel estimation must be considered when using cooperative techniques.

iii. Efficient Feedback Signaling

Efficient feedback signalling for every king of PHY layer procedure (measurements procedures, ACK/NACK feedbacks, ranging and bandwidth request) will have a beneficial impact on the latency of the network. An improved design of this kind of messages can help in achieving the goal of the PHY layer procedures in harsh conditions (many devices wanting to access, limited number of opportunity in time and frequency due to battery constraint or to load, etc.). As a first example, in certain applications, sending with the ACK/NACK feedback also the amount of additional mutual information needed by the receiver can help the transmitter to limit the number of retransmissions.

B. Scheduling

The study of MAC-layer scheduling policies and more generally channel-access is clearly of interest for M2M and certain gaming applications. In both application areas scheduling should be studied both from the point-of-view of the downlink and uplink. In the downlink the major issue is accommodating low-throughput and, more often than not, sporadic latency constrained traffic at the same time as conventional traffic.

On the uplink, the primary concern is channel access for sporadic traffic with minimal uplink signaling overhead. The latter is for energy concerns, in the sense that a low-throughput service should not require a significant energy overhead in order to maintain low-latency. In the extreme case, which could arise in remote sensing applications, one could clearly imagine the need for sending short packets with extremely low duty-cycle. Here a low-latency channel access protocol will keep energy consumption of the terminal device to a minimum, which in dense sensor networks is clearly a concern.

The trend in LTE which is culminating in the Release-10 standardization process is to reduce latency in the uplink channel access protocol. In the access stratum, this can occur with two-levels of granularity, basically depending on the activation state of the terminal. In the idle state (RRC_IDLE), the terminal must re-authenticate itself using the random-access procedure (to obtain a C-RNTI) which incurs a minimum-latency on the order of 16ms before being granted a transmission opportunity to upload a single packet. This value is significantly higher if the PRACH is configured with a high periodicity. This latency is difficult to circumvent and furthermore, the terminal must activate its transmission and reception circuitry during the access period, which is clearly not energy-efficient. It is clearly also a very inefficient access protocol for networks with a large number of low-throughput sporadic access nodes (e.g. sensor networks).

In the connected state (RRC_CONNECTED) the UE provides a scheduling request (SR) on the uplink control channel (PUCCH) resource in order to transmit a packet. Both in Release-8 and Release-10, the latency incurred by the channel access amounts to 6ms after the transmission of a SR. This is due to the reaction time of the eNB scheduler and the UL grant procedure via the downlink control channel (PDCCH). Aside from this constant latency, the remainder depends on the periodicity of the SR. In Release-8 LTE this can be at least 5 ms, but also much more and in Release-10 it is planned to reduce this to the strict minimum, namely 1ms. For SR periods larger than 5 ms, the random-access procedure is more efficient for sporadic packet arrivals than through the SR and thus may prove to be a more suitable access technique for some M2M and gaming traffic flows when it comes to the UL. Moreover, a very low period SR is not suitable for very sporadic traffic sources, especially in dense M2M networks, since the signaling overhead quickly becomes comparable to the data throughput, which is clearly unacceptable.

As a result of the limitations in both of these UE states, it is worthwhile to consider new channel access techniques to accommodate sporadic traffic sources in LTE, especially if many such new devices start to use the networks. One avenue to address this would be to introduce new contention-based random-access.

C. Hybrid Analog/Digital Transmission

In LTE/LTE-A network systems and many rapidly-deployable mesh network systems, energy-efficient and delay-limited transmission of analog samples with minimal distortion at the receiving is needed. For such systems, hybrid analog-digital (HAD) is a promising transmission technique. Several papers (see [1] and [2]) have shown that HAD transmission can greatly reduce the decoding latency of the system. In addition, HAD systems have some of the advantages of digital system and some of the advantages of analog system. They can theoretically achieve the Shannon rate-distortion-capacity limit at the designed signal-to-noise ratio. Although HAD is a promising technique for reducing the latency in LTE/LTE-A networks and mesh networks, the use of HAD technique is still face challenges. Because of the fundamental nature of this research, at this early stage it is still not clear how much benefit these techniques will bring with respect

to latency in the context of an LTE-like system or rapidly-deployable mesh network systems. Moreover, the application examples of HAD transmission technique in communication systems are very rare. Therefore, many challenging problem have to be solved before this technique can be applied in real communication systems.

In terms of hybrid D/A transmission for LTE/LTE-A network, it is important to demonstrate that a latency-constrained digital feedback protocol for transmission of analog samples can achieve comparable distortion performance to classical feedback-based control approaches without latency constraints. Suggestions for accommodating this type of transmission in and LTE framework will be provided. The more general multi-sensor case will be also considered.

Regarding HAD transmission technology for topology B, we first focus on link level optimization. This includes performance optimization of single-link HAD techniques for different channel models and various source distributions. System level optimization will also be considered. We will also design and optimize the HAD transmission technology for the defined mesh network scenarios. Practical HAD transmission schemes that can reduce latency in topology B will be proposed.

VII. CONCLUSION

Latency is becoming a key issue for network operators seeking solutions to support low latency applications, and in particular real-time machine-to-machine communication and interactive multiplayer game. Latency is identified as a major factor influencing the behavior and footprint of the application. Currently, LTE can provide on the order of 10ms latency for the E-UTRAN in the ACTIVE state. The core network adds a significant amount of delay depending on the region and the proximity of the server with respect to the access network serving the device. The upcoming emerging application scenarios will definitively require very low access layer latency. A significant latency improvement is possible through advanced access layer techniques as well as careful selection of various parameters and technologies.

ACKNOWLEDGMENT

This paper describes work undertaken in the context of the LOLA project – Achieving LOw-LAtency in Wireless Communications (www.ict-lola.eu). The research leading to these results has received funding from the European Community's Seventh Framework Programme under grant agreement n° 248993.

REFERENCES

[1] Skoglund, M., Phamdo, N. and Alajaji, F., "Hybrid Digital-Analog Source-Channel Coding for Bandwidth Compression/Expansion". IEEE Transactions on Information Theory, Vol. 52, No. 8, pp. 3757-3763, August 2006.

[2] Mittal, U. and Phamdo, N., "Hybrid digital-analog (HDA) joint source-channel codes for broadcasting and robust communications". IEEE Transactions on Information Theory, Vol. 48, No. 5, pp. 1082-1102, May 2002.

[3] I.Tomic, S.Krco, D.Vuckovic, A.Gluhak, P.Navaratnam, "SENSEI traffic impact on mobile wireless networks", Towards the Future Internet, pp. 257-266, IOS Press, 2010.

[4] 3GPP TR 25.912 V.9.0.0, "Feasibility study for evolved universal terrestrial radio access (UTRA) and universal terrestrial radio access network (UTRAN)", Rel. 9, Dec 2009.

[5] 3GPP TS 22.368 V10.0.0, "Service requirements for machine-type-communication (MTC)", March 2010. Available: http://www.3gpp.org/ftp/Specs/archive/22_series/22.368

[6] M. Claypool, K. Claypool, "Latency and Player Actions in Online Game", Communication of the ACM, 2006.

[7] LOLA consortium, "Deliverable D2.1, D3.2, and D4.1", FP7 EU LOLA Project, March 2010. Available: http://www.ict-lola.eu/deliverables

RFID tehnologija v IoT projektih

Andrej Planina, Špica International

Povzetek — RFID (radio frekvenčna identifikacija) je že zrela tehnologija, vendar v zadnjem času zaradi projektov Interneta stvari (Internet of Things, IoT) dobiva nov zagon. Članek opisuje razlike v izvedbi RFID tehnologije, navaja možnosti uporabe RFID v IoT projektih ter opiše nekaj obstoječih primerov uporabe. Kot poseben primer RFID je opisano tudi lociranje s pomočjo RFID (Real Time Location System, RTLS).

Ključne besede — RFID, NFC, RTLS

Abstract — RFID (Radio Frequency Identification) is mature technology and is getting even bigger interest because of Internet of Things projects. The article describes main characteristics of RFID, and discusses possible use of RFID in IoT projects. Some real-life use-cases are described. RTLS (Real Time Location System) is described as a special case of RFID usage.

Keywords — RFID, NFC, RTLS

I. UVOD

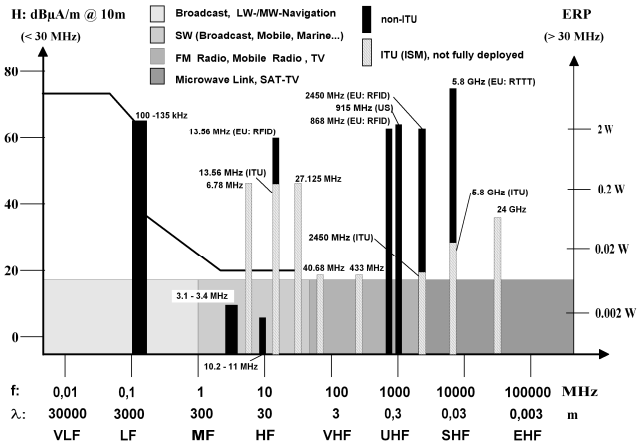
V okviru razmišljanj o internetu stvari (IoT) se tehnologija radio-frekvenčne identifikacije (RFID) pogosto omenja kot orodje s katerim računalniški sistem identificira fizične stvari. Pri uporabi RFID v IoT projektih je potrebno poznati lastnosti RFID, njene omejitve in posledice njene uvedbe. RFID tehnologija je sicer že zrela tehnologija, ki pa ravno zaradi IoT iniciativ doživlja nov zagon in mora izpolnjevati dodatne zahteve. Ravno zaradi zrelosti je njeno delovanje dovolj dobro poznano, standardi pa so se že uveljavili.

Zaradi zrelosti in široke osnovne uporabe RFID je na voljo že kar nekaj bolj naprednih rešitev, ki za svojo osnovo uporabljajo RFID, kot je na primer Real Time Location System (RTLS).

II. RFID FREKVENCE

Z napredovanjem tehnologije in aplikacijskih zahtev se spreminjajo tudi frekvence, na katerih delujejo RFID sistemi. Trenutno so v uporabi naslednji frekvenčni pasovi:

– pod 135 kHz (Low Frequency), domet do 1 m, tipično okrog 10 cm, kontrola pristopa, robustni sistemi, osnovna identifikacija
– 13,56 MHz (High Frequency), domet do 1 m (sa pasivnimi tagi), večja hitrost čitanja, kontrola pristopa, več možnosti za enkripcijo
– 860-930 MHz (Ultra High Frequency), doseg do nekaj metrov, občutljivost na materiale v okolici, uporablja jo EPC Gen2 standard, veliko proizvajalcev opreme, hkratno čitanje več RFID tagov
– 2,4 GHz (WIFI), novost za RFID, ni standarda, ni interoperabilnosti, nove aplikacije (RTLS …)



Slika 1: Uporaba frekvenc [1]

Frekvenco RFID sistema je potrebno izbrati na podlagi aplikativnih zahtev. Če se zahteva pozitivna identifikacija človeka za namen močne kontrole, je najbolj primeren HF. Za uporabo v logističnih sistemih, kjer se zahteva interoperabilnost in standardizacija, je najbolj primeren UHF in uporaba EPC Gen2 standarda. Tudi cena posameznega RFID taga je zaradi masovne proizvodnje najnižja v UHF področju. Ravno zaradi velike razširjenosti, nizke cene in velike dometa čitanja predvidevam, da se bo v IoT projektih najbolj pogosto uporabljalo ravno UHF RFID tehnologijo. Pri UHF EPC Gen2 je potrebno opozoriti še na razlike v dovoljenih frekvencah branja med ZDA in EU. Večina čitalcev lahko deluje tako na ZDA kot tudi na EU frekvenčnih področjih, le pravilno jih je potrebno nastaviti. UHF EPC Gen2 tagi pa že omogočajo branje tako na EU kot na ZDA frekvencah.

III. RFID STANDARDI

Poleg same frekvence delovanja je pomemben tudi zapis na RFID tagu. Na tem področju obstaja nekaj standardov (EPC Gen2, ISO 14443, ISO 15693, NFC ISO18000-3), ki zagotavljajo interoperabilnost.

V IoT projektih so pomembni tudi komunikacijski standardi, ki definirajo način prenosa podatkov s senzorjev oz. čitalcev do centralnega nadzornega sistema. Najbolj pogosto se uporabljata ali omenjata 6LoWPAN in ZigBee.

Za opremljanje večjega števila varnostno neproblematičnih objektov, še posebej v logističnih aplikacijah, se zaradi nizke cene in razširjenosti po celem svetu najbolj pogosto uporablja EPC Gen2 standard. Za varnostno bolj kritične aplikacije (osebe, vozovnice, denar) se najbolj pogosto uporablja ISO 14443, ki že vključuje enkripcijo prenosa podatkov med čitalcem in tagom. Vseeno velja omeniti, da obstajajo različni nivoji zaščite. ISO 14443 standard predpisuje le osnovno, priporočljiva pa je vsaj 128-bit AES ali 3DES.

IV. UPORABA RFID V IOT PROJEKTIH

V projektih interneta stvari (IoT) se predvideva povezovanje mnogih objektov. Objekti naj bi nosili nek elektronsko aktiven element, ki naj bi imel svojo identifikacijo in naj bi bil sposoben komunicirati z ostalimi objekti. Če želimo opremiti ogromno količino objektov, je cena take aktivne naprave zelo pomembna. Gotovo ne bo potrebno prav vseh »stvari« opremiti s polno funkcionalnostjo, pogosto bo dovolj že samo identifikacijska funkcija. Tip objektov, ki se bodo pojavljali v IoT lahko za naš namen razdelimo v dva tipa:

- smart objects – imajo lastno komunikacijsko sposobnost in možnost delnega lokalnega procesiranja lokalnih podatkov
- non-smart objects – imajo samo možnost javljanja svoje identifikacijske številke, čitalec oz. senzor pa doda druge relevantne podatke

Tako si ne predstavljam, da bi bil vsak stol ali omara povezana v internet stvari, bodo pa take enostavne stvari opremljene z identifikatorjem (RFID tag), ki ga bo zaznal senzor (RFID čitalec) v bližini. Senzor bo dogodek opremil še z drugimi podatki (čas, lokacija, okoliščine) in ga šele tako opremljenega poslal v omrežje.

V. RTLS

Real Time Location System (RTLS) je tehnologija, ki navadno s pomočjo fiksne RTLS mreže in identifikacije premičnih RTLS tagov lahko določi položaj RTLS taga v 3D prostoru. Obstaja več vrst RTLS, ki se med sabo razlikujejo po uporabljeni tehnologiji in posledično po natančnosti, ki sega lahko od nekaj centimetrov do nekaj metrov. Bolj natančni RTLS uporabljajo UWB pulze in triangulacijo na podlagi razlik v časih prejetih pulzov, manj natančni pa uporabljajo inovativne in cenejše metode razbitja večje površine na manjše področja, ki jih nadzirajo posamezne RFID antene. Vsi radijski RTLS sistemi uporabljajo aktivne RFID tage, trajanje baterije pa je v glavnem odvisno le od pogostosti zajema lokacije, ki je lahko na vsakih nekaj sekund do vsakih nekaj ur.

Če obravnavamo samo radijske RTLS sisteme in pozabimo na IR in druge RTLS sisteme, lahko RF RTLS sisteme razdelimo na več skupin:

a) UWB RTLS – delujejo s pomočjo dodatnih UWB pulzov, aktivni tagi, postaviti je potrebno dodatne RTLS antene, vsaj po 4 antene na en prostor, domet do 100 metrov, natančnost nekaj 10 cm, stene zelo poslabšajo natančnost, relativno drag sistem, potrebno je zelo natančno umerjanje sistema, pozicijo lahko določijo v treh dimenzijah, glavni proizvajalci: Ubisense.

b) WIFI RTLS – delujejo na obstoječih WIFI omrežjih in položaj izračunavajo s triangulacijo in s pomočjo merjenja velikosti prejetega signala na tagu, natančnost nekaj metrov oziroma »na prostor natančno«, programska oprema za triangulacijo je draga in nestandardna, delujejo na vseh standardnih WIFI mrežah, sledijo lahko vsakemu WIFI odjemalcu z MAC naslovom, uporabljajo tudi posebne aktivne WIFI RTLS tage, pozicijo lahko določijo samo v dveh dimenzijah. Glavna proizvajalca: Aeroscout, Ekahau.

c) inovativni RTLS sistemi – delujejo na 2,4 GHz področju, za lociranje uporabljajo posebne RF oddajnike »lokatorje«, za prenos podatkov o lokaciji s taga uporabljajo ločeno radijsko omrežje, natančnost odvisna od gostote lokatorjev, tipično nekaj metrov oz. »na prostor natančno«, pozicijo lahko določijo samo v dveh dimenzijah. Potrebno je natančno umerjanje sistema. Azijski proizvajalci.

VI. POSLEDICE UVEDBE RFID

Poplava podatkov (Data Flood) – ker je dogodkov na RFID čitalcih lahko izjemno veliko, nastane problem relevantnosti zajetih podatkov. Sicer znajo boljši čitalci že sami pri sebi izvesti prva filtriranja podatkov (odstranjevanje redundantnih in podvojenih čitanj), ki pa jih je potrebno pravilno nastaviti. Avtorji predlagajo več metod za upravljanje z RFID podatki, na prvem mestu je navadno primarna obdelava podatkov čim bližje zajemu [2].

Senzorsko omrežje – za izvajanje primarne obdelave podatkov in za komunikacijski vmesnik od RFID anten do nadzornega sistema je potrebno uvesti senzorske krmilnike (Sensor node). Ti morajo biti čim manjši, porabiti čim manj energije in biti sposobni izvajati primarno procesiranje zbranih podatkov. Zelo zaželeno je, da znajo komunicirati na čim več načinov. Pogosto se od njih zahteva, da lahko poleg zajema podatkov krmilijo še aktuatorje in tako delujejo kot

neke vrste periferni živčni sistem, ki je sposoben hitrih odzivov na vnaprej določene dogodke.

Komunikacijsko omrežje – zaradi velike količine predvidenih senzorjev v IoT omrežjih je nujna uporaba IPv6 protokola. Za zadnjih nekaj metrov komunikacije do senzorskega omrežja se uveljavlja brezžični protokol 6LoWPAN. V praksi se pogosto pojavlja tudi ZigBee (wireless mesh) protokol, ki pa v osnovi ni namenjen za kompleksne aplikacije. Oba uporabljata isto osnovo 802.15.4.

Shranjevanje in obdelava podatkov – zaradi obilice zbranih podatkov se lahko v slabo načrtovanih sistemih pojavi preobilica podatkov, ki jih je potrebno hraniti in obdelovati. Za zmanjšanje vpliva količine podatkov na sisteme za hranjenje in obdelavo podatkov, je potrebno načrtati tak sistem, ki bo nerelevantne podatke brisal ali zanemaril pri obdelavi. Avtorji predlagajo več metod za rešitev tega problema [2].

Vpliv na človeka – Eden od vplivov uvedbe RFID sistemov je tudi vpliv dodatnega RF sevanja na človeško telo. Eksperimentalna študija je pokazala, da dva HF čitalca vsak z oddajno močjo 1 W na razdalji 10 cm od glave človeka že povzročita SAR 2 W/kg, kar presega FCC dovoljeno SAR 1,6 W/kg [3]. Zelo podobni so bili rezultati na UHF področju [4]. To dejstvo je potrebno vzeti v obzir pri načrtovanju RFID sistemov in se izogibati dalj trajajoči in bližnji izpostavitvi ljudi sevalnemu polju RFID čitalcev.

VII. OPIS NEKAJ RFID PROJEKTOV [5]

Pošta Slovenije – sledenje premikov transportnih vozičkov. V projektu sledimo premike kovinskih transportnih vozičkov skozi dve vrati za nalaganje na vozila. Uporabljena je UHF EPC Gen2 tehnologija, domet čitanja je cca. 2 m, v projektu je kombinirana uporaba RFID in črtne kode. Problem uporabe RFID na kovinski podlagi smo rešili s posebnimi pasivnimi RFID tagi. Problem »nebranja« RFID tagov smo rešili z dodatno potrditvijo uporabnika po nalaganju vozičkov na vozilo.

Marina Veruda – sledenje prehodov plovil. Projektna naloga je zahtevala natančno evidentiranje prehodov plovil skozi 150 m širok vhodno/izhodni kanal v marino. Uporabili smo 2,4 GHz RFID tehnologijo in aktivne RFID tage, s katerimi smo dosegli 100 % čitanje tudi ob hitrejših prehodih plovil. RFID tag na plovilu je lahko nameščen celo znotraj kabine. Kasneje se načrtuje nadgraditev sistema še z določanjem točnejše lokacije plovila in s tem povezano večjo varnostjo plovil.

Gradbišče Arene Zagreb – evidentiranje prisotnosti delavcev. Na velikem gradbišču je bilo lahko tudi več 100 delavcev hkrati. Zaradi zakonskih in varnostnih predpisov mora imeti vodja gradbišča vedno natančno evidenco prisotnih delavcev in hkrati preprečevati vstop nepooblaščenim osebam. Vsem delavcem smo v notranjost čelad namestili samolepljivi pasivni UHF EPC Gen2 RFID tag, na vhodih pa so bile nameščene fizične bariere, ki so se odprle le po branju RFID taga. Prehodi delavcev skozi bariere so bili izjemno enostavni in hitri, evidenca delavcev je bila 100%. Po zaprtju gradbišča je naročnik sistem premestil na drugo gradbišče.

Ministrstvo za obrambo RS – odkrivanje nedovoljenih dogodkov v srednje varovanih conah s pomočjo RTLS. Raziskovalni projekt, sponzoriral ga je MORS, vodila TIA, kjer smo skupaj z IJS in FE UL izdelali sistem, kjer smo s kombinacijo kamer, UWB RTLS in učečega se inteligentnega nadzornega sistema ugotavljali nedovoljene dogodke v prostoru. Pooblaščene osebe in posebej varovani predmeti so bili opremljeni z aktivnim RTLS tagom, kamere so zaznavale vse premike v prostoru. Če je kamera zaznala premik, ki ga v RTLS sistemu ni bilo videti, je sistem sklepal na nedovoljeno situacijo in je sprožil alarm. Sistem je možno nastaviti tudi z vnaprej določenimi pravili. Nagrada za inovatorje leta na Slovenskem forumu inovacij 2009.

LITERATURA IN VIRI

[1] http://www.rfid-handbook.de, april 2011.
[2] Seven principles of effective RFID data management, M. Palmer - Progress Software, 2004.
[3] Impacts of RF Radiation on the Human Body in a Passive RFID Environment, Darmindra D. Arumugam, 2008.
[4] Specific Absorption Rates in the Human Head and Shoulder for Passive UHF RFID Systems at 915 MHz, Darmindra D. Arumuga, 2008.
[5] Interne projektne dokumentacije Špice International

Andrej Planina, univ. dipl. ing. el., je v Špici zaposlen že več kot 15 let in velja za strokovnjaka s področja poslovnih mobilnih rešitev in s področja tehnologij avtomatske identifikacije. Svoje obsežno znanje pridobiva kot vodja projektov z večjimi organizacijami v regiji. Dobro pozna tudi poslovne vidike informatizacije procesov. Avtor nekaj uspešnih Špicinih produktov in projektov.

Vpliv telemedicine na življenje ljudi in na razvoj Slovenije kot EU regije – projekt eBIOMED

Uroš Stanič, Kosezi d. o. o, Jana Stanič, Zavod Biomedicinska raziskovalna skupina – BRIS

Povzetek — Od leta 2004 smo v Sloveniji stalno izpopolnjevali načrt nacionalnega telemedicinskega in teleoskrbnega omrežja. Trenutni neformalni konzorcij Telemedicine, ki je nastal ob pripravi na razpis MVZT za kompetečne centre konec leta 2010, sestavljajo vodilni medicinski, raziskovalni, tehnološki in poslovni strokovnjaki.

Definirane so medicinske potrebe in pripravljene so funkcionalne in tehnološke rešitve, s katerimi bi bilo možno do leta 2020 postopno priključiti vseh 750.000 slovenskih gospodinjstev na telemedicinsko in teleoskrbnoomrežje preko širokopasovne komunikacijske infrastrukture. V tem primeru bi bila Slovenija med prvimi EU regijami, ki bi realizirala strategije EU na področju e-Zdravja, katerega pomembni del je telemedicina in teleoskrba. Le-ta bo dvignila kvaliteto zdravstvene nege obolelih ter starejših državljanov.

Glede na rezultate že opravljenih študij v svetu ter na podatke iz strokovne literature ocenjujemo, da bi z uvedbo telemedicine in teleoskrbe zmanjšali skupne letne stroške državnega proračuna za zdravstvo in socialno skrbstvo (cca. 25 % proračuna) za 10 % kar pomeni 2,5 % letnega državnega proračuna. Ob tem bodo bistveno manjši tudi izpusti CO_2 zaradi zmanjšanega števila voženj bolnikov do zdravstvenih institucij in zmanjšanih ostalih transportnih stroškov. Telemedicinsko omrežje se bo dopolnjevalo z obstoječim internetnim omrežjem in bo zato pripomoglo k večjim možnostim dela od doma, izobraževanju na daljavo in bolj učinkoviti e-upravi. Funkcionalno tehnološka rešitev telemedicinskega omrežja za 2 milijona naših državljanov, bi lahko postal odličen prodajni produkt Slovenije.

V tej luči dobi internetna in biomedicinska tehnologija, ki jo obravnava konferenca VITEL, strateški pomen za razvoj Slovenije, je osnova na kateri bomo razvili vrsto telemedicinskih in teleoskrbnih storitev, ki jih moramo realizirati po zahtevah vodilnih zdravnikov in socialnih delavcev. Ključna pri celotni zgodbi je pravočasnost in hitrost izvedbe. Ali bomo med prvimi na trgu, da poberemo smetano?

Ključne besede — Telemedicina, teleoskrba, razvoj Slovenije, zaposlovanje, široko pasovno omrežje do vsakega državljana

Abstract — Since 2004 we have constantly improved the plan for the national telemedicine and telecare network. The current informal Telemedicine consortium was formed for the application to the MHEST competence centers call in 2010 and is composed by leading medical, research, technological and business experts.

Medical needs were defined and technological and functional solutions were prepared, which will be ready, if the government so requires, to link up all 750.000 homes in Slovenia to the Telemedicine and Telecare network, which will be done over the internet (regular or broadband). In this case Slovenia would be the first EU region (country), which would realise EU strategy for e-Health, which envisages access to these solutions for all homes and for every citizen.

Based on the data available in literature we estimate, that this would lower the joint state budget for health and social care (25 %) for 10 % which represents as much as 2,5 % of the yearly state budget. The CO_2 emissions will be significantly lower as well, due to the fact that patients will not have to drive to health care institutions. In parallel these products made for the home will offer the possibility to work and learn from a distance as well as act as an infotainment portal. The solution for a telemedicine network for two million peoples (our citizens) would be an excellent market product of Slovenia.

When viewed in this light, the internet and biomedical technology which is the focus of the VITEL conference gains a strategic importance for the growth of Slovenia. It is the basis on which we will develop a series of telemedicine and telecare products, which should be realised based on the demands of the leading doctors and social workers.The key to this is speedy realisation. Will we be the first and get all the advantages?

Keywords — Telemedicine, telecare, growth of Slovenia, employment, broadband to each citizen

I. Uvod

Geneza telemedicinskega projekta eBIOMED temelji na pokrivanju funkcionalno tehnoloških zahtev izbranih medicinskih problemov štirih klinik Kliničnega centra v Ljubljani in funkcionalno tehničnih zahtev biomedicinskih raziskav, ki se izvajajo v Centru za biomedicinske planetarne raziskave v Planici. Tem ciljem je podrejena organizacija projekta eBIOMED, ki predstavlja prvo fazo udejanjenja nacionalnega telemedicinskega omrežja. Že ta faza bo omogočila konzultacije v celotnem omrežju zdravstvenih ustanov v Sloveniji, in sicer med klinikami, regionalnimi bolnicami, znanstvenimi ustanovami in domovi za starejše.

Slika 1: Geografska pokrititost slovenije z zdravstvenimi ustanovami

Tehnološki temelj projekta (IKT podprojekt in senzorski podprojekt) istočasno pokriva potrebe medicinskih problemov in problemov življenja v vesolju. Ker se slednje raziskave v raziskovalnem centru v Planici izvajajo že od leta 2007 lahko do sedaj razvite tehnološke rešitve smiselno uporabimo tudi pri uresničitvi telemedicinski rešitev za citirane medicinske probleme. V tem svojstvu predvidevamo za izvedbo celotnega projekta, da bo raziskovalna infrastruktura v Planici služila tudi kot živi laboratorij.

Slika 2: Center za planetarne biomedicinske raziskave – živi laboratorij (Living Lab) Planica

Pričujoči projekt bo imel velik učinek na spremembo zdravstvene in socialne oskrbe, identificiral bo glavne probleme življena v vesolju in potrebno tehnologijo za TM podporo. Istočasno pa bo bistveno prispeval k ustvarjanju velikega števila novih delovnih mest, novih proizvodov in storitev, zmanjšanju obremenitve okolja in pospešil ekonomski razvoj Slovenije.

II. IZBRANE TELEMEDICINSKE APLIKACIJE KLINIK UKC LJUBLJANA

A. "Zgodnje pobolnišnično spremljanje kirurškega bolnika", Klinični oddelek za travmatologijo, UKCL

Kirurškega bolnika spremljamo po operaciji zaradi pravočasne detekcije zgodnjih pooperativnih komplikacij. Te se, pri različnih operacijah, pojavijo v obdobju cca. 14 dni po posegu. Do nedavna smo takega bolnika spremljali v bolnišnici. Tendenca današnje zdravstvene politike je čim bolj skrajšati čas hospitalizacije. To je možno samo, če poskrbimo za detekcijo zgodnjih pooperativnih komplikacij na domu, ali v drugi nekirurški ustanovi. Danes zdravstveni sistem na to ni pripravljen. Zaradi neprilagojene patronažne službe in nezmožnosti rednega spremljanja takega bolnika na domu s strani zdravnika, je prišlo do povečanega pritiska na specialistične ambulante in se povečuje število kontrolnih pregledov po posegih.

Oskrbo kirurškega bolnika po operativnem posegu bi lahko izvajali v pogojih teleoskrbe. To je mogoče z opazovanjem merljivih, specifičnih in dovolj občutljivih parametrov, s pomočjo katerih bi lahko na daljavo spremljali bolnikovo zdravstveno stanje in s pomočjo katerih bi lahko pravočasno zaznali pojav zgodnje pooperativne komplikacije. Ti parametri bi morali biti taki, da bi nam lahko omogočili odločitev, ali bi lahko pri odpravljanju bolnika vodili na domu, ter mu po potrebi omogočili pravočasno strokovno intervencijo na domu ali v bolnišnici.

B. "Telemedicinska diagnostika v ortopediji": Ortopedska klinika, UKCL

Na področju ortopedije kljub razvejani mreži specialistov po Sloveniji ostaja problem konzultacij s terciarno ustanovo. Gre predvsem za urgentne primere s področja spinalne kirurgije, otroške ortopedije, septičnih procesov v kosti in kirurgije kostnih tumorjev, ki zahtevajo takojšnje ali čimprejšnje ukrepanje. Velika težava je tudi dostopnost terciarnega ortopedskega konzultanta v regijskih bolnišnicah v času izven rednega delovnega časa.

Družinski zdravnik, urgentni zdravnik ali ortoped iz regijske bolnišnice se danes lahko konzultira z ortopedom iz terciarne ustanove po telefonu, nima pa možnosti slikovno predstaviti bolnikovega kliničnega stanja, gibljivosti, slikovnih preiskav, trendov laboratorijskih in drugih izvidov. Za strokovno bolnikovo obravnavo mora biti zdravniku terapevtu in konzultantu ob trenutni obravnavi dostopna vsa bolnikova zdravstvena dokumentacija. Zdravnik potrebuje poleg dokumentacije o trenutni bolezni tudi podatke o alergijah, predpisanih zdravilih ter medicinske podatke dotedanjih ambulantnih in

bolnišničnih obravnavah z vsemi diagnostičnimi in terapevtskimi podatki: laboratorijske vrednosti parametrov in njihovi trendi (primerjave), slike, diagnoze, odpustnice, predpisana zdravila. Telekonzultacije bodo vključevale videokonferenčni pristop, vpogled v elektronski zdravstveni zapis, elektronsko izmenjavo slikovnega materiala (arhivskega ali v realnem času, npr. ultrazvok) in analizo kakovostne telekonzultacijske obravnave.

C. "Telemedicinska diagnostika pri obravnavi infekcijskih bolezni": Klinika za infekcijske bolezni in vročinska stanja, UKCL

Infektologi, podobno kot tudi nekateri drugi specialisti, so le v nekaterih regijskih bolnišnicah, bolnik z zahtevnejšo okužbo pa je lahko sprejet v bolnišnico kjerkoli v Sloveniji. Lečeči zdravnik se danes konzultira po telefonu z infektologom, nima pa možnosti slikovno predstaviti npr. bolnikovih kožnih sprememb, ugotovitev (slikovnih) preiskav, trendov laboratorijskih in drugih izvidov.

Izvedba projekta eBIOMED bo omogočila konzultacije z infektologom na način, da bo le-ta imel vpogled v vso bolnikovo dokumentacijo in bo preko povezave z lečečim zdravnikom na drugi lokaciji bolj strokovno in lažje pomagal pri odločanju glede ustreznih ukrepov. Na ta način bo zagotovljena večja varnost bolnika, zmanjšalo se bo podvajanje preiskav, zmanjšale se bodo nepotrebne premestitve oziroma povečala možnost za pravočasno premestitev v ustrezno ustanovo.

Telekonzultacije bodo vključevale videokonferenčni pristop, vpogled v elektronski zdravstveni zapis, elektronsko izmenjavo slikovnega materiala in analizo kakovostne telekonzultacijske obravnave.

D. "Telemedicinska diagnostika v intenzivni interni medicini": Klinični oddelek za intenzivno interno medicino, UKCL

Trenutno so v bolnišnicah v uporabi različni sistemi za zajem videa in slike. Vsak proizvajalec diagnostične opreme (endoskop, ultrazvok, kamere v operacijskih dvoranah …) ima svoj sistem za zajem videa in slike. Ti sistemi se razlikujejo v standardu video zapisa, načinu shranjevanja, mediju za shranjevanje, arhiviranju, dostopu, pregledovalnikih … Tako različni sistemi lahko da ustrezajo znotraj oddelkov oz. znotraj ene zdravstvene ustanove, vendar ne ustrezajo več, kadar potrebujemo izmenjavo informacij med različnimi zdravstvenimi inštitucijami. Vse zgoraj navedene razlike predstavljajo oviro za celovito ter hitrejšo diagnostiko in za konzultacije na daljavo pri bolnikih s srčno-žilnimi boleznimi.

Izdelan informacijsko-komunikacijski sistem telemedicinski bi uporabili za rešitev dveh ključnih kliničnih problemov. Prvi problem je pošiljanje dvanajst kanalnega EKG posnetka iz regionalnih bolnic ter predhospitalnih urgentnih enot in ZD v primeru suma na akutni miokardni infarkt. To bi omogočilo, da dežurni zdravnik, ki je prisoten 24 ur dnevno, odčita EKG pri bolniku s sumom na infarkt in po telefonu svetuje lečečemu zdravniku kaj naj stori z bolnikom. Drugi klinični problem je on-line pošiljanje koronarografskih posnetkov neposredno po izvedbi koronarografije iz drugih kateterskih laboratorijev (Izola, Šempeter, Celje), ki bi jih takoj pregledal interventni kardiolog in zdravniku v drugi bolnišnici lahko svetoval, kako naj opravi intervencijo oziroma kaj je najbolje za bolnika.

III. BIOMEDICINSKE PLANETARNE RAZISKAVE

Pričujoči projekt bo izkoriščal obstoječo infrastrukturo in nove raziskovalne programe, ki bodo prispevali k evropski mreži raziskovalnih laboratorijev in institucij, katere se ukvarjajo z raziskavami namenjenimi bivanju v vesolju. Poudariti gre, da je osebje Instituta »Jožef Stefan«, Odsek E1, razvilo lunarni simulator v katerem je možno izvajati dolgotrajne eksperimente mirovanja v horizontalnem položaju (bed rest) v pogojih hipoksije. Namen takšnih simulacij je, da se prouči kombiniran vpliv hipoksije in zmanjšane težnosti (0.16 zemljine gravitacije je jakost gravitacije na Luni) na fiziološke sisteme ljudi in da se razišče možne nasprotne terapevtske ukrepe, ki bi bili uporabni na Luni.

Serija poiskusov neaktivnosti (bed rest) in hipoksijo bo narejena na ljudeh v obstoječi raziskovalni infrastrukturi: Centru za biomedicinske planetarne raziskave Planica (Slovenija). Študije neaktivnosti bomo načrtovali kot ponavljajočo križno obliko. V teku študije bodo osebe trajno v vodoravnem položaju, osamitev brez izhodov iz stavbe v trajanju do 5 tednov. Osebe bodo vključene v tri protokole: hipoksična neaktivnost, normoksična neaktivnost ali hipoksična osamitev.

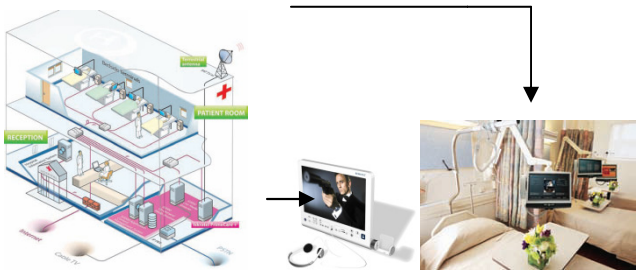
Med študijo neaktivnosti bodo osebe omejene na njihove postelje za vnaprej določen čas. Ves čas bodo deležne stalnega medicinskega nadzora, tj. 24 ur na dan, 7 dni na teden, celoten čas študije. Z namenom nadzora njihovega počutja kot tudi procesa dekondicije, bomo merili naslednje spremenljivke, neprestano ali v rednih intervalih:

– Srčni utrip
– Krvni pritisk
– Telesno temperaturo in podobno
– Dihanje
– Odvzem vzorcev krvi itd.

Cilj partnerjev v konzorciju je razviti in implementirati vse uporabljene brezžične tehnologije v »infotainment« portal. Ta bo omogočal tudi izpolnjevanje vprašalnikov, ki bodo obravnavali:

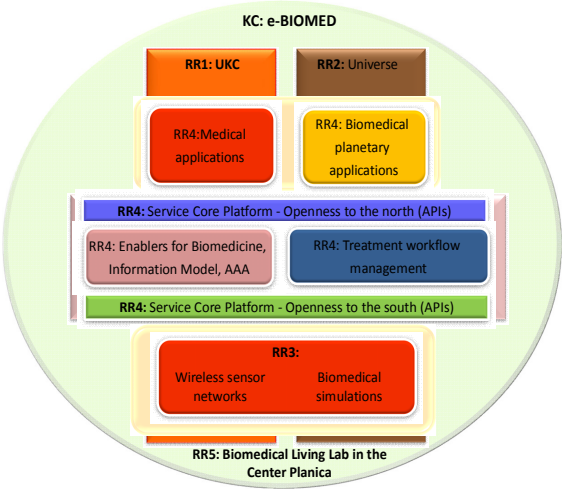
njihovo počutje, apetit, potencialne znake višinske bolezni, toplotno udobje itd.

Oris zgornjih informacij je med študijami neaktivnosti potreben, da se zagotovi varnost oseb kot tudi uspeh izvedenih študij. Običajno se informacije sprejemajo ob določenih dnevnih intervalih na zahtevo osebja. Z opisano opremo se bodo te meritve izvajale avtomatično in kontinuirano. Predvideva se, da bo potrebno minimalno posredovanje osebja. Poleg tega bo komunikacijska programska in strojna oprema, ki je prav tako del tega predlaganega projekta, razvita na način, da bo sodelavcem v vključenih regionalnih bolnicah in raziskovalnih institutih omogočila daljinski nadzor nad preiskovanci.



Slika 3: ISKRATEL Primacare Platform

IV. ORGANIZACIJSKA SHEMA PROJEKTA



Slika 4: Konceptualna shema kompetenčnega centra e-BIOMED

Projekt e-BIOMED sestavlja pet raziskovalnih projektov, od tega so štirje industrijske in eden eksperimentalno razvojno narave. RR1: Aplikacije v medicini in RR2: Biomedicinske planetarne raziskave sta vertikalna in aplikativna, medtem ko sta RR3: Brezžična senzorska omrežja in medicinske simulacije in RR4: Napredna IKT platforma za uporabo na področjih biomedicine, horizontalna projekta, ki zagotavljata infrastrukturne rešitve. Eksperimentalni razvoj vseh naštetih projektov je zaokrožen v RR5: Biomedicinski živi laboratorij v Centru Planica, ki bo stična točka raziskovalcev in razvijalcev pri preverjanju razvitih uslug in izdelkov na beta nivoju.

V. UČINEK PROJEKTA NA ŽIVLJENJE LJUDI IN NA RAZVOJ REGIJE

Ob zaključku dela v e-BIOMED bomo imeli pripravljene tehnološke in funkcionalne rešitve, s katerimi bo možno na zahtevo države vseh 750.000 gospodinjstev po Sloveniji v naslednjih letih priključiti na omrežje telemedicine/teleoskrbe preko širokopasovne komunikacijske infrastrukture. V tem primeru, bi bila Slovenija prva EU regija (država), ki bi realizirala EU strategije za e-Zdravje, ki načrtuje dostop teh rešitev v vsa gospodinjstva in do vsakega državljana. Glede na podatke iz literature ocenjujemo, da bi s tem skupne letne stroške državnega proračuna za zdravstvo in socialno skrbstvo, ki do 25 %, zmanjšali za 10 % kar predstavlja kar 2,5 % letnega državnega proračuna. Ob tem bodo bistveno manjši tudi izpusti CO2 zaradi nepotrebnosti voženj bolnikov do zdravstvenih institucij. Postavitev omrežja bo pomemben poslovni projekt, s katerim bodo partnerji in njihovi podizvajalci povečali gospodarsko rast in zaposlovanje v Sloveniji. S takšnim inovativnim pristopom center e-BIOMED, osnovan na potencialih in kreativnosti podjetij ter medicinske in raziskovalne sfere, udejanja namere »Izhodne strategije Slovenije« in druge prioritete strateških dokumentov RS in EU. Z možnostjo za dvigovanje kvalitete življenja obolele in ostarele/dementne populacije istočasno generira napredne in inovativne tehnološko medicinske produkte za globalni trg. Rešitev telemedicinskega omrežja za 2 milijona naših državljanov, bo odličen prodajni produkt Slovenije z možnostjo prodaje v več kot 200 EU regij in drugih tržišč po svetu kot je npr. Rusija in Kitajska. Ključna pri celotni zgodbi pa je pravočasnost in hitrost izvedbe.

Izvedba in vzdrževanje telemedicinskega in teleoskrbnega projekta bo zahteval velik človeški napor. Sama izgradnja širokopasovnega omrežja do 750.000 domov v Sloveniji zahteva predvsem finančna vlaganja in veliko zanesljivost, robustnost in koherentnost IKT tehnologij. TM in TO omrežje pa je povezano z šolanjem različnih nivojev strokovnjakov, ki bodo najprej naučili ljudi kako deluje omrežje in kako se ob potrebi v njega vključijo. Gre za obsežno delo na terenu in zagotovitev 24 urno neprekinjeno podporo končnim uporabnikom. Seveda bo potrebno tudi izvežbati ekipe za telemedicino in teleoskrbo v vseh zdravstvenih inštitucijah in domovih za ostarele. Celoten sistem je potrebno vzdrževati in dopolnjevati ter transnacionalno povezati najmanj do sosednjih držav, kar je povezano z mobilnostjo državljanov. Ob tem pa same telemedicinske konzultacije med zdravniki specialisti nimajo nobene omejitve in se lahko izvajajo med katerimi koli centri na svetu.

Možnost novih potencialnih delavnih mest za udejanjanje telemedicinskega in teleoskrbnega nacionalnega omrežja ocenjujemo med 30.000 in 50.000.

VI. ZAKLJUČEK

Z noveliranjem Strategije ministrstva za zdravstvo RS v zadnjih mesecih (članki, dokumenti in predstavite dr. Dorijana Marušiča in dr. Mateje deLeonni Stanonik) daje možnost začetka uresničitve vizije telemedicine projekta eBIOMED že do konca 2011. Poleg članov konzorcija eBIOMED bo potrebno vključiti še vrsto podjetij in strokovnjakov, kar bo pospešilo udejanjanje telemedicinskega omrežja predvsem tudi z prenosom že izvedenih rešitev iz držav EU, ZDA, zahodnega Balkana in ostalega sveta.

ZAHVALE

Zahvaljujeva se članom konzorcija eBIOMED za njihov prispevek pri pripravi projekta. Posebej pa Ani Robnik, Romanu Trobcu in Igorju Mekjaviću pri pripravi tega članka.

LITERATURA

[1] Projektna prijava KC eBIOMED, konzorcij eBIOMED, november 2010.
[2] R. Trobec in U. Stanič, Telehealth: A Myth or Reality; to be presented at MIPRO conference May 2011, Opatija, Croatia.
[3] U. Stanič in J.Stanič, Reginal Innovation Strategy of Slovenia Konferenca: Towards competitivnes by innovations, 30. 9. - 1. 10. 2010, Zagreb, Croatia.
[4] R.Latifi, R.C.Merrell, C.R. Doarn, at all, »Initiate-Build-Operate-transfer – A Strategy for Establishing Sustainable Telemedicine Programs in Developing Countries: Initial Lessons from the Balkans, Telemedicine and e-Health 15(19):956-69, 2009.
[5] Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij o koristih telemedicine za paciente, zdravstvene sisteme in družbo, Bruselj, 4. 11. 2008, COM(2008)689 konč.
[6] Teletrauma in Arizona, Mateja de Leonni Stanonik, MD, PhD, The Surgeon General, RS, Chief Executive, The Integrated Program for Telemedicine & eHealth of RS, Professor of Global Health. George Washington University; Rifat Latifi, MD, FACS, Professor of Clinical Surgery, Director, Southern Arizona Teletrauma and Telepresence Program, Associate Director, Arizona Telemedicine Program, University of Arizona, Tucson, Arizona.

Uroš Stanič je doktoriral je leta 1975 na Fakulteti za elektrotehniko Univerze v Ljubljani. Od leta 1974 je bil vodja Odseka za Automatiko, biokibernetiko in robotiko Instituta Jozef Stefan, leta 1994 ustanovitelj Pisarne za Transfer tehnologije in koordinator FEMIRC/IRC Slovenija. Od 204 do 2007 je vodil RTDI oddelek v Univerzitetni kliniki za respiratorne in alergijske bolezni Golnik. Istočasno je bil zunanji ekspert v mestni občini Ljubljana, Oddelek za gospodarske dejavnosti in turizem. Je avtor ali soavtor več kot 50 znanstvenih člankov, več kot 150 konferenčnih prispevkov, 18 patentov, 22 tehnoloških transferjev v industrijo in medicino. Bil je član številnih nacionalnih, EU in ZDA RRI projektov. Leta 1995 je ustanovil in je bil prvi predsednik International Functional Electrical Stimulation Society – IFESS. Od 2004 dalje je podpredsednik slovenske tehnološke platforme I-Techmed. Leta 2009 je bil izvoljen za predsednika sveta Zavoda Biomedicinska raziskovalna skupina BRIS.

Jana Stanič se je kot direktorica svetovalnega podjetja Kosezi d.o.o. specializirala za pripravo raziskovalnih in inovacijskih domačih in EU projektov, ki so sofinancirani z nepovratnimi sredstvi. V svoji karieri je napisala oziroma sodelovala pri pisanju prek 100 nacionalnih in EU projektov. Ima obširne izkušnje z vodenjem velikih konzorcijev, pripravo potrebne dokumentacije ter komunikacijo z razpisovalci.

Lokacijske storitve, RFID senzorji za uporabo v bolnišničnih okoljih

Matevž Mesojednik, Uroš Slak, Astec d. o. o.

Povzetek — V prispevku je predstavljen primer dobre prakse posvojitve koncepta »Internet stvari« med uporabniki informacijskega okolja sodobne bolnišnice. Uvedba novih komunikacijskih tehnologij, ki temeljijo na brezžičnih širokopasovnih povezavah, je na primeru Bolnišnice Golnik omogočila konsolidacijo kliničnih in administrativnih procesov znotraj bolnišnice, varnejšo izmenjavo informacij, boljšo podporo pri odločanju ter lažje povezovanje ljudi in informacij.

Prikazani so sodobni koncepti izmenjave informacij v bolnišničnem okolju, ki so zasnovani na integraciji storitev brezžičnega omrežja, telefonije, senzorskih omrežij za lociranje pacientov ter bolnišničnega inventarja, temperaturnih listov, inteligentnih sistemov za obveščanje in zalednih bolnišničnih aplikacij. Izpostavljena je dodana vrednost sinergije informacijsko-komunikacijskih in medicinskih znanj ter teh pozitiven vpliv na izkušnjo bolnišničnih pacientov in na poslovne procese organizacije.

Ključne besede — internet stvari, brezžično omrežje in storitve, lokacijske storitve, radijsko frekvenčna identifikacija, RFID, Vitel 2011

Abstract — Success story of Internet of Things – IoT adoption into modern Medical Grade Network is presented in this article. Introduction of these ground-breaking communication technologies based on wireless broadband connections, enables the hospital to consolidate its clinical and administrative procedures, safely exchange information, improve its decision-making process, and facilitate its interconnection of people and information. An example of good practice forms a basis to demonstrate the cutting-edge concepts of hospital information exchange involving an array of integrated elements, such as wireless IP telephony services, services to locate patients and hospital inventory, nurse call, intelligent notification systems, and background hospital applications. Above all, the emphasis is placed on the added value brought by the synergy of information communication know-how and medical expertise, and on the positive impact of these solutions on patient's experience and organization's business processes.

Keywords — Internet of Things, Wireless Network and Services, Location Services, Radio Frequency Identification, RFID, VITEL 2011

I. UVOD

Klinika Golnik je pacientom in osebju prijazna ustanova, ki se ves čas svojega delovanja trudi uvajati pristope, ki zagotavljajo hitrejšo, predvsem pa učinkovitejšo obravnavo bolnišničnih pacientov. V duhu vizije izboljšanja oskrbe in okrevanja pacientov je bilo v preteklem letu vzpostavljeno sodobno komunikacijsko omrežje, ki združuje pestro paleto komunikacijskih gradnikov, brezžičnih senzorjev (značk) in povezanih medicinskih pripomočkov.

Primarni cilj prenove informacijskega sistema je bilo zagotavljanje visoko razpoložljive brezžične informacijsko-komunikacijske infrastrukture, ki nudi nemoteno, hitro in stabilno uporabo bolnišničnih virov na vseh lokacijah bolnišnice. Novo storitveno okolje, ki odpira širok nabor možnosti za uveljavitev sodobnih bolnišničnih tehnologij in aplikacij, je postalo zgled sorodnim ustanovam tako doma, kot zunaj slovenskih meja.

V bolnišnicah se dobršen del informacij, s katerimi razpolaga in operira zdravstveno osebje, nanaša na paciente in potek njihove oskrbe. Zdravstveno osebje potrebuje za kvalitetno izvajanje zdravljenja vsak trenutek ažurne podatke ob pacientu, poleg tega pa tudi možnost neposrednega beleženja podatkov v bolnišnični informacijski sistem. Rešitev ponuja dodano vrednost razpoložljivosti informacij na mestu ob bolniški postelji.

Prenova lokalnega komunikacijskega omrežja Bolnišnice Golnik je bila od pobude do same realizacije zasnovana z željo po tesnejši integraciji zalednih bolnišničnih aplikacij z modernimi brezžičnimi komunikacijskimi storitvami. Slednje je uporabnikom bolnišničnih storitev ponudilo hitrejši pretok informacij in prijaznejše načine komunikacije, ki niso pogojeni z njihovo trenutno lokacijo.

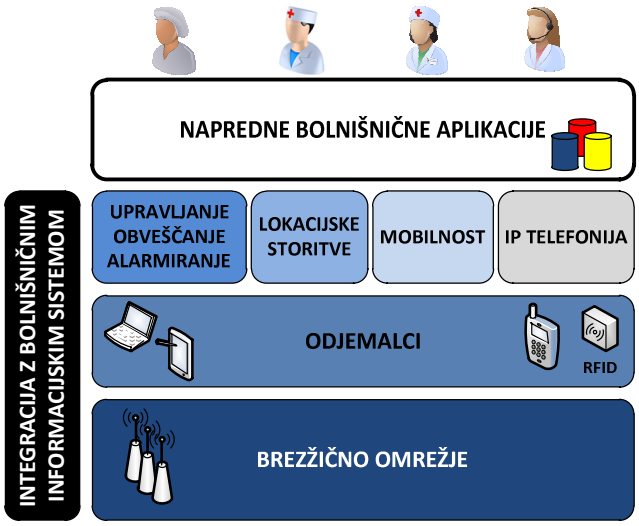
Vzpostavljeno brezžično omrežje sestavljajo t.i. lahke dostopovne točke (angl. LightWeight Access Point), ki so povezane na centralne krmilnike brezžičnega omrežja. Slednji predstavljajo jedro brezžičnega sistema in skrbijo za njegovo brezhibno delovanje, t. j. nazivno obratovanje dostopovnih točk ter upravljanje in nadzor nad dostopovnimi točkami in uporabniki. Temeljni gradnik lokacijske rešitve je lokacijski strežnik, čigar naloga je obdelava podatkov o lokacijah mobilnih postaj in senzorjev v brezžičnem omrežju. Sistem omogoča uporabo in kombiniranje različnih tehnik zaznave lokacije končnih točk (metoda

triangulacije, Time Difference of Arrivals – TDOA, Received Signal Strength Identification – RSSI).

Varovanje informacij v Bolnišnici Golnik je zaradi zaupne narave podatkov pacientov ključnega pomena. Nosilna brezžična tehnologija prinaša dodatna tveganja, zato je bila zasnova ustrezne varnostne politike in največja varnost v komunikacijskem sistemu prvotnega pomena. Varovanje informacijskih bolnišničnih virov je izvedeno z uporabo najsodobnejših varnostnih tehnologij, ki omogočajo kar najboljše možno varovanje tako za omrežje kot za uporabnike bolnišničnih storitev.

II. NAPREDNE BOLNIŠNIČNE STORITVE

V prvi polovici leta 2010 je bil v prostorih Bolnišnice Golnik organiziran promocijski dogodek, odprt širši javnosti, katerega namen je bil prikaz uporabe naprednih storitev v bolnišnični praksi [3]. Demonstracija uporabe storitev, razvitih in delujočih na vzpostavljenem brezžičnem omrežju, je naletela na topel odziv in spodbudo pri nadaljnji posvojitvi naprednih bolnišničnih aplikacij.



Slika 1: Storitveno IOT okolje Bolnišnice Golnik

V nadaljevanju navajamo paleto v Bolnišnici Golnik prikazanih storitev:

– uporaba naprednih lokacijskih storitev,
– uporaba brezžičnih telefonskih storitev na celotnem območju bolnišnice,
– integracija s sistemom sestrskega klica,
– računalnik ob pacientovi postelji,
– nadzor okoljskih dejavnikov,
– centralizirano upravljanje in nadzor komunikacijskega omrežja.

V zadnjem prispevku s področja medicinske informatike [1] smo ilustrirali koncepte uvajanja sodobnih komunikacijskih rešitev v bolnišnična okolja. Pozitivne učinke povezovanja bolnišničnih procesov in informacijsko komunikacijskih virov v bolnišnični sistem »internet stvari« želimo bralcu dodatno orisati s primeri dobre prakse uporabe brezžičnih senzorjev RFID za lociranje in identifikacijo bolnišničnih sredstev.

III. LOKACIJSKE STORITVE V BOLNIŠNIČNEM INFORMACIJSKEM SISTEMU IOT

V centralnem nadzornem sistemu brezžičnega komunikacijskega omrežja Bolnišnice Golnik so bile že ob vzpostavitvi podpornega omrežja vnesene mape celotnega kompleksa klinike. Lokacijski prikaz nudi hitrejše ravnanje v primerih morebitnih okvar (npr. izpad dostopovne točke ali centralnega krmilnika) in drugih anomalij v omrežju.

V integraciji z lokacijskim strežnikom in uvedbo značk RFID (angl. Radio Frequency Identification), ki omogočajo radiofrekvenčno identifikacijo, je mogoče storitev razširiti z natančnejšim lociranjem odjemalcev brezžičnega sistema in s sistemom inteligentnega obveščanja o dogodkih.

Uporaba lokacijskih storitev za lociranje bolnišničnih virov mora upoštevati ustrezne zakonske ureditve. Tekom snovanja scenarijev uporabe smo se v ta namen obrnili na strokovno mnenje informacijske pooblaščenke, katere odgovore povzemamo spodaj.

– Spremljanje gibanja pacientov s pomočjo brezžičnega omrežja v javnih zdravstvenih zavodih **ni dopustno**.
– Izvedba brezžičnega omrežja v javnih zdravstvenih zavodih, ki pacientom omogoča klicanje na pomoč v nujnih primerih in ki hkrati omogoča določitev lokacije pacienta v trenutku, ko pomoč pokliče, **je dopustna**.
– Daljinsko spremljanje zdravstvenega stanja (brez podatka o lokaciji) s pomočjo brezžičnega omrežja v javnih zdravstvenih zavodih **je dopustno**, če pacient to izrecno dovoli.
– Spremljanje gibanja zaposlenih s pomočjo brezžičnega omrežja v javnih zdravstvenih zavodih **ni dopustno**.

V nadaljevanju so navedeni primeri potencialno zanimivih storitev in dobrih praks vpeljave lokacijskih storitev v informacijskem sistemu bolnišnice. Vsi so bili praktično prikazani na komunikacijskem sistemu Bolnišnice Golnik.

A. Nadzor temperature in vlage

Z značkami RFID, ki imajo vgrajen temperaturni senzor, se lahko na enostaven način nadzoruje temperatura v prostorih, kjer se nahajajo zdravila ali oprema, občutljiva na temperaturne spremembe. Ob kritični spremembi temperature se sproži alarm, ki obvesti skrbnika o anomaliji.

Podjetje Astec je v okviru priprave predstavitvenih scenarijev razvilo aplikacijo, ki omogoča tudi prikaz proženih obvestil na ekranu pozvanega / naslovljenega brezžičnega (WiFi) IP telefona.

Slika 2: Nadzor temperature hladilnika

B. Optimizacija izkoriščenosti bolnišničnega inventarja

Z uporabo lokacijskih storitev lahko skrbnik bolnišničnega inventarja v vsakem trenutku ugotovi, kje se oprema nahaja in ali je v uporabi. Opremo, ki ni v uporabi, vrne na mesto, s katerega bo najhitreje zopet prišla v uporabo.

C. Popis bolnišničnega inventarja

Popis sredstev je proces, ki se v organizacijah tipično izvaja periodično, enkrat ali dvakrat letno. Predlagana programska oprema omogoča enostavno integracijo z zalednimi sistemi in bazami vodenja stvarnega bolnišničnega inventarja.

Merilni elektronski inštrumenti in drugi medicinski pripomočki so potrebni rednega vzdrževanja. Skrbniki tovrstnih sistemov imajo pregled nad njihovim stanjem in lokacijo ter možnost hitrega servisiranja v primerih okvar ali pretečenega roka, v katerem morajo biti merilni inštrumenti znova umerjeni (kalibrirani).

Slika 3: Primeri značk RFID

D. Nadzor pacientov v posebni oskrbi

Oskrba pacientov v posebni oskrbi ali pacientov z možnostjo prostega gibanja zahteva individualen in stalen nadzor s strani osebja v bolnišnici. Poseben izziv osebju bolnišnice predstavlja iskanje pacientov, ko ti zapustijo sobo ali območje, znotraj katerega je njihovo gibanje omejeno.

Bolnikom v posebni oskrbi se dodeli namenska zapestnica z vgrajeno značko RFID. Urgentni primer lahko s preprosto aplikacijsko logiko opišemo kot nadzorovan bolnišnični vir, ki je ob evidentiranem času zapustil zanj predvideno območje gibanja, vstopil v določen prostor ipd. Sistem lahko obvestilo o incidentu posreduje dežurni bolnišnični ekipi, ki bi v najkrajšem času ustrezno ukrepala.

IV. VPELJAVA LOKACIJSKIH STORITEV V BOLNIŠNIČNO OKOLJE

Z namenom učinkovite zasnove lokacijskih storitev v bolnišničnem okolju je bila vzpostavljena projektna skupina v kompetentno mešani sestavi; bolnišnično osebje (doktor, medicinska sestra in laboratorij), služba za informatiko in podjetje Astec v vlogi strokovnega koordinatorja skupine. Primarni ter dolgoročni cilj skupine je priprava scenarijev lociranja nadzorovanih sredstev bolnišnice in distribuiranega sistema obveščanja o definiranih lokacijskih dogodkih. V času priprave prispevka so bili v okviru projektne skupine predlagani naslednji scenariji uporabe lokacijskih storitev:

- nadzor temperature in vlažnosti v medicinskih hladilnikih za hranjenje imunoloških zdravil,
- nadzor temperature v strežniški sobi s komunikacijsko opremo,
- vodenje temperaturnih listov za nadzor okoljskih dejavnikov,
- lociranje kisikovih jeklenk v prostorih Bolnišnice (glej Sliko 4),
- lociranje pacientov, potrebnih urgentne oskrbe (uporaba senzorjev z vgrajeno urgentno tipko).

A. Načrtovanje lokacijske rešitve

Mape kompleksa Bolnišnice Golnik so vnesene v nadzorni in upravljalni sistem lokacijske rešitve. Slednji omogoča celovit prikaz aktivnih RFID senzorjev (značk) in upravljanje z lokacijskimi dogodki, ki so bili definirani v fazi načrtovanja scenarijev obravnave nadzorovanih bolnišničnih sredstev. V tehnični rešitvi, ki jo je pripravilo podjetje Astec v tesnem sodelovanju s projektno skupino, so bili uporabni scenariji prikazovanja lokacije preslikani na gradnike nadzornega sistema. V nadaljevanju sta predstavljena izvedbeni načrt in metodologija implementacije lokacijske rešitve v bolnišničnem okolju.

Konfiguracija RFID senzorjev: V prvem koraku se namenskim značkam za radiofrekvenčno identifikacijo pripišejo ustrezni tehnični parametri (aktivacija značk, aktivni radiofrekvenčni kanali, frekvenca oglaševanja, znački karakteristični parametri; npr. temperaturni razpon, konfiguracija urgentnih tipk, aktivacija senzorja gibanja). Nastavitev pogostosti osveževanja lokacije senzorja se prilagodi namenu uporabe senzorja:

– Tipično je za potrebe spremljanja temperature lokacija senzorja le drugotnega pomena, saj so stacionarni tudi hladilniki oz. prostori pod temperaturnim nadzorom. Na drugi strani pogojuje komunikacijo senzorja z lokacijskim strežnikom zahtevana frekvenca odčitavanja temperature, ki je osnova za poznejšo obdelavo in pripravo temperaturnih listov.
– V scenarijih uporabe lokacijskih storitev, kjer je odzivnost obveščanja o spremembah lokacije kritična, se pogostost osveževanja prilagodi na dovolj nizek časovni interval. Kot primere storitev navajamo lociranje dementnega pacienta pod posebno oskrbo, lociranje bolnišničnega inventarja v skupni rabi, urgentno obveščanje v primeru, ko pacient zapusti zanj predvideno območje gibanja.

Konfiguracija značk in njihova aktivacija omogočata takojšnjo detekcijo in lokacijski prikaz v nadzorno-upravljalnem sistemu. Vizualizacija samodejno prepoznanih značk služi hkrati kot preizkus preciznosti lociranja značk in pogostosti osveževanja njihove lokacije. Korak se ponovi večkrat (priporočeno periodično) v naslednjih fazah realizacije, t. j. po sami razporeditvi značk med nadzorovana sredstva.

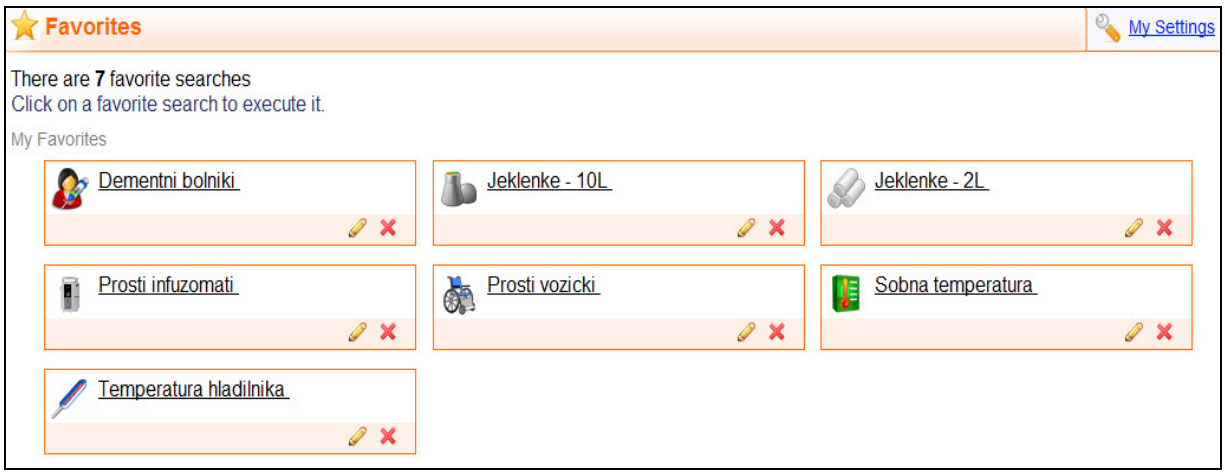
Nadzor nad bolnišničnimi sredstvi: Pomemben korak implementacije lokacijskih storitev predstavlja kategorizacija in asociacija značk z nadzorovanimi sredstvi v bolnišnici. Posameznim značkam se pripiše namen uporabe in ime, ki naj kar najbolj reprezentativno opisuje nadzorovani objekt (npr. temperaturni senzor v laboratorijskem hladilniku #5). Poln opis lokacije senzorja v kompleksu bolnišnice ni potreben, saj je lokacija senzorja v vsakem trenutku že razvidna v grafičnem upravljalnem vmesniku.

Lokacijska segmentacija: Intuitivni grafični vmesnik lokacijskega nadzornega sistema omogoča poljubno definicijo omejenih območij znotraj kompleksa bolnišnice. Na ta način se lahko pogosto kompleksen zemljevid celotne bolnišnice razdeli na manjše lokacijske cone, v katerih je pravočasno lociranje bolnišničnih sredstev ključnega pomena. Priporočena razdelitev je bodisi povsem logistična (npr. oddelki znotraj bolnišnice) bodisi prilagojena izbranemu sistemu obveščanja (npr. spremljanje razpoložljivosti vozičkov v sprejemni pisarni).

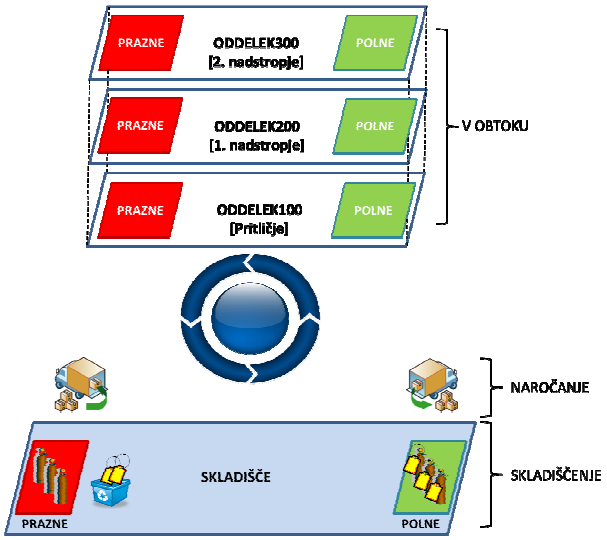
Namestitev senzorjev RFID: Sledi razporeditev in fiksiranje značk RFID na predhodno dogovorjena sredstva (koncept Internet Of Things) v prostorih bolnišnice.

Upravljanje z lokacijski dogodki: Zasnova ustrezne politike upravljanja z lokacijskimi dogodki je v procesu vzpostavitve lokacijske rešitve ključnega pomena. Lokacijski dogodek predstavlja nadzorovano spremembo na opazovanem senzorju, čigar stanje je v periodičnih časovnih intervalih zabeleženo na lokacijskem strežniku. Upravljalno-nadzorni strežnik evidentira zgolj dogodke, ki so kot taki v sistemu predhodno definirani. V nadaljevanju navajamo primere lokacijskih dogodkov, ki so bili v praksi preizkušeni v bolnišničnem okolju Klinike Golnik.

– Pacient je pritisnil na urgentno tipko.
– Temperatura je presegla # °C (oziroma poljubno definirano tolerančno območje).
– Nadzorovano sredstvo na prehodu med nadzorovanima conama (vstop in izstop).
– Pacient miruje več kot # minut.
– Nadzorovani objekt je zapustil kompleks bolnišnice.
– Kisikove jeklenke v dotičnem oddelku bolnišnice niso na voljo / so zopet na zalogi.



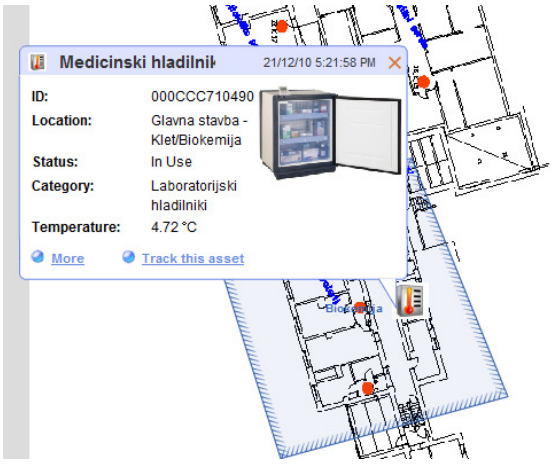
Slika 4: Upravljanje in lociranje bolnišničnih sredstev



Slika 5: Proces skladiščenja in vodenja inventarja O2 jeklenk

Obveščanje: Lokacijski dogodki se beležijo in v nastavljivem časovnem obdobju (angl. Data Retention) hranijo na lokacijskem strežniku. Kot taki so dostopni upraviteljem sistema, ki je lahko en sam skrbnik ali definirana skupina uporabnikov z nastavljivimi pravicami upravljanja (branja in/ali spreminjanja). Sistem obveščanja je sestavni del nadzornega sistema lokacijske rešitve, ki omogoča obveščanje in posredovanje lokacijskih obvestil poljubnemu uporabniku informacijskega sistema bolnišnice. Z ustrezno oblikovano politiko obveščanja in uporabo sodobnih komunikacijskih kanalov je mogoče sistem optimizirati na način, ki nudi kar najhitrejši dostop do informacij na uporabniku priljubljeni način (brezžični telefon, elektronska pošta, zvočni / svetlobni signal).

Poročanje: Nadzorni sistem lokacijske rešitve že v osnovi razpolaga s pestro paleto aplikativnih tipov poročanja o lokacijskih dogodkih. Poročila v različnih formatih zapisa prikazujejo kronološki potek zabeleženih lokacijskih dogodkov v nastavljivem časovnem obdobju.



Slika 6: Spremljanje temperature (in lokacije) medicinskega hladilnika

V. ZAKLJUČEK

Brezžično omrežje Bolnišnice Golnik je plod dobrega sodelovanja različnih skupin znotraj zdravstvene ustanove in sistemskega integratorja Astec d. o. o. Vzpostavljeno storitveno okolje je spodbuden začetek in uresničuje pomembno vizijo Bolnišnice – z novo komunikacijsko podporo do učinkovitejše obravnave bolnikov.

V prispevku so predstavljeni primeri dobre prakse uvajanja lokacijsko obarvanih elementov »interneta stvari« v bolnišnično okolje. Informacija o lokaciji nadzorovanih sredstev vnaša novo dimenzijo v ponudbo bolnišničnih storitev. Pozitivni učinki sinergije znanj ter tesnega sodelovanja medicinske in telekomunikacijske stroke tudi v praksi že vplivajo na kvalitetnejšo oskrbo in boljšo uporabniško izkušnjo v bolnišničnem okolju.

LITERATURA

[1] Dnevi Marije Tomšič; Matevž Mesojednik: Z novo komunikacijsko podporo do učinkovitejše obravnave bolnikov, januar 2011.
[2] Kongres medicinske informatike MI'2010; Uroš Slak, Matevž Mesojednik: Z novo komunikacijsko podporo do učinkovitejše obravnave bolnikov.
[3] Povezava do predstavitve storitev: http://www.youtube.com/watch?v=J53Qef2OKb0, maj 2010
[4] Astec d. o. o.: Lokacijske storitve http://www.astec.si/index.php/sl/lokalna-omreja/lokacijske-storitve, april 2010
[5] Aeroscout: Real-time Location, Status and Condition of Assets, Patients and Staff Throughout Your Hospital

Matevž Mesojednik se je rodil leta 1979 v Kranju. Magistriral je leta 2009 na Fakulteti za elektrotehniko Univerze v Ljubljani s področja informacijske varnosti. Že v času dodiplomskega študija se je pridružil Laboratoriju za telekomunikacije, kjer je uspešno sodeloval pri raziskavah, razvojnih projektih in izvajanju strokovnih izobraževanj. Leta 2007 se je v okviru eno letne specializacije v tujini pridružil podjetju Cisco Systems, od koder ga je pot vodila v domače podjetje Astec. V novem okolju je aktiven na širšem področju informacijske varnosti ter načrtovanju sodobnih informacijsko komunikacijskih sistemov in rešitev.

Povezan dom postaja resničnost za ljudi in stvari

Slobodan Bodnaruk, Mitja Golja, Ana Robnik, Gregor Smolej, Iskratel d. o. o, Kranj

Povzetek — Hiter prodor širokopasovnega Interneta v (skoraj) vsak dom skupaj z mobilnimi komunikacijami ter čedalje bolj prisotnimi TV napravami velikih dimenzij ponujajo bogato paleto novih informacijskih, komunikacijskih in zabavnih storitev slehernemu uporabniku. Rešitev »Povezan dom« ponuja uporabniku ob gledanju poljubne televizijske oddaje ali vsebin na Internetu tudi sprotni vpogled v status in aktivnosti odsotnih članov družine ali prijateljev, izmenjavo sporočil in fotografij z njimi ne gleda na njihovo oddaljenost, govorne in video klice s katerimkoli partnerjem, povezanim na fiksno ali mobilno omrežje. In vse to s pomočjo TV naprave, pridružene video kamere in pripadajočega daljinskega upravljalca ter poljubnega domačega telefonskega priključka.

Rešitev »Povezan dom« je odprta rešitev in primerna tudi za povezovanje stvari in ne le za povezovanje članov družine in prijateljev, ki uporabljajo multimedijske storitve. Inovativne zamisli uporabe na področju hišne avtomatizacije, energetike in na področju e-zdravje (njegov pomembni del je telemedicina) ter na ostalih področjih bodo ob potrebnih dopolnitvah prinesle novo kakovost bivanja in življenja v domu in izven njega.

Prispevek opisuje sodobne svetovne trende ter trenutne aktivnosti, razvojne plane in vizijo Iskratela na področju rešitev za »Povezan dom«, ki vsebujejo celotno paleto komponent, od naročniških naprav preko komunikacijskih povezav do infrastrukturne opreme potrebne za zagotavljanje vsebin, nadzora in zaračunavanja storitev. Obstoječa rešitev je odprta in kot taka odlično izhodišče tudi za povezovanje stvari med seboj.

Ključne besede — povezan dom, Iskratel, povezovanje stvari, internet stvari, IoT

Abstract — The rapid penetration of broadband internet in (almost) every home along with mobile communications, and increasingly present large TV devices offer a rich set of new information, communication and entertainment services to every consumer. The "Connected Home" solution offers a consumer the real-time presence status and information about the activities of absent family members or friends while watching television shows or any content on the internet, the option to exchange messages and photos with them regardless of their distance, and make voice and video calls with any partner connected to a fixed or mobile network. And all this with the help of a TV device with the associated video camera, the corresponding remote control and any home telephone line.

The "Connected Home" solution is an open solution suitable to connect both things and family members and friends who use multimedia services. Innovative ideas on use in the home automation, in the energy industry and on use in the e-health (its important part is telemedicine) and also in other areas, based on the necessary enhancements, will bring a new quality of life in the home and outside it.

This paper describes modern world trends and current activities, development plans and a vision of Iskratel in the field of Connected Home, which contain the entire range of components from consumer devices and communications links to infrastructural equipment required to provide the content, control and billing services. The current solution is open and thus an excellent starting point to interconnect things.

Keywords — Connected home, Iskratel, connecting things, Internet of Things, IoT

I. Uvod

Povezan dom predstavlja in omogoča nove oblike komunikacij in povezanosti med ljudmi in stvarmi ter med stvarmi samimi. Je najbolj naravno okolje za udejanjanje koncepta Interneta stvari (angl. Internet of Things – IoT).

Svetu današnje informacijske in telekomunikacijske povezljivosti dodajamo virtualne in dejanske stvari, ki jih povezujemo med seboj in z ljudmi. To prinaša poleg znanih tehnoloških izzivov in vplivov na samo omrežje ter količino med seboj povezanih entitet in izmenjanega krmilnega in podatkovnega prometa tudi povsem nove sociološke dimenzije, ki se odpirajo z dopolnjevanjem multimedijskih storitev in aplikacij zabavnih vsebin v povezanem domu s storitvami in aplikacijami ter vsebinami, ki povečujejo kakovost življenja vsakega od nas, in čim bolj enakovredno in aktivno vključenost v družbeno dogajanje socialno najbolj ranljivih članov družbe.

Evropska komisija želi z akcijskim načrtom za povečanje blaginje in dobrobiti v Evropi pospešiti uvajanje novih storitev in aplikacij na različnih področjih povezanega doma. Digitalna agenda ([1],[2]) za Evropo je prva od sedmih pobud v okviru strategije Evropa 2020 za pametno, trajnostno in vključujočo rast, ki jo je Svet Evrope potrdil 31.5.2010. Poseben pomen v tej pobudi imajo področja, ki so povezana s kakovostjo bivanja in življenja v domu in izven njega ter ta, ki omogočajo trajnostni razvoj in socialno vključenost.

Z uporabo naprednih storitev v Iskratelovi rešitvi »Povezan dom« želimo zadostiti zgoraj omenjenim visokim tehnološkim in sociološkim standardom.

II. REŠITEV »POVEZAN DOM«

Pomemben pokazatelj razvitosti današnje družbe je število domačih širokopasovnih priključkov. Sodobno opremljen dom razpolaga z dostopom v Internet, ki mu pomeni okno v svet informacij, zabave in komunikacij s pomočjo brskalnikov, elektronske pošte, sporočilnih in socialnih omrežij.

Takšen dom navadno razpolaga z novejšo TV napravo, ki omogoča sprejem video vsebin iz različnih virov kot so živi programi (Digital Video Broadcasting – Terrestrial oziroma DVB-T, satelit, kabel, Internet Protocol television oz. IPTV) in vsebine na zahtevo (angl. Video on Demand oz. VoD).

Družinski člani sodobnega doma za medsebojno komunikacijo uporabljajo mobilne telefone, s pomočjo katerih se pogovarjajo, izmenjujejo kratka sporočila (SMS), pošiljajo fotografije (MMS) in z novejšimi »pametnimi« telefoni spremljajo medsebojno stanje prisotnosti in pripravljenosti za komunikacijo.

Povezan dom združuje vse dobre lastnosti vseh treh predstavljenih elementov in sicer širokopasovni dostop, novejšo TV napravo in mobilne telefone v novo vrednost in kakovost:

– poleg informativnih in zabavnih vsebin prinaša na TV zaslon osebne komunikacijske kanale, ki se jih sodobni domači uporabnik sicer poslužuje z različnimi napravami kot so domači računalnik (PC), domači fiksni telefon ter družinski mobilni telefon(i).
– s pomočjo daljinskega upravljavca in pridružene video kamere ponuja uporabniku obilico aktualnih informacij o družinskih članih in prijateljih (prisotnost, pripravljenost za komunikacijo), možnost sprotne in hitre vzpostavitve kontakta v obliki izmenjave sporočil, slik, datotek ter govorne (avdio) in/ali slikovne (video) komunikacije.

Predstavljeni komunikacijski kanali Povezanega doma so le prvi korak v razvoju te rešitve. Naslednji koraki bodo ponudili tudi oddaljeni nadzor in upravljanje z domačimi napravami s pomočjo mobilnega telefona ali poljubnega internetnega dostopa. Uporabnik, ki je trenutno zdoma bo lahko nadzoroval lastni domofon, odpiral/zapiral vrata doma, spremljal kdo je pred vrati, fotografiral obiskovalca, prižigal/ugašal luči, nadzoroval temperaturo v prostorih, ipd.

III. STORITVE V POVEZANEM DOMU

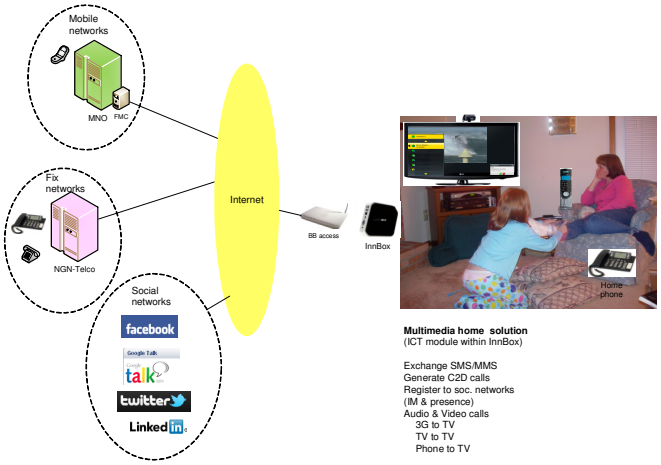
Rešitev »Povezan dom« v osnovi potrebuje relativno skromen nabor elementov za uporabnika:

– fiksni domači telefon,
– TV napravo s HDMI (angl. High-Definition Multimedia Interface) vhodom (LCD/Plasma/LED)
– širokopasovni dostop na domu,
– media center (n.p. naprava HD30) z daljinskim upravljavcem in USB kamero,
– VoIP račun (priključek) na fiksnega in/ali mobilnega operaterja (prednost rešitve je, da ima lahko priključen hkrati na oba operaterja)

ter za napredne storitve:

– vmesnike za nadzor domačih naprav,
– IP-domofon,
– dodatne USB kamere …

S pomočjo širokopasovnega dostopa se media center (n.p. InnBox HD30 [3]) poveže preko Interneta ter registrira VoIP (Voice over IP) telefonske priključke na fiksno in mobilno omrežje. Nato se poveže na vsa socialna omrežja, na katerih ima lastni (ali kar družinski!) račun.



Slika 1: Storitve v rešitvi »Povezan dom«

TV zaslon, ki je priključen na media center (n.p. napravo InnBox HD30) postane na ta način informacijsko/komunikacijsko središče, ki gledalcu omogoča hkrati z gledanjem poljubne video vsebine (živi program, YouTube, video vsebina z domačega računalnika) sprotni vpogled in izmenjavo sporočil z odsotnimi družinskimi člani ali prijatelji, sprejem MMS fotografij, sprejem in oddajo telefonskih klicev ter obvestila o zamujenih klicih.

A. *Povezava na fiksno in mobilno omrežje*

Media center (n.p. naprava InnBox HD30 [3]) se preko Interneta prijavi na lastni VoIP račun (ali več računov hkrati) in njegova TV naprava skupaj z zvočniki in mikrofonom na USB kameri postane telefon. Uporabnik lahko sprejema ali zavrača klice, sestavlja lasten imenik, kliče prijatelje s pomočjo daljinskega upravljavca neposredno iz imenika.

Če želi ohraniti uporabo lastnega klasičnega telefonskega aparata, lahko na podoben način (imenik,

daljinski upravljalec) proži klice na način »klikni-za-klic« (angl. Click-to-Dial), pri katerem mu najprej pozvoni lastni telefon in ko se javi, le-ta vzpostavi zvezo z izbrano številko.

Če ima uporabnik VoIP račun tudi pri mobilnem operaterju v okviru FMC (Fixed Mobile Convergence) rešitve, se lahko s tem računom prijavi preko media centra (npr. naprave InnBox HD30 [3]) tudi kot mobilni naročnik. Na ta način njegov televizor postane tudi mobilni telefon, kar mu omogoči, da dejanski GSM ugasne in tako varčuje baterijo in zmanjšuje elektromagnetno sevanje v svojem domu.

Postopki govornih telefonskih zvez so podobni kot pri fiksnem telefonu. Mobilna telefonija v Povezanem domu pa prinaša pomembno prednost – to je sprejem/oddaja kratkih sporočil preko TV naprave in še posebej sprejem MMS fotografij iz poljubnega mobilnega telefona na TV zaslon. Ker so prejete fotografije avtomatično shranjene na lokalnem disku, je priprava celotnega albuma in kasnejše predvajanje fotografij (angl. »slideshow«) zelo poenostavljeno.

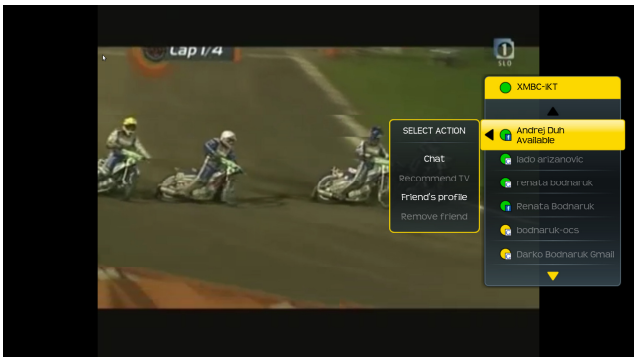
Mobilni 3G aparati omogočajo v Povezanem domu tudi video klice na TV. Tako video klic dobi novo dimenzijo, ker se namesto miniaturnega videa na zaslonu telefona prikaže celozaslonska slika na TV. Takšne video klice je možno uporabiti tudi za pregled domačih prostorov z oddaljene lokacije.

Video klice je prav tako možno prejemati tudi preko VoIP računov fiksnega omrežja kot tudi vzpostavljati s pomočjo daljinskega upravljavca.

B. Povezava v socialna omrežja

Sodobna in zelo popularna socialna omrežja (Facebook, Twitter, Google Talk ipd.) zahtevajo od domačega uporabnika, da se usede za računalnik (ali vzame prenosnik ali tablični računalnik) ob aktivnem TV zaslonu. Rešitev »Povezan dom« omogoča, da se po prijavi uporabnika v socialna omrežja in uporabi tega računa, prenesejo vse informacije (prisotnost, sporočila, novice) iz računalnika na TV zaslon. Tako je uporabniku omogočeno, da vzporedno z gledanjem TV spremlja prisotnost prijateljev, odgovarja na sporočila, pošilja prijateljem priporočila za programe ipd.

Vse opisane možnosti in prednosti rešitve »Povezan dom« ponujajo nov pristop uporabnikom, ki niso vajeni uporabe računalnika ali mobilnega telefona za vstop v danes zelo bogati svet informacij in komunikacij z eno samo preprosto napravo kot je daljinski upravljalnik.



Slika 2: Media center v rešitvi »Povezan dom«

IV. »POVEZAN DOM« - DOMAČA AVTOMATIZACIJA IN E-ZDRAVJE

V okviru povezanega doma je opaziti vse večji trend integracije storitev hišne avtomatizacije in pametnega doma skupaj s komunikacijskimi in zabavnimi storitvami. V današnjem času hitrega tehnološkega razvoja se spreminja bivalno in delavno okolje. Poslovni uporabniki potrebujejo celovite telekomunikacijske in informacijske rešitve, dodatne inteligentne in varnostne storitve.

A. Domača avtomatizacija

Tudi v domovih se uvajajo pametne naprave in inteligentno upravljanje. Razširil se je pojem inteligentna oziroma pametna hiša (pisarna). Inteligentno hišo bi lahko opredelili kot hišo, ki poseduje znanje o vseh svojih stanjih in lastnostih, zna komunicirati z zunanjim svetom ter je sposobna sama reagirati na določene situacije in pri tem spreminjati različna stanja v hiši. Funkcionalnosti, ki jih pripisujemo inteligentni hiši so:

– vklop/izklop luči,
– dviganje/spuščanje senčil,
– nadzor nad električnimi porabniki,
– regulacija temperature,
– integrirani alarmni sistem (detekcija plinov, požara, gibanja),
– nadzor nad porabo energije,
– video nadzor.

Pod domačo avtomatizacijo lahko zajemamo tudi skupino različnih tehnologij in naprav, sistemov in storitev, ki zgradbam dodajajo nove funkcionalnosti in neko dodatno »inteligenco«. Ti uporabniku omogočajo lažji, bolj učinkovit in predvsem mobilen nadzor ter možnost upravljanja s svojimi nepremičninami.

Pameten oziroma inteligenten sistem je zmožen samodejnega upravljanja z napravami, za katere je zadolžen, detekcije morebitnih napak v delovanju in ustreznem odzivu nanje ter upoštevanja ukazov uporabnikov. Uporabniki lahko upravljajo s pametnimi sistemi s pomočjo različnih terminalnih naprav, od

stacionarnih do mobilnih. Možna je uporaba osebnih računalnikov, tablic, mobilnih telefonov ali TV sprejemnika. Pri tem sta ključnega pomena enostavnost in varnost uporabe ter tudi mobilnost.

Slika 3: Primer implementacije domače avtomatizacije na media centru in TV sprejemniku v rešitvi »Povezan dom«

V Iskratelu smo tako v okviru rešitve »Povezan dom« implementirali storitev domače avtomatizacije, kar na media centru (Innbox HD30 [3]). To dodatno demonstrira univerzalnost naprave in enostavnost dodajanja novih aplikacij. Uporabnik tako lahko upravlja z razsvetljavo in sistemom prezračevanja ter si nastavi različne časovne scenarije le-teh.

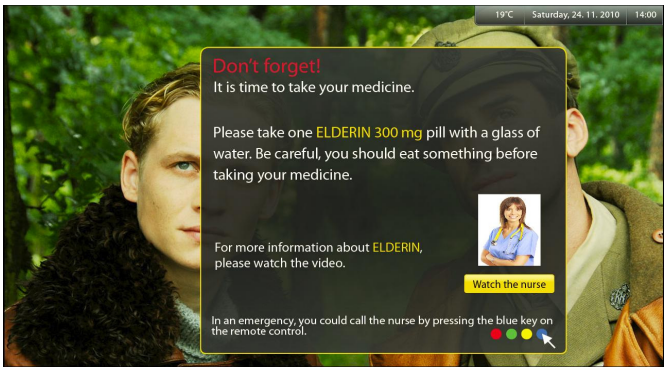
B. e-zdravje

E-zdravje (angl. e-health) predstavlja širši pojem in bolj uporabniško naravnano uporabo informacijskih in telekomunikacijskih tehnologij, še zlasti Interneta za izboljšanje zdravja in zdravstvene oskrbe. S pomočjo storitev e-zdravja lahko izboljšamo zdravstveno stanje v smislu osveščanja o zdravem načinu življenja in izboljšanju kakovosti zdravstvene oskrbe. Izjemno pomemben del e-zdravja je telemedicina, ki pomeni uporabo najsodobnejših telekomunikacijskih in informacijskih tehnologij za zdravniško pomoč na daljavo.

Glavni motiv tovrstnih storitev je na eni strani izboljšanje zdravstvene oskrbe, preventive, bolj udobno nadzorovanje zdravljenja, na drugi strani pa predstavlja vpeljava tovrstnih storitev zmanjšanje stroškov zdravstva. To je danes ob negativnih demografskih gibanjih in staranju prebivalstva eden ključnih motivov.

Kot primer e-zdravja smo v Iskratelu pripravili implementacijo nekaj storitev, ki smo jih podkrepili tudi s študijo uporabnosti.

Pripravili smo aplikacijo opomnik za zdravila, ki omogoča zlasti starejšim izboljšati nadzor nad jemanji zdravil. Poleg opomnikov se uporabniku izpišejo tudi navodila za jemanje zdravil, možna pa je tudi komunikacija z zdravstvenim osebjem v primeru nujnih situacij. Ključno vodilo pri snovanju tovrstnih aplikacij je bilo enostavnost uporabe, kar je potrdilo tudi testiranje pri uporabnikih.



Slika 4: Primer aplikacije opomnika za zdravila na media centru in TV sprejemniku v rešitvi »Povezan dom«

Trenutno storitve e-zdravja nadgrajujemo z zajemom različnih zdravstvenih parametrov, prenos podatkov v sprejemni center in morebitno pomoč osebi v stiski. S pomočjo različnih senzorjev se lahko zajemajo različni parametri, npr. gibanja, temperature in vlažnosti kože. Senzorji v določenih časovnih intervalih pošiljajo preko brezžične povezave podatke in alarme v media center, ta pa preko Interneta v sprejemni center. Podatki in alarmi se obdelajo in analizirajo, v primeru resnega alarma pa se sproži intervencija.

Tovrstna storitev je namenjena predvsem zaščiti starejših ljudi pri boleznih, kot so demenca, Alzheimerjeva bolezen, izguba spomina, srčne bolezni in podobno. Prednosti takšnega načina nadzora in oskrbe so olajšana oskrba na domu, finančni prihranki, oskrba 24 ur na dan, hiter odziv na stisko bolnika, ipd.

Uporabnikom s posebnimi potrebami in starejši populaciji je potrebno prikazati in približati dosežke, možnosti in izzive današnjega sodobnega življenja in tako izboljšati kakovost njihovega življenja. S tem se bo povečala njihova zdravstvena in socialna varnost in spodbudilo komuniciranje z okoljem (individualnim in družbenim), v katerega se lahko enostavneje in enakovredneje vključijo.

V. SMERNICE V PRIHODNJE

V Iskratelu bomo nadaljevali z razvojem rešitve »Povezan dom« ter tudi s spremljanjem trendov s področja internetnih aplikacij in storitev. Na področju komunikacijskih storitev vidimo glavne poudarke v smeri RCS (angl. Rich Communication Suite [4]) in integraciji ter povezovanju različnih komunikacijskih aplikacij (Google Talk, Skype, Facebook …) v enoten uporabniški vmesnik. Na segmentu zabavnih storitev se glavni trendi v smeri dodajanja aplikacij in trgovine z le-temi. Mednje spadajo tudi dodatne aplikacije s področja domače avtomatizacije in e-zdravja, ki jih bomo razširjali z dodatnimi funkcionalnostmi.

VI. ZAKLJUČEK

Iskratel je s svojo rešitvijo »Povezan dom« odgovoril na najpomembnejše tehnološke in sociološke izzive današnjega časa. Svojo rešitev je obogatil s sodobnimi in inovativnimi usmeritvami na področju Interneta stvari, in sicer s povezovanjem stvari (storitev, pametnih naprav in objektov, senzorjev in atenuatorjev …) s člani družine in prijatelji, ki uporabljajo poleg multimedijskih storitev v različnih omrežjih tudi napredne storitve na področju hišne avtomatizacije in e-zdravje, katerega pomembni del je tudi telemedicina.

Rešitev »Povezan dom« prinaša tudi gradnik širše rešitve za uresničitev akcijskega načrta za povečanje blaginje in dobrobiti v Evropi v okviru Digitalne agende Evropa 2020.

LITERATURA

[1] Evropska komisija: Digitalna agenda za Evropo (objava) http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/571&format=PDF&aged=1&language=SL&guiLanguage=en

[2] European Commision: A Digital Agenda for Europe http://ec.europa.eu/information_society/digital-agenda/documents/digital-agenda-communication-en.pdf

[3] Povezava do Iskratelove rešitve »Povezan dom« in Iskratelovega produkta Innbox HD30, http://www.iskratel.com/en/access/iskratel_CPE/media_center/nettopbox/home.aspx

[4] Domača stran GSMA, Rich Communication Suit, http://www.gsmworld.com/our-work/mobile_lifestyle/rcs/gsma_rcs_project.htm

[5] Stojmenova E., Debevc M., Zebec L., Imperl B. Assisted Living Solutions for the Elderly through Interactive TV. SAME 2010 – 3rd International Workshop on Semantic Ambient Media Experience (NAMU Series) November 2010.

Slobodan Bodnaruk je leta 1974 zaključil univerzitetni študij elektrotehnike na Univerzi v Sarajevu, na Fakulteti za elektrotehniko. V Iskratelu je zaposlen 35 let, najprej v razvojnemu oddelku, kjer je vodil sektor za razvoj programske opreme SI2000 nato pa se je leta 1995 vključil v prodajni Zadnje leto opravlja delo produktnega vodje za rešitve »Povezan dom«, teleglasovanje, kontaktni centri.

Mitja Golja je diplomiral s področja interaktivnih video storitev leta 1999 na Fakulteti za elektrotehniko v Ljubljani. Leta 2003 je magistriral z nalogo »Promet video storitev v širokopasovnih paketnih omrežjih« in sodeloval v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko. Leta 2005 se je zaposlil v podjetju Iskratel, kot vodja oddelka multimedijskih rešitev in kasneje kot vodja produktne linije CPE. Njegovo področje raziskav obsega različne video sisteme in napredne komunikacijske aplikacije.

Ana Robnik je leta 1985 zaključila univerzitetni študij uporabne matematike na Univerzi v Ljubljani, Fakulteta za matematiko, fiziko in mehaniko in 1989 magisterij iz računalništva na Univerzi v LJ, Fakulteta za računalništvo. V Iskratelu je zaposlena 20 let, najprej v IT oddelku, nato pa se je leta 1993 vključila v razvoj nove verzije produktov SI2000 in nato SI3000 ter do leta 2009 vodila sektor za upravljanje in nadzor omrežni elementov portfelja Iskratela. Zadnje leto opravlja delo svetovalke za telekomunikacije, vodi raziskovalno skupino podjetja Iskratel ter koordinira delo v standardizacijskih organizacijah in je aktivna v Telemanagement Forumu.

Gregor Smolej je leta 2000 diplomiral na temo prenosa video vsebin preko ATM omrežij na Fakulteti za elektrotehniko v Ljubljani. Po študiju se je pridružil Iskratelu kot član razvojne ekipe za širokopasovni dostop. V nadaljevanju je postal produktni vodja za strateško produktno družino Iskratela – SI3000 MSAN, kjer je bil zadolžen za rešitve širokopasovnega dostopa (DSL, FTTH, Ethernet). Od leta 2005 je produktni vodja za dostopovno opremo pri uporabniku. Njegovo področje raziskav obsega zagotavljanje večje ergonomije FTTH opreme pri uporabniku in optimalnejše arhitekture gradnikov v domačem omrežju.

Interakcija s fizičnimi objekti v namene upravljanja komunikacijskih storitev

Darko Bodnaruk[1]
Klemen Peternel[2], Urban Sedlar[2]
[1]Obelisk d. o. o.
[2] Univerza v Ljubljani, Fakulteta za elektrotehniko, Laboratorij za telekomunikacije

Povzetek — Prispevek opisuje postopek za krmiljenje telefonske komunikacije na osnovi otipljivega uporabniškega vmesnika, ki je realiziran z uporabo tehnologije NFC. Krmiljenje komunikacije sestoji iz proženja telefonskih klicev, izgradnje konferenčnih klicev in nastavljanja preusmeritev. Članek dodatno opisuje tudi postopek programiranja oznak NFC, prirejen za namene krmiljenja komunikacije.

Ključne besede — NFC, posamezniki s posebnimi potrebami, otipljiv uporabniški vmesnik, komunikacije

Abstract — This article explains a procedure for controlling communications services on the basis of tangible user interface, which is realized by the use of NFC technology. It enables user to trigger phone calls, add participants to the conference, redirect calls and set forwarding by touching appropriate photos and pictograms.

Keywords — NFC, individuals with special needs, tangible user interface, communications

I. UVOD

Krmiljenje telefonskih komunikacijskih storitev zahteva podrobno poznavanje delovanja terminalne opreme, ustrezne motorične spretnosti (vnos podatkov preko pogosto premajhnih tipk), oster vid (branje podatkov prikazanih na zaslonu telefonskega aparata) ter kognitivno sposobnost uporabnika, ki mu omogoča pomnjenje telefonskih številk in navigacijo po večstopenjskih hierarhičnih menijih (npr. izbira klicane številke iz telefonskega imenika ali izbira telefonske funkcionalnosti). Znaten del populacije (starejši, posamezniki s kognitivnimi in motoričnimi motnjami, slepi in slabovidni) ima posledično težave z uporabo tudi najpreprostejših komunikacijskih rešitev.

Članek v nadaljevanju opisuje rešitev tehničnega problema osnovnega in naprednega krmiljenja komunikacijskih storitev z uporabo otipljivega uporabniškega vmesnika (angl. Tangible User Interface – TUI) na osnovi tehnologije komunikacij v bližnjem polju (angl. Near Field Communication – NFC).

Rešitev je bila implementirana s strani podjetja Obelisk d.o.o.

II. TEHNOLOGIJA RADIJSKE FREKVENČNE IDENTIFIKACIJE - RFID

Tehnologija, ki se zdi za implementacijo robustnega vmesnika TUI kot naročena, je tehnologija radijske frekvenčne identifikacije (angl. Radio Frequency Identification – RFID). Slednja ima korenine že v času druge svetovne vojne, zato njena prisotnost danes ne predstavlja velike novosti, vendar pa večjo prepoznavnost med širšo javnostjo uživa šele v zadnjih letih. Razlog je predvsem ta, da se jo vedno bolj pogosto povezuje z dejavnostmi kot sta logistika in trgovina (Walmart, Gillete, DHL), hkrati pa zamenjuje vlogo črtne kode v mnogih knjižnicah po svetu in pri nas (primer je splošna knjižnica Kranj). Njen preboj je povezan v največji meri z dejstvom, da je industrija danes zmožna proizvajati RFID oznake ceneje kot kadarkoli prej (optimizirani se procesi izdelave RFID vezja, antene in končnega pakiranja v celoto). Nakup oznak je namreč običajno največji strošek pri vpeljavi tehnologije v obstoječi poslovni proces, z zniževanjem končne cene pa se posledično pojavljajo novi in novi načini njene uporabe. Da bi število implementacij hitreje naraščalo po celem svetu, skrbi mednarodna organizacija EPCglobal, ki je razvila lasten standard, katerega so sprejeli tudi znotraj ISO standardizacijskega telesa. Govorimo namreč o arhitekturi, kjer je na eni strani čitalec, na drugi pa ustrezna oznaka. Slednja je lahko tudi popolnoma pasivna, kar pomeni, da za svoje delovanje ne potrebuje lastnega vira energije. Za oddajo podatka, ki ga nosi, ji zadošča že energija, ki jo s signalom dobi s strani čitalca. Tehnologija deluje na različnih frekvenčnih območjih, pri čemer smo si za našo rešitev izbrali območje visokih frekvenc (13,56 MHz). V tem primeru se podatek med oznako in čitalcem prenaša s pomočjo pojava elektro-magnetne indukcije. Domet je tako majhen in omejen tudi z velikostjo obeh anten (čitalec, oznaka).

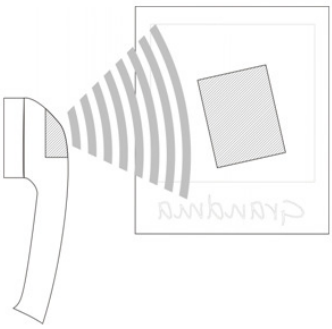
Tehnologija RFID se na omenjenem frekvenčnem področju v zadnjem času pod imenom komunikacije v bližnjem polju pojavlja tudi v svetu telekomunikacij, kot del klasičnih mobilnih aparatov (standard ISO/IEC 14443-A). Princip ostaja popolnoma enak, le da tokrat vlogo čitalca (lahko pa tudi oznake) prevzemajo mobilni telefonski aparati. Tako se pojavljajo številne

možnosti novih aplikacij na tem področju. Največkrat se govori o področjih, kot so mobilno plačevanje, t.i. pametni plakati ter elektronske vstopnice. Tako je NFC največji preboj do sedaj doživel v ZDA in na Japonskem, kjer obstaja kar nekaj primerov dobrih praks s področja javnega transporta, plačevanja in oglaševanja preko pametnih plakatov.

III. OBELISK TUI

Obelisk TUI omogoča proženje komunikacijskih storitev z interakcijo med fizičnim svetom (objekti) in digitalnim sistemom, ki ga podpira komponenta klicnega strežnika Obelisk One.

Vmesnik je sestavljen iz pasivnega in aktivnega dela. Pasivni del predstavlja omejeno področje, na katero je mogoče namestiti objekte, opremljene z oznakami NFC, ki pri uporabniški interakciji služijo kot vizualna sidra. Primer takšnih objektov predstavljajo fotografije, slike in piktogrami. Pasivni del je lahko realiziran kot plutovinast stenski pano, ki omogoča pritrjevanje fotografij, slik in piktogramov, opremljenih z ustreznimi oznakami NFC. Aktivni del predstavlja sonda NFC, ki na osnovi oddaje in sprejema elektromagnetnih impulzov identificira unikatno kodo (angl. Uniform Resource Identifier) oznake NFC, nameščene na posameznem objektu na panoju. Sonda je priključena neposredno na telefonski terminal ali je vanj vgrajena in komunicira s programskim odjemalcem, ki teče na strojni opremi telefonskega terminal (Slika 1).



Slika 1: Sonda NFC je lahko del telefonskega terminala

Z uporabo predlagane rešitve je izvedba klica preprosta in intuitivna ter se izvaja neposredno preko interakcije z objekti v fizičnem svetu. Slika 2 predstavlja primer dotika fotografije osebe, označene z oznako NFC, z aktivno sondo NFC, ki je vgrajena v telefonsko slušalko terminala v namene proženja telefonskega klica.

Terminalna oprema služi tudi podajanju zvočnih in vizualnih potrdil, opozoril ali navodil uporabniku, kar uporabo vmesnika dodatno olajšuje s podajanjem povratnih informacij.

V nadaljevanju so podrobneje opisani postopki za nadzor telefonske komunikacije na osnovi otipljivega uporabniškega vmesnika, ki temelji na uporabi tehnologije NFC in uporablja oznake NFC v kombinaciji s samostojno sondo NFC, ki je povezana s telefonskim aparatom, ali s sondo NFC, ki je vgrajena v določen del telefonskega terminala, npr. v telefonsko slušalko.

Slika 2: Proženje klica z uporabo Obelisk TUI

IV. POSTOPKI UPORABE

Postopke uporabe lahko razdelimo v tri skupine: postopek za izvedbo telefonskega klica, postopki za upravljanje s potekom telefonskega klica ter postopek za programiranje oznak NFC za uporabo v namene krmiljenja telefonske komunikacije.

A. Postopek za izvedbo telefonskega klica

Postopek za izvedbo telefonskega klica poteka na sledeč način. Uporabnik, ki želi poklicati določeno telefonsko številko, prime v roko sondo NFC, ki je del telefonskega aparata. Uporabnik sondo NFC, katere oddajno/sprejemni del je vidno označen na površini ohišja, v katerega je vgrajena, približa vnaprej določenemu fizičnemu objektu, opremljenemu z oznako NFC. Fizični objekt je lahko fotografija osebe, ki jo uporabnik želi poklicati. NFC oznaka, s katero je fizični objekt opremljen, vsebuje elektronski zapis telefonske številke uporabnika ali ustrezno identifikacijsko kodo, ki je enolično povezana s telefonsko številko uporabnika. Ko uporabnik sondo NFC približa oznaki NFC, s katero je fizični objekt opremljen, ali se je dotakne, se sproži postopek radijsko-frekvenčne identifikacije, v katerem sonda prebere podatke, zapisane na oznaki NFC. Po uspešno opravljenem postopku radijsko-frekvenčne identifikacije oznake programski agent, ki teče na strojni opremi telefonskega aparata, izvede postopek validacije prebranih podatkov. V primeru, da podatki predstavljajo veljavno telefonsko številko oziroma, da je mogoče iz podatkov na enoličen način pridobiti veljavno telefonsko številko, programski agent izvede vizualno, zvočno ali zvočno-vizualno potrditev uspešne prepoznave telefonske številke. V naslednjem koraku programski agent, ki teče na strojni opremi telefonskega terminala, izvede telefonski klic z

uporabo mehanizma, vgrajenega v telefonski aparat, ki zagotavlja transparentno izvedbo klica neodvisno od tehnologije telefonskega omrežja (npr. PSTN, ISDN, SIP, idr.).

B. Postopki za upravljanje s potekom telefonskega klica

Upravljanje s potekom telefonskega klica obsega postopek za ustvarjanje novega konferenčnega klica, postopek za dodajanje naročnika v obstoječ konferenčni klic, postopek za nastavitev preusmeritve dohodnih klicev na drugo številko in postopek za preusmeritev trenutno aktivnega klica na drugo številko.

Postopek za ustvarjanje novega konferenčnega klica poteka na sledeč način. Ko se uporabnik nahaja v stanju običajnega klica, se s sondo NFC dotakne fizičnega predmeta (npr. fotografije), opremljenega z oznako NFC. Sonda NFC izvede postopek radijsko-frekvenčne identifikacije, nakar programski agent izvede validacijo prebranih podatkov. V primeru, da podatki predstavljajo veljavno telefonsko številko, oz., da je mogoče iz podatkov na enoličen način pridobiti veljavno telefonsko številko, programski agent izvede vizualno, zvočno ali zvočno-vizualno potrditev uspešne prepoznave telefonske številke. V naslednjem koraku programski agent, ki teče na strojni opremi telefonskega terminala, kreira konferenčni klic ter vanj doda novega telefonskega naročnika, oboje z uporabo mehanizma, vgrajenega v telefonski aparat.

Postopek nastavljanja preusmeritve novih dohodnih klicev na drugo številko poteka na naslednji način. Ko se uporabnik ne nahaja v stanju aktivnega klica, se s sondo NFC dotakne fizičnega predmeta, opremljenega z oznako NFC, na kateri je zapisano sporočilo z zahtevo po preusmeritvi. Sonda NFC izvede postopek radijsko-frekvenčne identifikacije, nakar programski agent izvede identifikacijo zahteve po preusmeritvi, zapisane na NFC oznaki. V primeru uspešne identifikacije zahteve po preusmeritvi programski agent sproži zvočno, vizualno ali zvočno-vizualno potrditev. V naslednjem koraku se uporabnik s sondo NFC dotakne fizičnega predmeta, opremljenega z oznako NFC, na kateri je zapisana telefonska številka izbranega naročnika. Programski agent izvede identifikacijo in validacijo telefonske številke naročnika, zapisane v NFC oznaki. V primeru uspešne identifikacije in validacije programski agent sproži zvočno, vizualno ali zvočno-vizualno potrditev ter nastavi preusmeritev z uporabo mehanizmov, vgrajenih v telefonski aparat.

Postopek preusmeritve trenutno aktivnega klica na drugo številko poteka na naslednji način. Ko se uporabnik nahaja v stanju aktivnega klica, se s sondo NFC dotakne fizičnega predmeta, opremljenega z oznako NFC, na kateri je zapisano sporočilo z zahtevo po preusmeritvi. Sonda NFC izvede postopek radijsko-frekvenčne identifikacije, nakar programski agent izvede identifikacijo zahteve po preusmeritvi, zapisane na NFC oznaki. V primeru uspešne identifikacije zahteve po preusmeritvi programski agent sproži zvočno, vizualno ali zvočno-vizualno potrditev. V naslednjem koraku se uporabnik s sondo NFC dotakne fizičnega predmeta, opremljenega z oznako NFC, na kateri je zapisana telefonska številka izbranega naročnika, na katerega naj se klic preusmeri. Programski agent izvede identifikacijo in validacijo telefonske številke naročnika, zapisane v NFC oznaki. V primeru uspešne identifikacije in validacije programski agent sproži zvočno, vizualno ali zvočno-vizualno potrditev ter izvede preusmeritev aktivnega klica z uporabo mehanizmov, vgrajenih v telefonski aparat.

C. Postopek za programiranje oznak NFC

Postopek za programiranje oznak NFC za namene krmiljenja telefonske komunikacije poteka na sledeč način. Uporabnik, ki želi oznako NFC opremiti s telefonsko številko ali s kodo, ki je enoznačno povezana s telefonsko številko, najprej izvede zahtevo po programiranju oznake. Zahtevo po programiranju oznake lahko izvede preko menija na telefonskem aparatu ali preko programske opreme na osebnem računalniku, ki je povezana s telefonskim aparatom (npr. preko serijskega ali omrežnega vmesnika). Po uspešni izvedbi zahteve po programiranju uporabnik preko tipkovnice telefonskega aparata ali preko uporabniškega vmesnika s telefonskim aparatom povezanega osebnega računalnika vnese podatke o telefonski številki ali o kodi, ki je enoznačno povezana s telefonsko številko.

Ko uporabnik potrdi vnos telefonske številke, ga telefonski terminal s priključeno ali vgrajeno sondo NFC zvočno, vizualno ali zvočno-vizualno obvesti, naj sondo NFC približa oznaki NFC. Ko uporabnik medsebojno približa sondo NFC in oznako NFC, sonda zazna oznako in nanjo zapiše podatke. Po zapisu programski agent, ki teče na strojni opremi telefonskega terminala in nadzoruje postopek zapisa, uporabnika obvesti o uspehu zapisa (uspešno, neuspešno), ter v primeru neuspešnega zapisa ponudi možnost ponovnega zapisa.

V. ZAKLJUČEK

Prispevek opisuje implementacijo tehnologije za izgradnjo komunikacijskega otipljivega uporabniškega vmesnika. Slednji končnemu uporabniku omogoča proženje nekaterih osnovnih in bolj naprednih komunikacijskih storitev s preprostimi dotiki med sondo NFC in objekti iz fizičnega sveta. Navedeni in podrobneje opisani so tudi posamezni postopki uporabe.

Tipični uporabniki so posamezniki s posebnimi potrebami, ki imajo običajno težave z uporabo obstoječih komunikacijskih naprav.

Rešitev je bila implementirana v okviru razvojnih aktivnosti znotraj podjetja Obelisk. Vložena je bila tudi patenta prijava v namene formalne zaščite intelektualne lastnine.

LITERATURA

[1] Obelisk Phone, dostopno na http://obelisk.si/telephony/obelisk-phone
[2] K. Finkenzeller, RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, second ed., John Wiley and sons, 2004.
[3] P. Sanghera, RFID+ Study Guide and Practice Exams, Syngress Publishing, 2007.
[4] NFC Forum, NFC Data Exchange Format (NDEF), 2006.
[5] NFC Forum, URI Record Type Definition, 2006.
[6] T. Mandel, The Elements of User Interface Design, John Wiley and sons, 1997.
[7] H. Ishii, The tangible user interface and its evolution, Communications of the ACM Vol. 51, No. 6 (2008) pp 32-36.
[8] H. Ishii, B. Ullmer, Tangible bits: towards seamless interfaces between people, bits and atoms, Proceedings of the SIGCHI conference on Human factors in computing systems, 1997, pp 234-241.

Darko Bodnaruk (darko.bodnaruk@obelisk.si) je leta 2002 diplomiral na Fakulteti za računalništvo in informatiko, Univerza v Ljubljani. Med študijem in po njem je delal kot raziskovalec v Laboratoriju za telekomunikacije na Fakulteti za elektrotehniko. Med letoma 2007 in 2009 je kot upravljavec premoženja delal v NLB ter magistriral na Ekonomski fakulteti, v začetku leta 2010 pa je skupaj z nekdanjimi sodelavci ustanovil podjetje Obelisk d. o. o, ki ga tudi vodi.

Klemen Peternel (klemen.peternel@fe.uni-lj.si) je diplomiral leta 2007 na Fakulteti za elektrotehniko Univerze v Ljubljani s področja telekomunikacij. V Laboratoriju za telekomunikacije opravlja razvojno-raziskovalno delo na področju načrtovanja in razvoja telekomunikacijskih sistemov in storitev naslednje generacije. Sodeluje tudi pri pripravi in izvedbi izobraževanj s področja telekomunikacij in programskega jezika Java. Je soustanovitelj in sodelavec v podjetju Obelisk d. o. o.

Urban Sedlar (urban.sedlar@fe.uni-lj.si) je diplomiral leta 2004 na Fakulteti za elektrotehniko, Univerze v Ljubljani in doktoriral leta 2010. Zaposlen je v laboratoriju za telekomunikacije (LTFE) na Fakulteti za elektrotehniko, kjer se ukvarja z raziskavami na področju internetnih sistemov in storitev. Je soustanovitelj in sodelavec v podjetju Obelisk d. o. o.

Seznam avtorjev

A

Alič, Kemal 67–72
Arkko, Jari 58–61

B

Baños, Janie 93–99
Baškovec, Domen 81–84
Bešter, Janez 11–15
Bizjak, Mitja 32–36
Bodnaruk, Darko 118–121
Bodnaruk, Slobodan 113–117

C

Cipriano, Antonio Maria 93–99

Č

Černe, Gregor 32–36

F

Fortuna, Carolina 47–52
Fuertes, Manuel Garcia 93–99

G

Gabrovšek, Fedor 73–76
Golja, Mitja 113–117

H

Humar, Iztok 53–56

J

Javornik, Tomaž 67–72
Jenko, Primož 85–89
Jurjevec, Janez 43–46
Juvan, Uroš 43–46

K

Kastelic, Marko 67–72
Knopp, Raymond 93–99
Kos, Andrej 11–15
Krco, Srdjan 93–99
Kunc, Urban 16–23

L

Laner, Markus 93–99
Larsson, Eric 93–99
Lisec, Simeon 73–76

M

Marinšek, Zoran 32–36
Marović, Djordje 93–99
Mesojednik, Matevž 108–112
Mihelin, Marko 47–52
Mohorčič, Mihael 6–10, 47–52, 67–72

N

Nikaein, Navid 93–99

P

Papič, Igor 27–31
Pavlu, Petr 90–92
Pesko, Marko 77–80
Peternel, Klemen 11–15, 118–121
Pfajfar, Tomaž 27–31
Planina, Andrej 100–102
Pollet, Thierry 2–5

R

Robnik, Ana 113–117

S

Saje, Iztok 85–89
Sedlar, Urban 11–15, 118–121
Sernec, Radovan 73–76
Slak, Uroš 108–112
Smolej, Gregor 113–117
Smolnikar, Miha 47–52, 67–72
Sodja, Jure 62–66
Souvent, Andrej 27–31
Stanič, Jana 103–107
Stanič, Uroš 103–107
Sterle, Janez 11–15
Sušnik, Rudolf 62–66
Svoboda, Philipp 93–99

Š

Škrabl, Denis 67–72
Šmid, Janez 37–42
Štular, Mitja 77–80

T

Tomšič, Andrej 24–26
Tomić, Igor 93–99

U

Umberger, Mark 53–56
Uršič, Goran 43–46

V

Vidmar, Luka 77–80
Vidonja, Tomaž 11–15

Volk, Mojca 11–15
Vučković, Divna 93–99
Vučnik, Matevž 47–52

W

Wu, Yi 93–99

Z

Zebec, Luka 11–15

Ž

Željković, Nenad 93–99