Revija

ISSN 1332-1382

Broj/No 1, 2012. Ericsson Nikola Tesla d.d.

ARHITEKTURA MREŽE
ZA M2M KOMUNIKACIJE

SIGURNOST U M2M KOMUNIKACIJI

M2M KOMUNIKACIJE
U PRIMJENI NAPREDNIH
ELEKTROENERGETSKIH MREŽA

M2M KOMUNIKACIJE
KORIŠTENJEM POKRETNIH MREŽA

ERICSSON

Elektroničko izdanje ISSN 1334-045X

Revija

Broj 1/2012. ISSN 1332-1382

Izdavač:
Ericsson Nikola Tesla d.d.
Krapinska 45, p.p. 93
HR – 10 002 Zagreb
Hrvatska

e-mail: etk.company@ericsson.com

tel.: +385 1 365 4647
tel.: +385 1 365 4055

Priprema:
Kompanijske komunikacije
Ericssona Nikole Tesle

M2M U GLAVNOJ ULOZI

Usred tehnološke revolucije u kojoj primijenjene informacijsko-komunikacijske tehnologije stvaraju umreženo društvo i mijenjaju čitav svijet, sve se veći značaj pridaje novoj komunikacijskoj paradigmi pod nazivom M2M (*Machine-to-Machine*) komunikacija, pod kojom podrazumijevamo autonomnu komunikaciju između strojeva, neovisnu o trenutačnoj interakciji korisnika. Prema predviđanjima Ericssonovih stručnjaka u 2020. godini očekuje nas postojanje 50 milijardi povezanih uređaja čije će se koristi ogledati u mnogim područjima ljudskog djelovanja, poput prometa, sigurnosti, industrije ili zdravstva. Ericssonova vizija budućeg umreženog društva u kojem će svi uređaji od čijeg međusobnog povezivanja možemo ostvariti dodatnu korist, upravo zbog te diferencijalne dobiti, i biti umreženi, otvara neograničene mogućnosti za inovativnost, ali i potrebu za kontinuiranim unaprjeđenjem aktualnih ICT rješenja, portfelja usluga i stručnih znanja svih dionika ICT tržišta.

U želji da vam približimo značaj i potencijal spomenutog tržišta, čija godišnja stopa rasta premašuje 30 posto, cijeli ovaj broj Revije posvećujemo upravo M2M komunikaciji.
Kako bismo osigurali što bolje razumijevanje i unijeli neophodnu standardizaciju u stručnu terminologiju, objavljujemo i odgovarajući glosar, tj. kratki rječnik pojmova na kojem je radilo više znanstvenika i stručnjaka, a rado ćemo ga unaprijediti i vašim prijedlozima/dopunama. Ukratko, u ovom broju možete saznati više o specifičnostima arhitekture mreža za M2M komunikaciju, o komunikaciji između strojeva korištenjem pokretnih mreža te o jednom od primjera korištenja M2M komunikacije, preciznije o njenoj primjeni na polju naprednih elektroenergetskih mreža.
Posebno izdvajamo „gostujući“ članak o sigurnost u M2M komunikacijama, čiji je autor dr. sc. Mario Čagalj, izvanredni profesor s Fakulteta elektrotehnike, strojarstva i brodogradnje u Splitu.

Razvoj industrije je već do sada pokazao veliki potencijal inovativnih usluga koje koriste razmjenu podataka bez ljudske interakcije, a neprestano se ispituju i nove aplikacije te novi modeli poslovanja. Nadamo se da će stranice novog broja Revije pridonijeti vašem boljem razumijevanju izazova koje sa sobom donosi M2M komunikacija, a možda i pomoći konkretizaciji barem dijela ovog velikog tržišnog potencijala koji je pred nama.

Jasna Glavaš
glavna urednica

KRATKI RJEČNIK POJMOVA

M2M i računalstvo u oblaku

Engleski	Hrvatski
Access Point Name (APN)	Konfigurabilni mrežni identifikator
Actuator	Aktuator
Application programming interface, API	Aplikacijsko programsko sučelje
Asset management	Upravljanje imovinom
Asset tracking	Praćenje kretanja imovinom
Authentication	Autentikacija; utvrđivanje vjerodostojnosti; provjera autentičnosti
Authorization	Autorizacija
Automatic Meter Reading (AMR)	Automatsko daljinsko očitanje brojila
Automatic Meter Management (AMM)	Automatsko upravljanje brojilima
Automotive industry	Automobilska industrija
Back-end system	Pozadinski sustav
Backhaul	Mobilno rješenje za sporednu vezu; posrednička mreža; spojna mreža
Bootstrapping	Podizanje sustava
Brokering model	Posrednički model
Bundling	Objedinjavanje
Business to business communication (B2B)	Međusobna poslovna komunikacija; elektronička veleprodaja
Business Support System (BSS)	Sustav poslovne potpore
Charging	Naplata
Cloud Computing	Računalstvo u oblaku
Connectivity	Povezivost
Control plane	Nadzorna ravnina
Consumer electronics	Potrošačka elektronika
Core network	Jezgrena mreža
Dashboard	Prilagođeni izgled stranice
Data centers	Podatkovni centri
Data plane	Podatkovna ravnina
Deep Packet Inspection (DPI)	Duboka inspekcija paketa
Edge and backhaul networks	Ujedinjeni rubni i posrednički dijelovi mreže
Embedded systems	Ugrađeni sustavi
e-reader	Elektronički čitač knjiga
Fleet management	Upravljanje vozilima

Goods tracking	Praćenje robe
Home automation	Automatizacija u kućanstvu
Holistic approach	Holistički pristup; prikaz elementa u funkciji sustava, a ne zasebno
Jitter	Varijacija kašnjenja
Latency	Vrijeme čekanja; latencija
Machine-to-Machine Communication (M2M)	Komunikacija između strojeva (M2M)
Messaging	Usluga prijenosa poruka; poručivanje
M2M area network	M2M prostorna mreža
M2M gateway	M2M pristupnik
M2M capillary network	M2M kapilarna mreža
M2M device	M2M uređaj
M2M management functions	Upravljačke funkcije M2M komunikacije
M2M service bootstrapping	Inicijalizacija M2M usluge
Mesh networks	Isprepletena struktura mrežnih čvorova
Middleware	Međuprogram; program koji djeluje između aplikacije i mreže
Mobility	Pokretljivost, mobilnost
Monitoring	Nadgledanje
Mobile Virtual Network Operator (MVNO)	Mobilni virtualni mrežni operator
Network proxy	Mrežni zastupnik (posrednik)
Operations Support System (OSS)	Sustav operativne potpore
Orchestration	Orkestracija; proces automatiziranog uređivanja, koordiniranja i upravljanja kompleksnih informacijskih sustava i servisa.
Plug and play	Uključenje i pokretanje, pojednostavljenje, pojednostavljene instalacije
Policy enforcement	Provođenje politike
Power Line (Powerline) Communication (PLC)	Komunikacijska mreža koja koristi vodove električne mreže
Provisioning	Pridjeljivanje i rezervacija
Proxy	Zastupnik; posrednik
Public safety	Javna sigurnost, zaštita
Radio Access Network (RAN)	Radijska pristupna mreža
Rating	tarifiranje
Reusable	Ponovno iskoristiv
Revenue management	Upravljanje prihodima
Roaming	Prelaženje između mreža
Service capabilities	Mogućnosti usluge
Scalability	Skalabilnost, prilagodljivost veličini
Service Level Agreement (SLA)	Ugovor o razini kvalitete pružanja usluga
Service enabler	Omogućitelj usluge
Service enablement	Osposobljenost za pružanje usluge; omogućavanje usluge
Smart grid	Napredna elektroenergetska mreža
Smart meter	Pametno brojilo
Smart metering	Pametno mjerenje
Standard	Standard, norma
Surveillance	Nadzor
Telematic	Telematika, prometna telematika
Telemetry	Telemetrija
Uplink	Uzlazna veza
Use case	Slučaj korištenja
Utilities	Komunalne službe
Value chain	Vrijednosni lanac
Web browser	Web preglednik
Wide Area Network (WAN)	Mreža širokog područja; široko rasprostranjena mreže
Wireless sensor network	Bežična senzorska mreža

SADRŽAJ:

Željko Popović, Vanesa Čačković, Darijo Burjan

Ericsson Nikola Tesla d.d., Zagreb, Hrvatska
Ericsson Nikola Tesla d.d., Zagreb, Croatia

ARHITEKTURA MREŽE ZA M2M KOMUNIKACIJE

NETWORK ARCHITECTURE FOR M2M COMMUNICATION

Sažetak

Broj umreženih strojeva i uređaja stalno raste, mjenjajući percepciju uobičajene komunikacije prema mrežama koje su neovisne o ljudskoj interakciji. Komunikacija između strojeva (M2M, Machine-to-Machine) je nastala kao nova komunikacijska paradigma koja omogućava da strojevi međusobno komuniciraju bez ljudske intervencije. M2M komunikacije su potaknule široku paletu aplikacija uključujući pametna mjerenja, udaljeno praćenje zdravstvenog stanja, upravljanje vozilima i praćenje vozila, udaljeni nazor, i automatizaciju u industriji. Ovo zahtjeva razvoj novih rješenja za učinkovito posluživanje velikog broja uređaja koji djeluju autonomno.
Ovaj rad daje pregled Ericssonove cjelovite M2M arhitekture. Rad uglavnom pruža cjelovitu perspektivu M2M komunikacija, integraciju M2M uređaja i omogućavanje M2M usluge. Razmatrana je integracija u specifičnim poslovnim aplikacijama i odnos prema ostalim ključnim omogućiteljima potrebnim za M2M orijentirane usluge.
Opisana Ericssonova cjelovita M2M arhitektura nudi pogled unaprijed i može se koristiti kao temelj za definiranje horizontalnog sustava i mogućnosti usluga kao i za dizajn industrijski specifičnih rješenja koja adresiraju potrebe poput transporta, komunalnih službi, zdravstva i rješenja u drugim područjima primjene.

Abstract

The number of networked devices is continuously increasing, changing the conventional perception of communication towards networks that are idependent from human interaction. Machine- to-machine (M2M) communications has emerged as a new communication paradigm that allows machines to directly communicate with no human intervention. M2M communications has insired a wide variety of applications, including smart metering, healthcare monitoring, fleet management and tracking, remote security sensing, and industrial automation. This requires development of novel solutions to efficienty serve a huge number of devices that interact autonomously at global level.
This paper provides an overview of the Ericsson end-to-end M2M architecture. It mainly provides an end-to-end perspective of M2M communications, integration of M2M devices and M2M service enablement. Integration into specific business applications and the relation to other key enablers required for M2M-oriented services is introduced.
The Ericsson end-to-end M2M architecture described here is forward looking and will be used as a foundation to define horizontal system and service capabilities as well as to design industry specific solutions addressing the needs of, for example, transport, utilities, eHealth, and solutions in other application domains.

KLJUČNE RIJEČI:	KEY WORDS:
M2M komunikacije	M2M Communication
Mrežna arhitektura	Network infrastructure
Omogućavanje M2M usluga	M2M Service Enablement
Ericssonova platforma za M2M komunikaciju	Ericsson Device Connection Platform

1 Uvod

Najnovije procjene ukazuju da s pet milijardi trenutno uspostavljenih pokretnih veza diljem svijeta razvijena tržišta upravo dostižu točku zasićenja. Najveći dio tih veza je uspostavljen za potrebe glasovne ili podatkovne komunikacije pokretnim telefonom. Nasuprot tome, broj preostalih vrsta uređaja koji se mogu umrežiti je i dalje relativno malen. Različite analize predviđaju da bi ukupan broj svim pokretnih umreženih uređaja mogao narasti na 15 milijardi do 2015. godine i na više od 50 milijardi do 2020. godine. S obzirom na zasićenost pokretnim telefonima, najveći rast u ukupnom broju umreženih uređaja predviđa se preostalim vrstama pokretnih uređaja.
Prema procjenama konzultantske tvrtke Bergt Insigth očekuje se rast broja umreženih uređaja za M2M komunikaciju putem pokretne mreže, po godišnjoj stopi od 27,2%, da bi u 2016.godini dosegnuo brojku od 359,3 milijuna veza [2].
Sagledavajući značaj poslovnog potencijala koji usluge zasnovane na M2M komunikaciji donose telekomunikacijskim operaterima, pretpostavka je da će se operateri aktivnije uključivati u daljnji razvoj M2M rješenja.
S obzirom na povećanje složenosti M2M eko-sustava, za očekivati je da će se usluge zasnovane na M2M komunikaciji realizirati kroz partnersko udruživanje više strana. No izostanak globalnih normi za komunikaciju između uređaja te razvoj aplikacija, kao i druga otvorena pitanja iz segmenta korisničke podrške, kvalitete usluga, ugovora o uporabi pokretnih telefona na području stranih mreža i druga, svakako će predstavljati aktualne izazove uspostavi usluga zasnovanih na M2M komunikaciji. Iznos prosječnog mjesečnog prihoda po uređaju, koji se obično kreće na razini od 10 posto onog koji ostvaruje prosječan „čovjek-korisnik“, nameće potrebu da se poslovni model zasniva na velikom broju korisnika. I konačno, veliki broj različitih usluga koje se prilagođavaju specifičnim potrebama pojedinih korisnika predstavljat će veliki izazov u prilagođavanju postojećih sustava za obračun i naplatu usluga.

Glavne potrebe za aplikacijama zasnovanim na M2M komunikaciji s udaljenim uređajima predstavljanju potrebe i zahtjevi poslovnog sektora i vlada. Dok su poslovni korisnici usmjereni k smanjenju troškova i povećanju učinkovitosti, vlade razloge takvim rješenjima pronalaze u održivosti, sigurnosti i sociološko-ekonomskim učincima. Jednako je tako bitno spomenuti i rastući trend broja uspostavljenih servisa zasnovanih na M2M komunikaciji a namijenjenih potrošačkoj elektronici (poput slanja informacija o trenutnim vremenskim i prometnim prilikama uređajima za prometnu navigaciju).
Ovi odvojeni segmenti tržišta ukazuju na potrebu za pronalaženjem zajedničkog rješenja za M2M komunikaciju kojim bi se preoblikovao dosadašnji M2M eko-sustav s ciljem pomirenja poslovnih i tehnoloških aspekata različitih tržišnih domena. Osim što iziskuje razbijanje, odnosno dijeljenje vrijednosnog lanca na nove aktere, ovakva transformacija također zahtijeva standardizaciju usluga, tehnologija, komponenti i aplikacija koje sudionici uvode u transformirani vrijednosni lanac s ciljem. Normizacijom bi se osiguralo deregulirano tržište te potakla konkurentnost za sve komponente vrijednosnog lanca.

Jedna od bitnih pretpostavki za razvoj rješenja zasnovanih na M2M komunikaciji ostvarena je tehnološkim napretkom uređaja nadograđenih mogućnošću njihova umrežavanja te neprestanim smanjenjem njihove jedinične cijene proizvodnje. Time uređaji postaju cjenovno pristupačni za masivniju uporabu te rješenjima za M2M komunikaciju osiguravaju uspostavu ekonomije razmjera. S druge strane svojim umrežavanjem i podrškom za IP tehnologije, ovakvi uređaji otvaraju brojne mogućnosti proizvođačima aplikativnih rješenja.
Ekonomija razmjera potiče i nove trendove u drugim dijelovima M2M sustava. Pritisak na upravljanje velikim brojem pretplatnika, različitim tipovima pretplata, grupama podataka koji se u komunikaciji razmjenjuju, okidačima, alarmima i drugim, iziskuje od proizvođača M2M platformi uspostavu funkcionalnosti za efikasno upravljanje cjelovitim M2M sustavima. U isto vrijeme, s ciljem postizanja još višeg stupnja automatizacije i operativne izvrsnosti, prema dobavljačima M2M platforme postavljaju se zahtjevi za integracijom same platforme sa sustavima za operativnu, ali i poslovnu podršku. Pri tome se poseban naglasak stavlja na integraciju sa sustavima za naplatu i fakturiranje te sa sustavima drugih sudionika u vrijednosnom lancu.

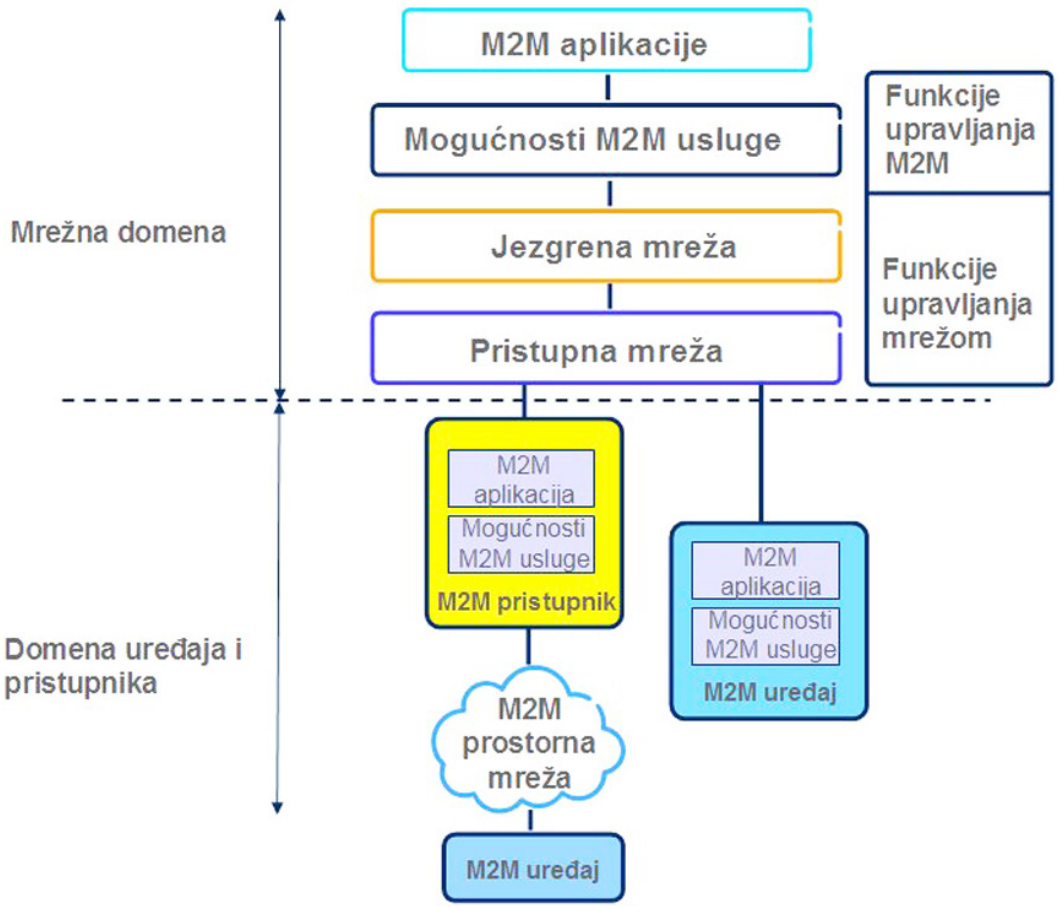
2 M2M arhitektura

2.1 Standardizacija arhitekture M2M sustava

Veliki tržišni potencijal komunikacijskih sustava umreženih strojeva javlja se kao posljedica brojnih potencijalnih primjena i slučajeva uporabe, ali i dostupnosti različitih pristupnih tehnologija koje se mogu iskoristiti u njihovoj implementaciji. Ti sustavi moraju biti pouzdani, skalabilni, sigurni i upravljivi. Najjednostavniji način za postizanje toga jest prilagodba korištene prijenosne tehnologije (npr. javne pokretne mreže) specifičnim zahtjevima M2M komunikacije (veliki broj umreženih uređaja, različiti tipovi uređaja, niska potrošnja energije itd.). To se postiže standardizacijom, u okviru koje se velika pažnja posvećuje razmatranju arhitekture mreže za M2M komunikacije.

2.1.1 Standardizacijske aktivnosti instituta ETSI

Tehnički odbor zadužen za komunikaciju strojeva u okviru standardizacijske udruge ETSI dao je pregled arhitekturalnog koncepta [15] za podršku pružanja takvih usluga.



Slika 2-1: Pojednostavljena arhitektura M2M komunikacija prema ETSI

Slika 2-1 prikazuje pojednostavljenu arhitektutru M2M sustava s njegovim komponentama. M2M sadrži mrežnu domenu i domenu uređaja i pristupnika.

Mrežna domena (eng. Network domain) se sastoji od sljedećih elemenata:

» Pristupna mreža: mreža koja omogućuje domeni M2M uređaja i pristupnika komunikaciju s jezgrenom mrežom. Pristupne mreže uključuju razne fiksne i bežične pristupne tehnologije poput xDSL, HFC, satelit, GERAN i UTRAN te eUTRAN, W-LAN i WiMAX.

» Jezgrena mreža (eng. Core Network, CN) osigurava:
- minimalno IP povezivost, a potencijalno i druge načine povezivosti,
- funkcije kontrole usluga i mreže,
- međusobno povezivanje s drugim mrežama,
- prelaženje između pokretnih mreža (eng. roaming).
Različite jezgrene mreže nude različiti skup mogućnosti, pri čemu jezgrene mreže uključuju 3GPP CN, ETSI TISPAN CN i 3GPP2 CN, ali nisu ograničene isključivo na njih.

» Mogućnosti M2M usluga (eng. M2M Service Capabilities) osiguravaju:
- M2M funkcionalnosti koje dijele različite aplikacije,
- ponudu funkcionalnosti kroz niz otvorenih sučelja,
- korištenje funkcionalnosti jezgrene mreže,
- pojednostavljenje i optimizaciju razvoja aplikacija te implementaciju skrivanjem nekih specifičnosti komunikacijske mreže.

» M2M aplikacije koje pokreću logiku pružanih usluga i koriste mogućnosti usluge koje su dostupne putem otvorenog sučelja.

» Funkcije upravljanja mrežom koje se sastoje od svih funkcija potrebnih za upravljanje pristupne i jezgrene mreže, poput provizioniranja, nadzora, upravljanja kvarovima, itd.

» Funkcija upravljanja M2M komunikacijom sastoji se od svih funkcija potrebnih za upravljanje mogućnostima M2M usluga u mrežnoj domeni. Upravljanje M2M uređajima i pristupnicima koristi određene mogućnosti M2M usluge.

» Skup M2M upravljačkih funkcija za M2M usluge inicijalizacije (eng. Bootstrap) M2M uređaja i pristupnika. Ova funkcija se skraćeno naziva MSBF (M2M Service Bootstrap Function), a ostvaruje se u odgovarajućem poslužitelju.

Domena uređaja i pristupnika sastoji se od sljedećih elemenata:

» M2M uređaja (engl. M2M devices),

» M2M pristupnika (engl. M2M gateway) te

» prostorne mreže umreženih uređaja (engl. M2M area network).

Aplikacije na uređajima koriste mogućnosti usluge i omogućuju samostalnu izmjenu podataka između njih.

Umreženi uređaji povezuju se na mrežnu domenu na dva različita načina: izravno ili putem pristupnika koji služi kao mrežni posrednik. Pristupnik također koristi mogućnosti usluge kako bi pokrenuo aplikacije i omogućio suradnju i povezivanje uređaja posredstvom komunikacijske mreže. Prostorna mreža umreženih uređaja, koja se često naziva i kapilarna mreža, povezuje pristupnik s uređajima koji se ne mogu izravno povezati na pristupnu mrežu.

2.1.2 Standardizacijske aktivnosti udruge 3GPP

Umreženi strojevi u okviru standarda udruge 3GPP označuju se kao MTC (Machine-Type Communication), a povezuju se preko MTC sučelja na odabranu infrastrukturu pokretne mreže (UTRAN, eUTRAN, GERAN itd.). Ona pruža transportne i komunikacijske usluge, uključujući uslugu prijenosa, višemedijskog IP podsustava (engl. IP Multimedia Subsystem, IMS) i slanja kratkih poruka (engl. Short Message Service, SMS), optimizirane za komunikaciju umreženih strojeva i poslužitelja, odnosno za međusobnu komunikaciju između umreženih strojeva. MTCu sučelje omogućuje umreženim strojevima pristup na mrežu i izmjenu prometa korisničke i kontrolne protokolne ravnine, a može se zasnivati na sučeljima raznih generacija pokretnih sustava, ovisno o tome koja se mreža koristi (Uu, Um, Ww i LTE-Uu). Slična je situacija i s preostala dva sučelja. Poslužitelji koriste MTCi sučelje (može se bazirati na sučeljima Gi, Sgi, i Wi) kako bi pristupali umreženim strojevima koristeći usluge prijenosa i IMS-a, odnosno MTCsms za pristup putem usluge 3GPP SMS (Slika 2-2) [5].

Slika 2-2: 3GPP M2M mrežna arhitektura

Razlikujemo dva temeljna komunikacijska scenarija koja uključuju umrežene uređaje i poslužitelje [4]. U prvom scenariju umreženi uređaji komuniciraju s jednim ili više MTC poslužitelja koji mogu biti smješteni u domeni operatora ili izvan nje. Drugi scenarij predviđa izravnu komunikaciju između umreženih uređaja, bez posredovanja poslužitelja. Potonji scenarij nije u okviru postojećih standarda detaljno razrađen, a razlog tome je pretpostavka kako se većina primjena može svesti na scenarije koji uključuju poslužitelje. Međutim, drugi scenarij u sebi krije alternativan pogled na umreženi sustav te potencijal za poboljšanje mnogih područja primjene i namjena, uključujući kvalitetnije upravljanje sustavom i razmjenom informacija.

3 Ericssonov koncept arhitekture M2M komunikacija

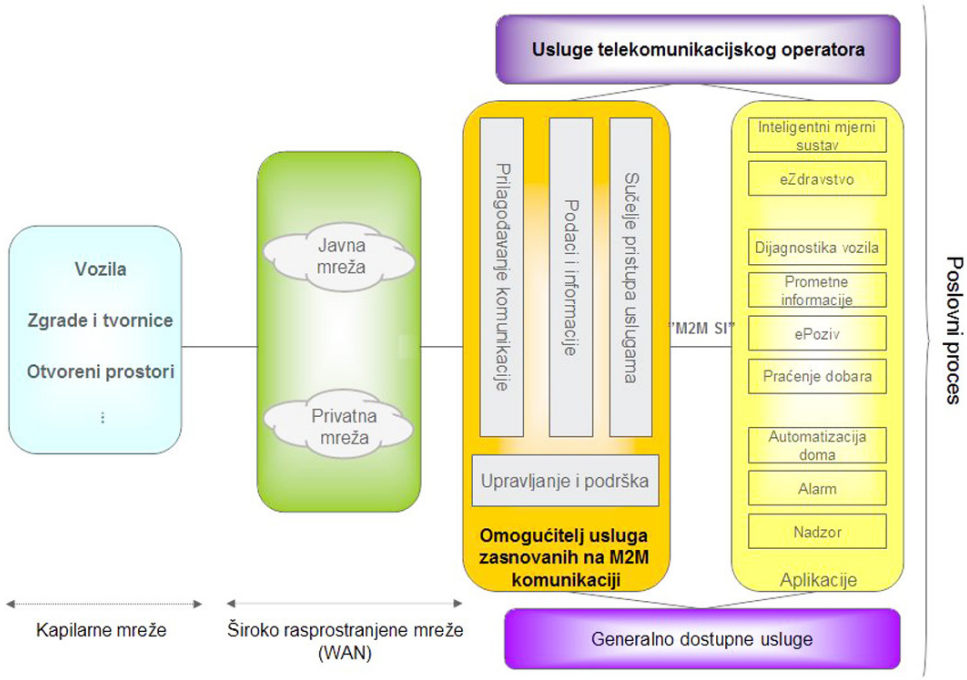
M2M arhitektura koja je tema ovog članka biti će u narednom tekstu opisana na način koji čitatelju jasno objašnjava komponente arhitekture kao i mogućnosti koje arhitektura pruža različitim aplikacijama. Aplikacije su namjenjene raznim područjima u industriji, društvu i gospodarstvu kao što su npr. komunalna služba, zdravstvo, transport itd.

Budući sa pojedini dijelovi arhitekture još nisu do kraja standardizirani, važno je napomenuti da ova arhitektura nije konačna već prikazuje osnovnu M2M arhitekturu kako je vidi Ericsson u ovom trenutku.

Također treba istaknuti nekoliko osnovnih pretpostavki ili ciljeva koji uvjetuju izgled M2M arhitekture:

- M2M arhitektura je horizontalna, slojevita arhitektura s istaknutim ključnim sučeljima kao i zajedničkim funkcionalnostima koje koriste vertikalne aplikacije.
- M2M arhitektura omogućuje implementaciju više aplikacija i više korisnika povrh jednog M2M sustava održavajući pritom principe sigurnosti i integriteta.
- Komunikacijske usluge i podatkovne/informacijske usluge podjeljene su u dvije zasebne logičke cjeline što znači da se M2M sustav može implementirati u postojeću komunikacijsku infrastrukturu s minimalnim ili nikakvim promjenama na postojećoj infrastrukturi. Sloj za komunikacijske usluge služi omogućavanju komunikacije između krajnjih M2M uređaja, čvorova u sloju omogućavanja usluga i aplikacija.
- Odvojeno od komunikacijskih usluga postoji funkcionalnost koja je zadužena za obradu aplikacijskih podataka. Dakle, funkcionalnosti koje se odnose na podatke i informacije (od strane senzora i aktuatora) logički su odvojene na M2M podatke i informacijski sloj koji se nalazi povrh sloja za komunikacijske usluge.
- Pretpostavka je da su M2M krajnji uređaji povezani IP baziranim protokolom barem do prvog prijenosnika, ako ne i čitavim putem do M2M platforme.
- Arhitektura, osim IP baziranih komunikacijskih tehnologija, kroz sučelja za međudjelovanje (koja se nalaze na nekoliko razina u arhitekturi) podržava i druge komunikacijske tehnologije (starije tehnologije ili protokol nekog proizvođača). Sučelja za međudjelovanje definirana su prema M2M krajnjim uređajima, na sloju omogućavanja usluga kao i na aplikativnom sloju.
- Na senzorske podatke kao zadatke aktuatora gleda se kao da su usluge. Fokus nije na samom senzoru ili senzorskom čvoru, već na usluzi koju omogućuje.
- M2M podatkovni i informacijski logički sloj zadužen je za obradu podataka, informacija i usluga koje šalju senzori i aktuatori. Senzorski podaci se na ovom sloju mogu ukloniti, izdvojiti ili sumirati.
- Radi postojanja nekoliko standarda kao i starih tehnologija ili tehnologija svojstvenih nekom proizvođaču, u arhitekturi je podržana je harmonizacija različitih senzorskih i aktuatorskih usluga.
- Arhitektura omogućuje priključak „plug-and-play“ (automatsko prepoznavanje, autentifikacija i objava) krajnjih M2M uređaja.
- Na M2M sloju za omogućavanje usluga definirano je standardno sučelje za razvoj aplikacija, eng. API (Application Programming Interface) preko kojeg se pojednostavljuje integracija s raznim korisničkim aplikacijama.

Cjelokupnu arhitekturu i glavne sastavne blokove prikazuje slika 3-1. Valja istaknuti da je u arhitekturi ključna nova funkcionalnost omogućavanja usluga zasnovanih na M2M komunikaciji (M2M Service Enablement) koja će se u daljnjem tekstu spominjati i kao M2M SE i uloga vanjskih usluga treće strane.



Slika 3-1: Ericsson M2M arhitektura

Slojevi u perspektivi, koje prikazuje slika 3-1, su sljedeći:

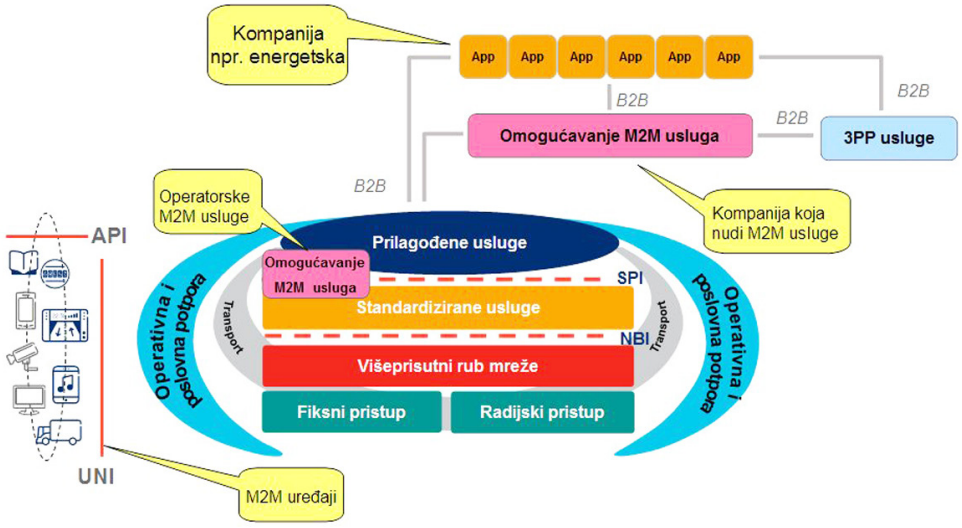
- kapilarne mreže,
- široko rasprostranjene mreže (WAN),
- omogućavanje usluga zasnovanih na M2M komunikaciji (M2M SE) te
- aplikacije.

Dodatno nad ovim dijelovima M2M arhitekture stoji i relacija između postojećih usluga telekomunikacijskih operatora i široko dostupnih usluga omogućenih od treće strane. Usluge koje nudi operator koriste se ili direktno od strane M2M SE (primjer: lokacijske usluge) ili od strane M2M aplikacija (primjer: događaj koji pokreće postavljenu sesiju prema nadzornoj kameri povezanoj na mrežu).

Sa stajališta operatorske mrežne arhitekture, M2M komunikacija ima arhitekturne i poslovne zahtjeve koji nadilaze tradicionalne telekomunikacijske mreže.

Tipična poslovna sučelja između različitih uloga podržavaju i koriste različite usluge i time izgrađuju potpunu M2M ponudu.

Kako se M2M arhitektuta tipično uklapa u mrežu operatora prikazano je na slici 3-2.



Slika 3-2: M2M u mrežnoj arhitekturi

Slika 3-2 M2M prikazuje nekoliko različitih načina kako kompanije ili operatori mogu nuditi M2M usluge. Telekom operator može primjerice dodati M2M SE u svoj protfelj usluga. Drugi način je kompanija koja nudi M2M SE „u oblaku“ (eng. cloud based) koji može udomaćiti nekoliko različitih M2M aplikacija. Konačno, kompanija može nuditi komplet M2M usluga u ulozi posrednika.

3.1 Aplikacije i poslovni procesi

M2M aplikacije primjenjive su u mnogo segmenata industrije i mogu biti prilično različite. Tipične aplikacijske domene su automatizacija u industriji, transport i logistika, upravljanje sredstvima, komunalne službe i zdravstvo. Dodatno se, zbog naglog porasta broja potrošačke elektronike s ugrađenom mogućnošću povezivanja i uslugama, može i potrošačka elektronika smatrati kao aplikacijska domena. Ona je ujedno najnoviji i najbrže rastući segment globalnog bežičnog M2M tržišta. Primjeri potrošačke elektronike kao što su električni čitači knjiga (eng. e-reader), izvođači mp3 datoteka i digitalni foto okviri imaju praktično iste karakteristike kao i tradicionalni uređaji za M2M komunikaciju iako svojim izgledom sliče pametnim telefonima. Zbog takvih karakteristika, potrošačka elektronika je svrstana u novu kategoriju umreženih uređaja. Prema procjenama raznih istraživačkih kuća, broj umreženih uređaja potrošačke elektronike bi trebao doseći brojku od 4 milijarde do 2020. godine. Umreženost uređaja će odigrati značajnu ulogu u penetraciji, ali i porastu generiranog prometa korištenjem potrošačke elektronike.

M2M skup mogućnosti je generalno integiran u poslovne procese kompanije. Neke od tih mogućnosti se koriste zasebno npr. sakupljanje očitanja brojila, dok su druge više uvezane sa poslovnim procesima, npr. alarm ili događaj koji zahtjeva slanje ekipe koja ima dostatne informacije o događaju. U nekom slučaju je potrebna i uspostava multimedijalne veze između ekipe i središnjice. Za uspostavu multimedijalne veze može se koristiti IP Multimedijski Podsustav (IMS) ili usluga za poručivanje kao SMS ili e-pošta.

Za neke M2M aplikacije potrebne su informacije ili usluge nekih drugih sustava kao što su npr. zemljopisne baze ili mape.

Ako M2M aplikacije gledamo sa stajališta poslovnih procesa i potrebe integracije s drugim sustavima, jasno je da se one moraju realizirati s tri grupe usluga:

- M2M omogućavanje usluga (M2M SE),
- usluge telekom operatora i
- generalno dostupne usluge.

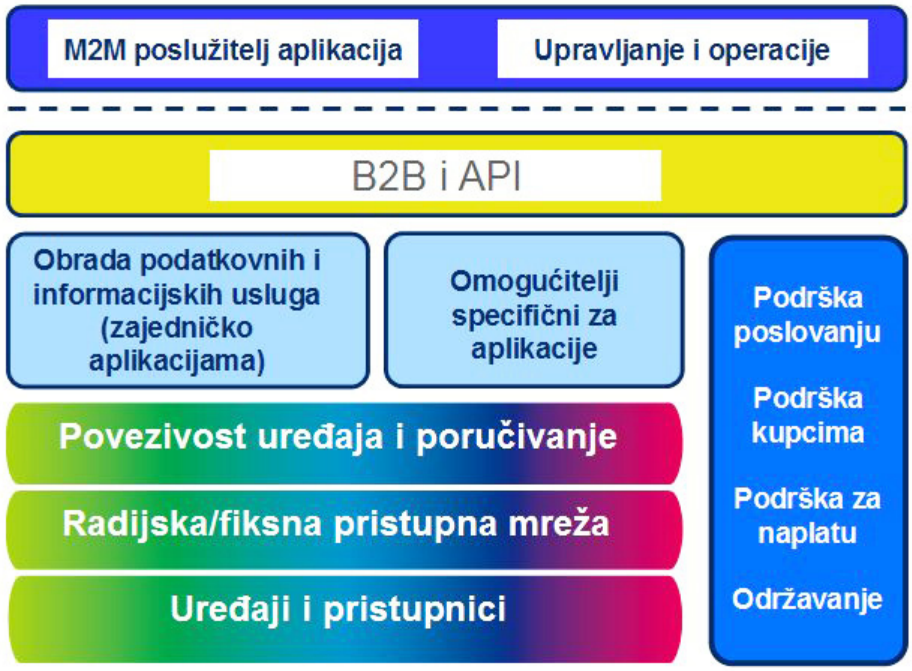
3.2 Omogućavanje usluga zasnovanih na M2M komunikaciji

Funkcionalnost omogućavanja M2M usluga podrazumijeva prikupljanje, pohranu i obradu podataka i informacija koje šalju različiti M2M uređaji specifičnih primjena, a koje potom obrađuju M2M aplikacije.

Svrha omogućavanja M2M usluga je razdvajanje jezgre aplikacija i funkcija koje su za mnoge aplikacije zajedničke te postavljanje tih zajedničkih funkcija kao zajedničke usluge.

Omogućavanje M2M usluga se nadalje oslanja na odvajanje temeljnih komunikacijskih usluga od jezgrenih informacija i podatkovno orijentiranih usluga. Odvajanje je uzrokovano činjenicom da je M2M komunikacija orijentirana uslugama i informacijama a ne uređajima. Kao takve, komunikacijske usluge mogu biti osigurane kroz web temeljenu (Web Services/REST) ili neku sličnu arhitekturu. Zaključak je da sredstvo komunikacije treba biti transparentno za podatkovno i uslužno orijentirane usluge kao i za M2M aplikacije. Ova činjenica ima utjecaj na imenovanje i adresiranje u smislu da je za usluge senzora i aktuatora potrebno zasebno imenovanje i adresiranje od onog koje se koristi za komunikacijske usluge.

Slika 3-3 prikazuje funkcionalne blokove u sloju za omogućavanje M2M usluga.



Slika 3-3: Funkcionalni blokovi - omogućavanje M2M usluga

Omogućavanje M2M usluga možemo podijeliti u četiri glavne funkcijske domene:

- **Povezivost uređaja i poručivanje:**
  Domena obuhvaća istovrsan pristup M2M uređajima neovisno o komunikacijskom mehanizmu (pretpostavlja se da se radi o IP protokolu). Izvršava potrebne prilagodbe prema različitim komunikacijskim uslugama i podržava adresiranje uređaja i usluga na temelju URI adresiranja. Može obuhvaćati i sakupljanje podataka od M2M uređaja prema zahtjevu ili rasporedu. Pod rasporedom podrazumijevaqmo push i pull podataka.
- **Podatkovne i informacijske usluge:**
  Domena obuhvaća podatkovno orijentiranu obradu kao što je kreiranje algoritama za programiran prihvat podataka, pohranu i čuvanje podataka i održavanje različitih usluga direktorija. Domena također obuhvaća i kompoziciju usluga poput agregacije senzorskih podataka na razinu veće apstrakcije informacija ili kontrolu grupe senzora i aktuatora kao automatiziranu uslugu. Pravila za kontroliranje pristupa informacijama i uslugama su također uključena u ovu domenu.
- **B2B pristup uslugama:**
  Domena obuhvaća pristup M2M uslugama i aplikacijama kroz uglavnom standardizirana ili otvorena sučelja (API). Tipično se radi o web temeljenim (Web Services ili REST) B2B sučeljima. Domena je zadužena i za kontrolu pristupa i provedbu pravila na zahtjev usluga kao i za obračunavanje (eng. accounting) u svrhu praćenja prometa.
- **Podrška poslovanju i operacijama:**
  Domena obuhvaća automatsko uključenje i pokretanje (eng. plug-and-play) uređaja i udaljeno upravljanje uređajima. Može se proširiti i funkcionalnostima za obradu prihoda specifičnim za M2M, osiguravanjem ugovora o razini kvalitete pružanja usluga (eng. Service Level Agreement, SLA), dijagnostikom uređaja itd. Ovaj skup funkcionalnosti obuhvaća i nove funkcionalnosti te iskorištavanje postojećih funkcionalnosti kao što je npr. omogućavanje krajnjim korisnicima i pružateljima usluga administriranje uređaja i pratećih usluga.

Gore navedene funkcijske domene mogu se paketirati na razne načine ovisno o potrebnom paketu usluga, kao što je npr. platforma za upravljanje uređajima, platforma za prihvat podataka ili posredovanje upravljanjem usluga. Fleksibilnost paketiranja je nužna kako bi se omogućilo pravilno adresiranje nezrelog, ali s druge strane brzo nadolazećeg tržišta M2M usluga.

3.3 M2M pristupnik

M2M pristupnik je poseban tip M2M uređaja koji povezuje zasebno implementirane senzore i aktuatore prema WAN mreži. Senzori i aktuatori su, tipično, jednostavni uređaji niske cijene a s mogućnošću lokalnog umrežavanja. Senzorski i aktuatorski čvorovi se obično implementiraju na fizički malom prostoru npr. blok kuća, unutar zgrade, automobila ili čak na ljudsko tijelo.

M2M pristupnik može imati više ili manje napredne mogućnosti, a osnovne funkcije koje mora podržavati su:

- terminacija protokola, konverzija i međudjelovanje protokola na fizičkom, podatkovnom, mrežnom sloju,
- mapiranje identiteta, npr. rješavanje zahtjeva za uslugom prema određenom senzorskom čvoru,
- transformacija informacija i podataka iz specifičnog u jedinstveni format,
- agregacija podataka, npr. podaci s nekoliko izvora u jedan informacijski objekt,
- privremeno spremanje podataka,
- kontrola pristupa, određivanje rasporeda interakcije senzorskih čvorova te
- osnovne funkcionalnosti upravljanja pristupnikom (udaljeni pristup, mogućnost nadogradnje softvera, podrška za priključak na sustav za podršku).

3.4 Usluge telekom operatora

Telekomunikacijske mreže pružaju set usluga koje su u izravnoj vezi sa M2M uslugama ili su pak potrebne za integraciju aplikacija u M2M orjentirane usluge. Za integraciju su potrebna aplikacijska sučelja preko kojih se prosljeđuju zahtjevi, npr. SOAP/XML ili web bazirano sučelje. Primjeri su i lokacijske usluge, multimedijalne usluge ili usluge poručivanja.

3.5 Generalno dostupne usluge

Mnoge M2M SE funkcionalnosti za rad trebaju usluge koje su generalno dostupne preko partnera. Primjeri takvih usluga su društvene ili profesionalne mreže, meteorološke usluge, usluge podržane rezolucije, usluge globalnog pozicioniranja itd.

3.6 Kapilarna mreža

Kapilarna mreža je skupni naziv za senzore i aktuatore koji su položeni u mrežu i kojima se pristupa preko WAN mreže. Pristup je moguće ostvariti preko pristupnika (Gateway) ili M2M modula. M2M uređaji također mogu u zadnjem koraku biti povezani na lokalnu mrežu koja se naziva Last Drop. Takva mreža ima transportno orijentirani mrežni čvor (Hub) koji omogućava koncentraciju prometa. Kapilarna mreža je heterogena i za komunikaciju se oslanja na bežične protokole kao što su ZigBee, Bluetooth te žične poput PLC-a. Pristupnik omogućava i međusobnu komunikaciju i medijaciju lokalnih usluga stvarajući prepoznatljiv format prema aplikacijskoj strani.

Implementacija kapilarnih mreža obuhvaća zgrade, automobile, otvorene prostore, pa čak i sama ljudska tijela. Pristupnik može biti rezidencijalni, poslovni, otvoreni prostor, automobil ili mobilni telefon.

Postoje dva posebna slučaja korisnički orijentirane opreme. To su mobilni uređaji i korisnički elektronički uređaji posebne namjene. Mobilni uređaji imaju dvije glavne uloge: pristupnik prema senzorima i aktuatorima te ulogu aplikacijskog sučelja za interakciju između korisnika i lokalnih ili udaljenih senzora i aktuatora. Različite uloge zauzimaju različito mjesto u arhitekturi. Korisnički elektronički uređaj je sličan M2M uređaju budući da radi automatski, bez potrebe za nadzorom – korisnik obično ne treba biti uključen u proces omogućavanja veze ili podešavanja specifičnih parametara uređaja i paketa usluga.

3.6.1 Bežična tehnologija kratkog dometa

Bežična tehnologija kratkog dometa (Short-Reach Wireless Technology - SRWT) postaje sve popularnija za sveprisutno povezivanje različitih instrumentacija, nadzora i mjernih sustava putem bežične mreže senzora i

aktuatora (Wireless Sensor and Actor Networks – WSAN). U kontekstu M2M komunikacije SRWT ima ključnu ulogu za komunikaciju M2M uređaja bez ili s vrlo malo dodatnog ljudskog podešavanja. Uređaji s takvom komunikacijom će se proširiti u raznim okruženjima s različitim aplikacijama i tako nuditi velike mogućnosti poput detektiranja sigurnosti u kući, kontrole osvjetljenja, nadziranja zdravstvenih uvjeta i drugo. To su samo neki od brojnih izazova u razvoju M2M mreža.

Različite bežične tehnologije prijenosa za M2M mreže i njihove funkcionalnosti prikazani su u tablici 4. IEEE 802.15.4 temeljeni protokoli, kao što su 6LoWPAN i ZigBee, pogodni su za osobne mreže s malom propusnošću, manjim dometom i malom potrošnom energije. Ovakvi komunikacijski protokoli nastali su kao potreba za umrežavanjem velikog broja uređaja između kojih se prenosi mala količina podataka, a aplikacije zahtijevaju veliku energetsku autonomiju uređaja. Tipični primjeri aplikacija s ovakvim zahtjevima su bežične mreže senzora, kontrolne mreže, prikupljanje medicinskih podataka i slično. Uređaji bi trebali biti maleni, jeftini i pouzdani. S druge strane IEEE 802.11 (Wi-Fi) protokol je primjereniji za aplikacije koje zahtijevaju podršku za veće udaljenosti i veće podatkovne brzine, uključujući aplikacije za audio i video streaming. Bluetooth je pak pogodan za komunikaciju ravnopravnih subjekata (peer-to-peer) kraćeg dometa i niže propusnosti.

	802.15.4 (ZigBee/6LoWPAN)	Bluetooth i Bluetooth low energy (LE)	802.11 (Wi-Fi)
Maks. brzina prijenosa	250kb/s	3Mb/s (enhanced) 1Mb/s (basic or LE)	22Mb/s (802.11 g) 144Mb/s (802.11 n)
Doseg (unutrašnji)	10-20m	klase od 1m, 10m i 100m	45m
Snaga	Niska	Srednje niska (LE)	Visoka
Vijek trajanja baterije	Godine	Dani, godine (LE)	Sati
Frekvencijski pojas	2,4GHz, 868MHz i 915MHZ	2,4GHz	2,4GHz, 3,6GHz i 5GHz
Pristupa kanalima	CSMA/CA (non beacon based) ili superframe struktura (beacon based, non-contention)	Preskakivanje frekvencija ili CSMA/CA	CSMA/CA
Aplikacije	Pametni aparati Inteligentni mjerni sustavi Kontrola osvjetljenja Sigurnost u domu Automatizacija u uredu	Glasovne aplikacije Inteligentni mjerni sustavi Prijenos podataka Kontrola igara Nadziranje u zdravstvu (LE) Računalna periferija (LE)	Umrežavanje između WAN mreže i korisnika M2M mreže Digitalni zvuk

Tablica 3-1. Pregled M2M bežičnih mreža kratkog dometa

3.7 Široko rasprostranjena mreža (WAN)

Svrha široko rasprostranjene mreže (Wide Area Network – WAN) je omogućavanje komunikacije između M2M funkcija koje omogućavaju usluge i krajnjih WAN točaka. Pod terminom WAN krajnja točka podrazumijeva se komunikacija koja završava na pristupniku ili u podatkovnom centru koji je domaćin M2M funkcijama koje omogućavaju usluge.

WAN mreža ne uključuje same M2M krajnje točke već omogućava komunikaciju s određenim senzorskim čvorom.

WAN mreža pokriva licenciran i nelicenciran spektar koristeći bežične ili žičano bazirane pristupne tehnologije: DSL, WiMax, WiFi, Ethernet itd. Prometni modeli za M2M komunikaciju razlikuju se prema namjeni za koju su postojeće mreže dizajnirane i mogu se značajno razlikovati. Ne postoji jedinstven M2M prometni model već svi modeli ovise o aplikaciji. Različite prometne karakteristike mogu indicirati da su za primjenu M2M aplikacije potrebna poboljšanja i optimizacije u postojećim RAN i CN mrežama i procedurama.

Funkcijski, WAN uključuje navedene karakteristike:

- Glavna funkcija WAN mreže je uspostava povezivosti između kapilarnih mreža, domaćina senzora i aktuatora s M2M funkcijama za omogućavanje usluga. Standardni komunikacijski model je paketski i temelji se na TCP/IP protokolu.
- Prihvat ili isporuka različitih tipova paketa poput SMS poruka poslana od strane senzora.

» Upravljanje identitetima (primarnih uređaja), ćelijskih i ne-ćelijskih domena koji se uglavnom koristi kako bi se dozvolio pristup WAN resursu a obuhvaća:
  - MCIM (Machine Communications Identity Module) – modul za udaljeno provizioniranje pretplatničkih podataka,
  - SIM (Subscription Identity Module) – modul za identifikaciju pretplatnika,
  - MAC (drugi tip identiteta za uređaje koji nisu ćelijski),
  - funkcije tipa autentikacije/registracije (orijentirane na uređaje),
  - usluge direktorija (orijentirane na uređaje tipa LDAP),
  - usluge pretplate (orijentirane na uređaje) te
  - razne probe koje omogućuju mjerenja.

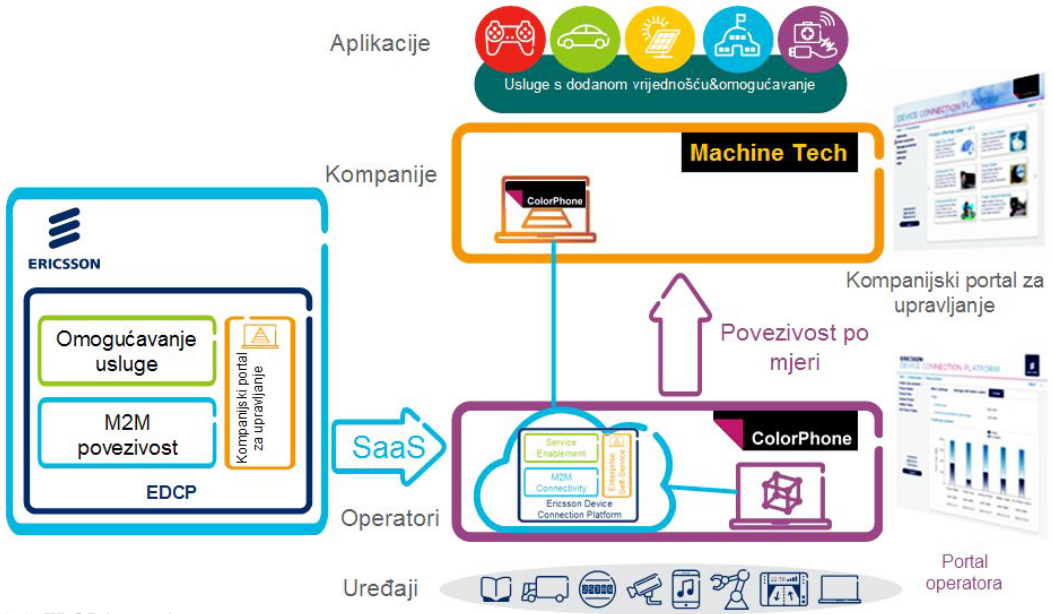
Područje WAN mreža trenutačno prolazi kroz proces modernizacije, tj. prelazi u potpunosti na All-IP tehnologije. Jedno od rješenja za WAN mreže je Multimedijski podsustav zasnovan na Internet protokolu (IP Multimedija Subsystem – IMS) koji može biti pogodan za M2M aplikacije.

IMS omogućava mnoge komunikacijske usluge potrebne za implementaciju M2M usluga kao i neke funkcionalnosti za isporuku usluga. Funkcionalnosti za isporuku usluga su posredovanje upravljanjem uslugama, usluge registracije tj. općenito kompozicija usluga. IMS se može koristiti za omogućavanje komunikacijskih usluga prema ili od infrastrukture M2M funkcija za omogućavanje usluga. IMS može služiti za komunikaciju prema kapilarnim mrežama i prema aplikacijskim serverima. Neke M2M aplikacije mogu iskoristiti postojeće IMS funkcionalnosti kao što su adresiranje, osiguravanje sigurnosti, autentifikacija, osiguravanje kvalitete usluge (eng. Quality of Services,QoS), prioritiziranje prometa, poručivanje, upravljanje grupama, informacije o prisutnosti, NAT traversal, prevođenje IPv4/IPv6 adresa i izvještavanje o događajima. M2M specifična logika može se protumačiti kao aplikacija koja radi povrh IMS arhitekture. Važno je napomenuti da je M2M specifičnoj logici potrebno dopustiti pristup IMS sustavu preko standardiziranog NBI (eng. Northbound) sučelja.

4 Ericssonova platforma za M2M komunikaciju

Ericssonova platforma za M2M komunikaciju EDCP (Ericsson Device Connection Platform) je ključna komponenta cjelokupnog vrijednosnog lanca za M2M komunikacije i ostvarenja vizije 50 milijardi povezanih uređaja. EDCP omogućuje operatorima pokretne mreže i kompanijama ulazak na M2M tržište na troškovno učinkovit način.

Ericsson nudi EDCP platformu kroz poslovni model SaaS (eng. Software as a Service) u kojem je operatorima pokretne mreže i kompanijama pružena mogućnost uporabe dostupnih usluga na platformi EDCP , a smještena je u infrastrukturi oblaka (eng. Cloud). Usluge podržane EDCP platformom dostupne su operatoru ili kompanijama kroz portale i otvorena sučelja. Pod uslugama se ovdje misli na promet, upravljanje pretplatama i nadgledanje uređaja. Slika 4-1 prikazuje koncept EDCP platforme kao usluge.



Slika 4-1: EDCP kao usluga

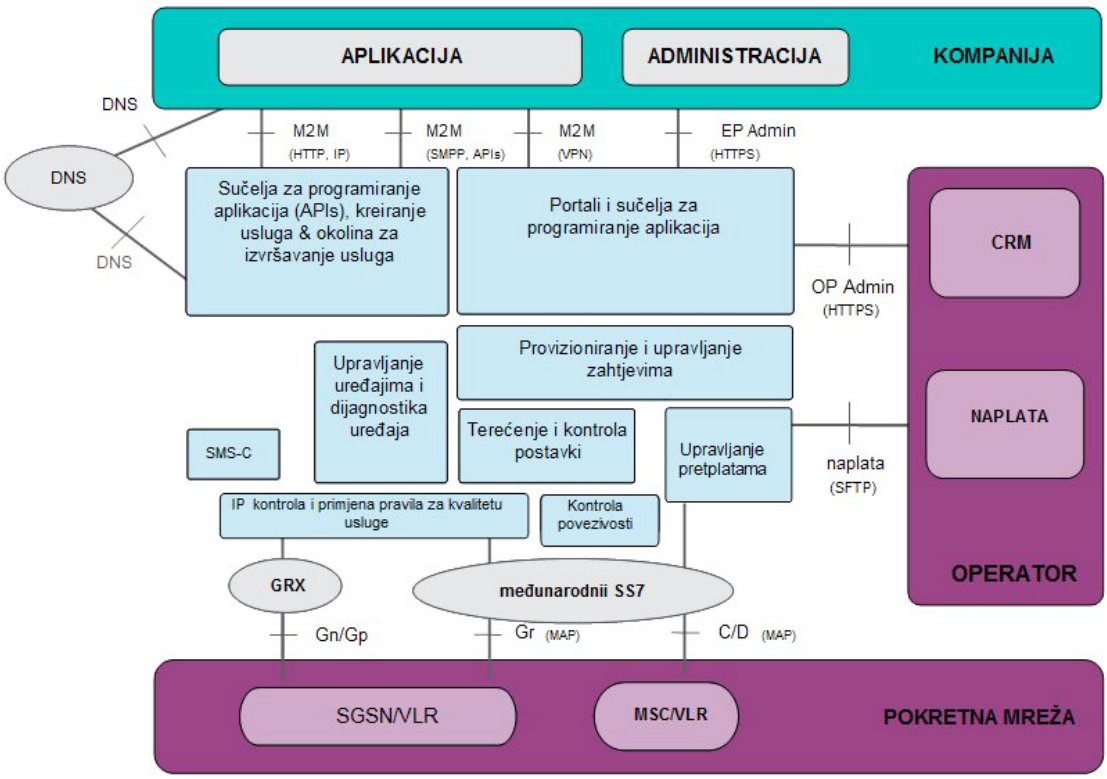
Kroz uslugu koja im se iznajmljuje (eng. hosted service) na vremenskoj bazi, godišnje, mjesečno, kvartalno ili sl. operatori i kompanije imaju mogućnost:

- praćenja sustava i nadogradnje sustava,
- podrške i pomoći oko platforme 24/7,
- pristupa alatima za kreiranje i provizioniranje usluga,
- pristupa upravljanju zahtjevima za uslugama,
- pristupa upravljanju incidentima,
- pregleda standardnih statističkih podataka i standardnog nadgledanja platforme te
- zahtjeva za hitnim intervencijama.

Razlikujemo dva različita načina nuđenja M2M usluge kompanijama:

- Povezivost za M2M promet (GPRS, SMS, glasovna komunikacija i promet u mrežama komutacije kanala), gdje glasovna komunikacija i promet u mrežama komutacije kananala nisu dio EDCP platfome već su realizirane od strane mreže operatera. EDCP može obavljati funkcionalnosti autentifikacije i autorizacije SIM-ova. Nadalje, EDCP može obavljati i funkcionalnosti tarifiranja, terećenja i poslovne logike koristeći podatke za naplatu koji dolaze iz mreže sa komutacijom kanala (eng. Transferred Account Procedure, TAP podaci).
- Usluge za podršku poslovanju koje uključuju npr. administriranje i upravljanje kompanijom, EDCP pretplatama, rasponima brojeva dodjeljenim kompaniji, pretplatničkim paketima i modelima naplate.

EDCP se integrira u mrežnu okolinu kompanije ili operatora preko vanjskih sučelja (Slika 4-2).



Slika 4-2: EDCP vanjska sučelja

Kako bi se osigurala sigurna komunikacija između Ericssona i operatora ili kompanije potrebno je razmjeniti informacije o IP adresama, portovima i postavkama za pristupanje platformi te konfigurirati vatrozide (eng. firewalls) koji se nalaze između operatora, kompanije i Ericssona. Virtualna privatna veza (eng. Virtual Private Network, VPN) može se korisiti za siguran pristup nekoliko sučelja.

Operator i Ericsson povezuju se preko standardiziranih vanjskih sučelja:

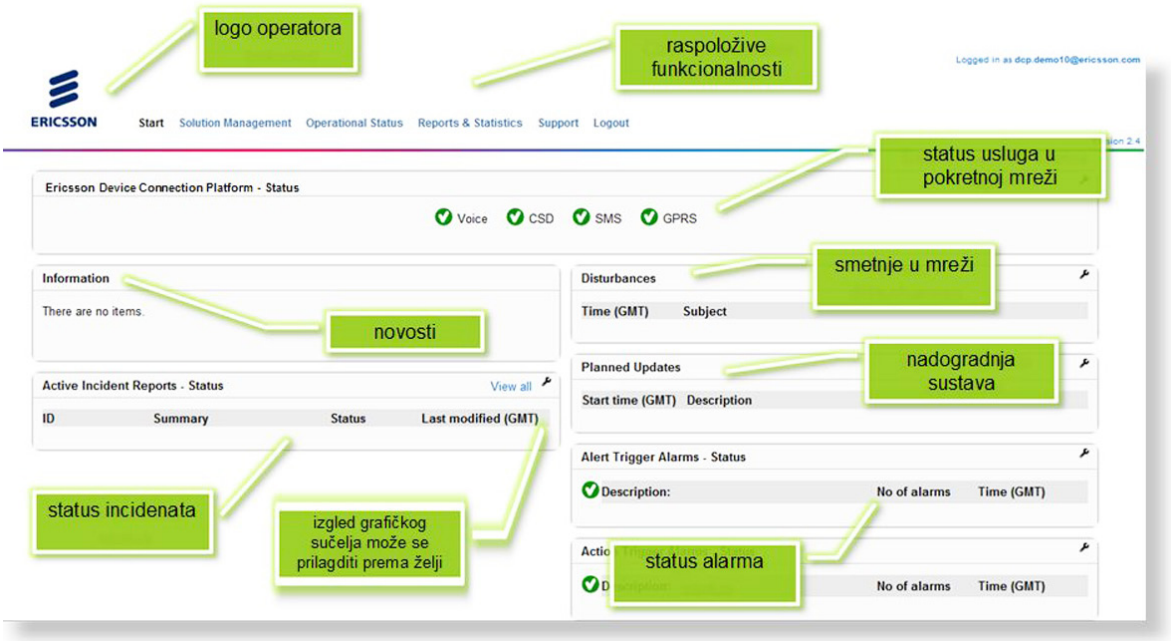
- Preko OP Admin sučelja operatoru je omogućeno upravljanje kompanijama, kontaktima, pretplatničkim paketima kao i rasponima brojeva pridjeljenim kompanijama.

» IT sučelje služi za prijenos podataka za naplatu koje generira platforma, kao i za prijenos podataka za naplatu iz mreže s komutacijom kanala koji služe kako bi se naplatilo korištenje npr. glasovne komunikacije. Sučelje prema IT lokaciji služi i za prijenos SNMP (Simple Network Management Protocol) podataka prema operatoru.

» Povezivanje na pokretne mobilne mreže operatora, 2.5G ili 3G radi se preko Gn/Gp, Gr i C/D sučelja.

Kompanija i Ericsson povezuju se također preko standardiziranih vanjskih sučelja gdje se odvija pretvorba IP adresa u imena servera, upravljanje pretplatama i SIM-ovima, pristupanje podacima o radu u nekom proteklom vremenskom periodu, pristupanje podacima o statusu sustava te povezivanje krajnjih M2M korisničkih uređaja s aplikacijom.

Primjer izgleda grafičkog sučelja prikazujeslika 4-3.

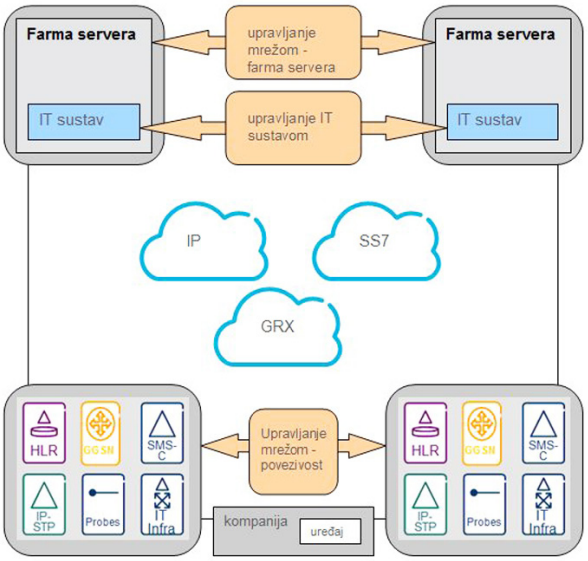


Slika 4-3: EDCP grafičko sučelje

U trenutnoj reviziji produkta, realizacija platforme napravljena je na geo-redundantan način i sastoji se četiri glavne lokacije (Slika 4-4):

» Dvije geo-redundantne lokacije za IT sustav (upravljanje uslugama, naplata i terećenje, izvješća i web portali), obije smještene u Švedskoj.

» Dvije geo-redundantne lokacije koje obavljaju funkcionalnosti osnovnih telekomunikacijskih usluga (HLR, GGSN i SMSC) od kojih se jedna nalazi u Nizozemskoj, a druga u Švedskoj.



Slika 4-4: EDCP lokacije

Danas su prisutna dva dominantna poslovna modela pružanja platforme za M2M komunikaciju. Dok je prvi model temeljen na izgradnji vlastite platforme ili akviziciji platforme u obliku proizvoda, drugi model je zasnovan na plaćanju korištenja tuđe platforme pružane u obliku usluge. U slučaju poslovnog modela temeljenog na vlastitoj platformi, platforma će biti sastavni dio IT-a operatora. No u slučaju alternativnog poslovnog modela, platforma za M2M komunikaciju će biti sastavni dio IT-a kompanije koja pruža uslugu korištenja platforme.

Poslovni model koji podrazumijeva izgradnju vlastite platforme za M2M komunikaciju će osigurati operatoru veću kontrolu nad samom platformom, njenim funkcionalnostima i daljnjim razvojem. Cijena takve kontrole će biti dugo vrijeme razvoja i troškovi razvoja vlastite platforme ili dugotrajan i skup postupak nabavke platforme te veliki troškovi upravljanja životnim tijekom sustava koji će uključivati, prije svega, i napore za standardizaciju platforme kako odgovarajuće norme i njihove izmjene budu usvajane. S druge strane, poslovni model zasnovan na najmu platforme će pružati operatoru manju kontrolu nad samim životnim tijekom platforme, ali će u velikoj mjeri velike kapitalne troškove uspostave M2M infrastrukture zamijeniti mnogo nižim operativnim troškovima te u velikoj mjeri smanjiti vrijeme uvođenja platforme za M2M komunikaciju u organizaciju. Rizik od lošeg upravljanja životnim tijekom platforme, od strane njenog vlasnika, smanjuje se pažljivim odabirom pouzdanih, iskusnih i provjerenih proizvođača.

Odabir poslovnog modela operatora svakako nije jednostavan i primjenjiv na sve. Oba poslovna modela mogu biti opravdana. Stoga će konačan odabir na kraju u velikoj mjeri biti uvjetovan strateškim opredjeljenjem i vlastitom vizijom pojedinog operatora kao jedinog ili jednog od više sudionika u transformiranom vrijednosnom lancu na tržištu M2M usluga.

5 Zaključak

Sa stajališta operatorske mrežne arhitekture, M2M komunikacija ima arhitekturne i poslovne zahtjeve koji nadilaze tradicionalne telekomunikacijske mreže.

Primijenjena M2M arhitektura temelji se na sustavu koji je horizontalno položen međutim cijeli koncept je dosta nov i u sljedećem će razdoblju doživljavati brojna prilagođavanja.

Ericsson Device Connection Platform – EDCP je važan korak prema realizaciji vizije 50 milijardi umreženih uređaja. EDCP omogućuje operatorima i kompanijama, kroz alate za upravljanje M2M platformom, pretplatama i uslugama, ulazak na M2M tržište putem raznolikih M2M aplikacija koje mogu egzistirati povrh EDCP platforme.

Ericsson vidi EDCP platformu kao idealan način kako operator može ući na sve brže rastuće M2M tržište s minimalnim troškovima, minimalnim rizicima, a s druge strane, s mogućnošću proširenja prema poslovnim potrebama.

6 Literatura

[1] ETSI, TS 102 690 v 1.1.1, “Machine- to- Machine communications (M2M); Functional architecture”, October 2011.

[2] ETSI, TS 102 689 v 1.1.1, “Machine-to-Machine communications (M2M); M2M service requirements”, August 2010.

[3] ETSI, TS 102 921 v 1.1.1., “Machine-to-Machine communications (M2M); mIa, dIa and mId interfaces”, February 2012.

[4] “3GPP Technical Specification 22.368“, v11.3.0, 3GPP, 2011.

[5] “3GPP Technical Report 23.888“, v1.5.0, 3GPP, 2011.

[6] “3GPP Technical Report 33.812“, v9.2.0, 3GPP, 2010.

[7] “3GPP Technical Report 33.868“, v0.5.0, 3GPP, 2011.

[8] Berg Insigth, “The Global Wireless M2M Market”, M2M Research, 2012.

[9] M.Blockstrand, T.Holm, Lars-Orjan Kling, R.Skorg, B. Wallin, “Operator opportunities in the internet of things”, Ericsson Review, No.1, 2011.

[10] Ericsson White Paper, “More than 50 billions connected devices”, February 2011.

[11] Ericsson White Paper, “Device connectivity unlocks value”, January 2011.

[12] M.Chen, J.Wan, F.Li, “Machine-to-Machine Communications: Architectures, Standards and Applications”, KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 6, NO. 2, Feb 2012.

[13] Beecham Research, “report from Research Study: M2M Service Enablement Services”, December 2011.

7 Popis kratica

3GPP	3rd Generation Partnership Project
API	Application Provider Interface
B2B	Business to Business
DPI	Deep Packet Inspection
DSL	Digital Subscriber Line
EDCP	Ericsson Device Connection Platform
ETSI	European Telecommunications Standards Institute
eUTRAN	Evolved UTRAN
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node

HRAN	High RAN
IEEE	Institute of Electrical and Electronics Engineers
IMS	IP Multimedia Subsystem
IoT	Internet of Things
IPv6	Internet Protocol version 6
LTE	Long Term Evolution
M2M	Machine-to-Machine
M2M SE	M2M Service Enablement
MAC	Media Access Control
MCIM	M2M communications identity module
MTC	Machine-Type Communication
NAT	Network Address Translation
NBI	Northbound Interface
OPEX	Operating Expenditure
OTT	Over - the - Top
PLC	Powerline Communication
REST	Representational State Transfer
QoE	Quality of Experience
QoS	Quality of Service
SE	Service Enablement
SGSN	Serving GPRS Support Node
SIM	Subscriber Identification Module
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOAP	Simple Object Access Protocol
SRWT	Short-Reach Wireless Technology
RAN	Radio access network
UTRAN	Universal Terrestrial Radio Access Network
VPN	Virtual Private Network
WAN	Wide area network
WCDMA	Wideband Code-division multiple access
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WSAN	Wireless Sensor and Actuator Networks
XML	Extensible Markup Language

Adrese autora:

Željko Popović
e-mail: zeljko.popovic@ericsson.com

Vanesa Čačković
e-mail: vanesa.cackovic@ericsson.com

Darijo Burjan
e-mail: darijo.burjan@ericsson.com

Ericsson Nikola Tesla d.d.
Krapinska 45
p.p. 93
HR-10002 Zagreb
Hrvatska

Uredništvo je primilo rukopis 15. svibnja 2012.

Mario Čagalj

Sveučilište u Splitu, FESB
University of Split, FESB

SIGURNOST U M2M (MACHINE-TO-MACHINE) KOMUNIKACIJAMA

M2M (MACHINE-TO-MACHINE) COMMUNICATIONS SECURITY

Sažetak

Osnovni cilj ovog rada je približiti problematiku sigurnosti u budućim *Machine-to-Machine* (M2M) komunikacijama. Karakter M2M komunikacija, veliki broj distribuiranih i izloženih M2M uređaja (50 milijardi do 2020.), potencijalno ograničenih resursa, predstavljaju posebne i složene sigurnosne izazove. U radu su prvo predstavljene najvažnije sigurnosne prijetnje u M2M sustavima. Zatim je dan pregled najvažnijih standardizacijskih aktivnosti alijanse 3GPP i standardizacijskog instituta ETSI, vezanih uz problematiku sigurnosti u M2M komunikacijama. Konačno, predstavljeno je nekoliko sigurnosnih mehanizama i protokola prilagođenih M2M komunikacijama koje je razvila istraživačka grupa autora članka, djelomično u suradnji i pod pokroviteljstvom Ericssona Nikole Tesle d.d. iz Zagreba.

Abstract

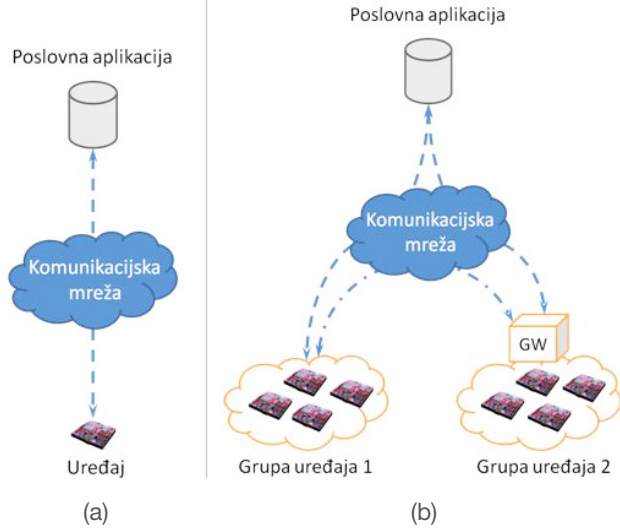
It is our goal in this paper to present some of the major security concerns and issues within the framework of Machine-to-Machine (M2M) communications. One of the key elements for a successful deployment and adoption of such systems is to ensure trustworthiness, authenticity, and privacy of data being communicated. The scale (Ericsson forecasts 50 billion connected M2M devices by 2020) and highly distributed nature of M2M systems present unprecedented challenges for security professionals. In this paper, we first present the most important security threats. Then we overview recent M2M security-related standardization activities by the 3GPP alliance and ETSI standardization institute. Finally, we present several security mechanisms and protocols appropriate for M2M systems, which have been developed within the author's group – in collaboration with and partially funded by Ericsson Nikola Tesla d.d., Zagreb.

KLJUČNE RIJEČI:	KEY WORDS:
Machine-to-Machine (M2M) komunikacije	Machine-to-Machine (M2M) communications
Machine Type Communication (MTC)	Machine Type Communication (MTC)
sigurnost	security
standardizacija	standardization activities
3GPP	3GPP
ETSI	ETSI

1 Uvod

Machine-to-Machine (M2M) komunikacije (ili *Machine Type Communications* - MTC) označavaju skup tehnologija koje omogućavaju razmjenu različitih tipova podataka između uređaja - sustava za automatska mjerenja (generalno „skrivenih“ od korisnika), prikupljanje i obradu mjerenih rezultata te ljudi kao korisnika prikupljenih informacija. Osnovna uloga M2M sustava je uspostava i osiguravanje uvjeta koji omogućavaju M2M uređaju dvosmjernu komunikaciju prema poslovnoj aplikaciji [1].Tipične M2M arhitekture prikazane su na slici 1.

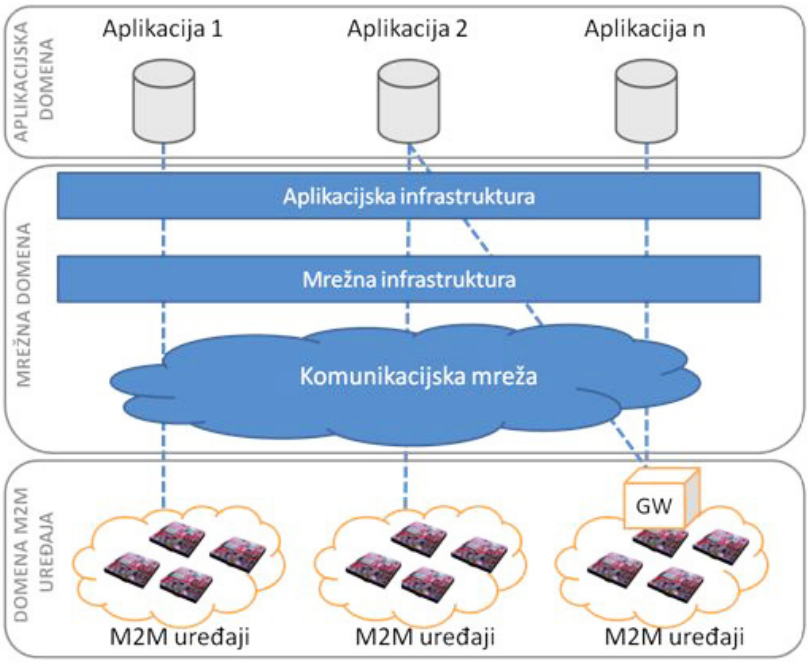
Na slici 1(a) prikazan je uređaj u M2M komunikaciji s odgovarajućom poslovnom aplikacijom. Nadzor i upravljanje razinom tekućine u danom spremniku je primjer aplikacije gdje M2M uređaj periodično komunicira (npr. putem SMS poruka) svoja očitanja backend aplikaciji. Slika 1(b) prikazuje složeni scenarij u kojem je više grupa uređaja uključeno u M2M komunikaciju s poslovnom aplikacijom/aplikacijama, bilo izravno ili putem posredničkog uređaja (*gateway*). Primjeri aplikacija koje se uklapaju u ove scenarije uključuju upravljanje i nadzor prijevoza roba i ljudi (*fleet management*), optimizaciju energetskih sustava za distribuciju električne energije (*smart power grids*), osobnu zdravstvenu zaštitu (uglavnom iz domene m-zdravstva), pametne kuće, autonomne sustave za nadzor i optimizaciju industrijskih postrojenja i mnoge druge.



Slika 1: Tipična M2M arhitektura i scenariji: (a) jedan uređaj i (b) grupa uređaja u M2M komunikaciji (izravnoj ili posrednoj – primjenom posredničkog uređaja)

Osnovna karakteristika M2M sustava je veliki broj različitih M2M uređaja postavljenih u čovjekovu okolinu i organiziranih u automonmnu (bez ljudskog nadzora) distribuiranu mrežu. Mrežni operateri (posebno operateri celularnih mreža) kao i proizvođači mrežne opreme imaju visoka očekivanja od ovakve vizije umreženih uređaja. Snažni motivi za brzi rast M2M sustava proizlaze iz činjenice da je mobilno tržište već ušlo u zasićenje i postaje sve teže povećati postojeće dobiti i profite. Uistinu, procjenjuje se da je danas umreženo odnosno povezano 4,9 milijardi ljudi (od ukupne populacije od 7,08 milijardi) [2]. Stoga operateri i proizvođači opreme predviđaju da će do 2020. godine broj instaliranih M2M uređaja popeti na 50 milijardi [3]. Time se planiraju stvoriti uvjeti za snažniji rast kako podatkovnog prometa kroz postojeće mrežne infrastrukture (celularne i internet) tako i zahtjeva za M2M uslugama, što će konačno rezultirati i snažnijim rastom profita.

U svrhu ostvarivanja vizije o 50 milijardi umreženih M2M uređaja, najvažnije svjetske standardizacijske organizacije 3GPP, ATIS, CCSA, OMA, IEEE i European Telecommmunications Standards Instututе (ETSI) pokrenule su standardizacijske aktivnosti vezane uz MTC odnosno M2M komunikacije [4]. Pri tome je 3GPP orijentiran na tehničke specifikacije i unaprjeđenja postojećih i budućih celularnih mreža (UMTS i LTE) za bolju podršku MTC odnosno M2M komunikacija. Glavni fokus 3GPP-a je na optimizaciji M2M signalnog i podatkovnog prometa unutar celularnih mreža, u svrhu smanjenja rizika od zagušenja i preopterećenja mreže, što je vrlo važan aspekt u kontekstu vizije od 50 milijardi umreženih uređaja u budućnosti. S druge strane, standardizacijsko tijelo ETSI definira specifikacije vezane uz MTC/M2M servisnu i funkcionalnu arhitekturu, njihove osnovne komponente, kao i međusobnu povezanost između tri osnovne domene M2M sustava: aplikacijske, mrežne i domene M2M uređaja (slika 3). ETSI u svojim tehničkim specifikacijama TS 102 690 i TS 102 921 detaljno definira sigurnosne mehanizme M2M servisne razine (M2M *Service Layer security*); podršku za međusobnu autentifikaciju, zaštitu integriteta (cjelovitosti) poruka kao i povjerljivosti na sučelju (komunikacijskom kanalu) između M2M uređaja i pristupne mreže koja prenosi M2M promet [5, 6].



Slika 2: Horizontalna integracija u budućim M2M komunikacijama: aplikacijska razina dijeli zajedničku infrastrukturu i mrežne elemente (prema ETSI).

Usprkos ogromnom potencijalu kojeg M2M vizija nosi, postoje još uvijek brojni tehnički izazovi koje moramo riješiti da bi svjedočili stvarnosti s 50 milijardi M2M uređaja instaliranih do 2020. godine. Neki od izazova uključuju razvoj M2M softvera, zatim ostvarivanje energetski efikasne M2M komunikacije, te osiguranje pouzdanog rada i **sigurnosti** M2M komunikacija, što je i centralna tema ovog članka. Kao što je to slučaj sa svakom novom tehnologijom, uz prednosti i pogodnosti koje tehnologija donosi društvu obično postoji i određeni faktor rizika od zlouporabe iste. Ovi rizici mogu biti vrlo ozbiljni, posebno u kontekstu M2M aplikacija kao što su e-zdravstvo, *smart grids*, upravljanje transportnim sustavima i drugo. U tom smislu veliki broj M2M uređaja kao i distribuirana priroda M2M mreža predstavljaju posebne izazove u smislu potencijalnih sigurnosnih prijetnji kao i zaštite od istih.

U okviru ovog rada najprije ćemo kroz različite M2M scenarije (*use-cases*) diskutirati i naglasiti neke od najvažnijih sigurnosnih zahtjeva u kontekstu budućih M2M sustava. U nastavku ćemo dati kratak pregled najvažnijih sigurnosnih specifikacija za M2M komunikacije prema 3GPP i ETSI tehničkim specifikacijama. Konačno, u članku ćemo opisati neke od aktivnosti autora članka i njegovih suradnika na sigurnosnim temama vezanim uz M2M komunikacije. Konkretno, fokusirat ćemo se na problem uspostave povjerenja (*trust*) odnosno sigurnosnih asocijacija između M2M entiteta pri inicijalizaciji M2M mreže. Opisat ćemo nekoliko novih mehanizama i protokola za uspostavu sigurne komunikacije i zaštitu podataka koji se uklapaju u sigurnosnu M2M arhitekturu, a koji imaju odlike jednostavnosti uporabe (*user-friendliness*) i/ili energetske efikasnosti (*energy-efficiency*).

2 Sigurnosni zahtjevi u M2M komunikacijama

Generalno, pojam (informacijske) sigurnosti označava skup mjera (tehnika, postupaka, radnji) za zaštitu informacija i informacijskih sustava od raznih prijetnji kao što su neautorizirani pristup i korištenje informacija, otkrivanje i promjena informacija, uskraćivanje pristupa informacijama i uslugama danog informacijskog sustava. Tri ključna faktora u informacijskoj sigurnosti jesu: zaštita povjerljivosti (*confidentiality*), integritet podatka i izvorišta podataka (*data and source integrity*) i osiguravanje dostupnosti (*avaliability*) usluge. Moderni komunikacijski sustavi definiraju razne mehanizme za osiguravanje navedenih sigurnosnih usluga. Sustavi za M2M komunikacije, u tom smislu, nisu iznimka. Činjenice koje značajno otežavaju zaštitu M2M komunikacija jesu veličina M2M mreže (potencijalno veliki broj M2M uređaja) te rad M2M uređaja u nekontroliranim (neprijateljskim - *hostile*) okruženjima bez ljudskog nadzora. U nastavku ćemo detaljnije razraditi sigurnosne zahtjeve kroz nekoliko M2M scenarija (*use cases*) – scenariji su uzeti iz [7].

2.1 M2M scenariji

Scenarij 1: Nadzor prometa putem kamera

Prometne kamere opremljene radio modemima (celularnim i WLAN) postavljene su uzduž prometnice pa kamera predstavlja M2M uređaj. Kamere bilježe događanja na prometnici (prekoračenja brzine, prometne nesreće, oštećenja ceste), međusobno izmjenjuju podatke (npr. u slučaju potrebe određivanja prekoračenja brzine), potencijalno integriraju podatke lokalno i integrirane verzije šalju backend aplikaciji u svrhu daljnje obrade i arhiviranja podataka. Promjena cijene usluge ili nepokrivenost signalom može razlog za promjenu operatora.

Scenarij 2: Aparati za autonomnu distribuciju robe (*vending machines*)

Aparati za distribuciju robe (kave, slatkiša, duhanskih proizvoda) mogu biti opremljeni radio modemima (npr. celularnim) preko kojih su povezani sa backend aplikacijom koja nadzire njihov rad pa su aparati u M2M komunikaciji s poslovnom aplikacijom. Aparati se nalaze u nekontroliranom okruženju i često su izloženi napadima u kojima je ugrožen njihov sadržaj. Vlasnici aparata mogu proizvoljno mijenjati operatora kojeg koriste za ostvarivanje komunikacije između aparata i svojih poslovnih aplikacija ili mogu promijeniti vrstu pretplate.

Scenarij 3: Inteligentni mjerni uređaji (*smart metering* i *eHealth*)

Veći broj mjernih uređaja, opremljenih odgovarajućom komunikacijskom opremom (celularni, WLAN, IEEE 802.15.4 modemi) i osjetnicima/senzorima (električna brojila, osjetnik vlage, temperature), postavljeni su na odgovarajuće lokacije (strujne utičnice, energetske vodove, vodovodne cijevi) i/ili na ljude i životinje, gdje očitavaju razne fizikalne pojave i stanja (npr. vitalne znakove života). Neka mjerna osjetila/brojila su postavljena na udaljene lokacija gdje nemaju pristupa izvoru električne energije pa su napajana baterijskim putem. Uređaji prikupljaju podatke, bilježe lokaciju i vrijeme kada je pojava izmjerena odnosno detektirana, lokalno procesiraju podatke, međusobno ih razmjenjuju te ih u konačnici šalju putem transportne mreže (direktno ili posredno) odgovarajućoj poslovnoj aplikaciji.

2.2 Analiza M2M scenarija

U ovoj sekciji analiziramo potencijalne sigurnosne prijetnje u gore opisanim M2M scenarijima.

Sigurnosni problem 1: DoS napad (napad na dostupnost usluge)

Postoje brojni načini na koje je moguće ograničiti/blokirati dostupnost usluge u navedenim scenarijima. S obzirom da svi navedeni scenariji uključuju komunikaciju putem radio kanala, najjednostavniji način bi bilo izravno ometanje radio signala (*jamming*). Uistinu, na tržištu su lako dostupni i vrlo rasprostranjeni specijalizirani uređaji za ometanje npr. celularnih frekvencija; vrlo kvalitetne ometače radio signala je moguće dobaviti za cijenu ispod 100 USD [9]. Posljedice ovakvih nelegalnih aktivnosti za operatera M2M sustava mogu biti vrlo ozbiljne. Dulji prekid komunikacije može rezultirati gubitkom odnosno nepravodobnom isporukom važnih podataka (u oba smjera) u sva tri scenarija. Nepravodobna isporuka poruka može ugroziti:

- proces nadogradnje softvera na M2M uređajima;
- proces daljinske promjene mrežnog operatera – zbog specifičnosti M2M sustava, ovakve promjene će se raditi na daljinu putem radio kanala – *Over-the-Air* (OTA) programiranje [10]);
- protokole za sigurnu vremensku sinkronizaciju (nužnu u sva tri scenarija) – M2M uređaji ne mogu primati poruke o točnom vremenu putem GPS-a ili od celularne mreže;
- poruke sigurnih lokalizacijskih protokola (npr. u slučaju mobilnih mjernih M2M uređaja);
- prikupljene podatke npr. od strane M2M mjernih uređaja – ukoliko je memorija za pohranu prikupljenih podataka relativno mala, neki podaci će se nužno morati brisati;
- baterije na M2M uređajima koji nisu povezani na energetsku mrežu (npr. u *mHealth* i *smart metering* scenarijima) – M2M uređaji će neuspješno i repetitivno pokušavati komunicirati prikupljene podatke;
- rad mreže (celularne) koja prenosi podatke za veći broj M2M uređaja – npr. u trenutku u kojem je napadač prestao ometati komunikaciju većeg broja M2M uređaja, isti će pokušati simultano pristupiti celularnoj mreži, što može prouzrokovati veliki broj signalnih poruka unutar celularne mreže i ozbiljno ugroziti njene performanse.

Primijetite nadalje da operater M2M mreže (ne transportne mreže) neće uvijek biti u mogućnosti razlikovati situaciju u kojoj je komunikacija namjerno ometana u odnosnu na situaciju u kojoj je M2M uređaj jednostavno neispravan. Stoga se može dogoditi da M2M operater nepotrebno pošalje na teren tehničara – što značajno

povećava operativne troškove. Navedena lista potencijalnih problema nije iscrpljena, međutim i ovakva ukazuje na moguće ozbiljne posljedice napada na dostupnost radio signala. Iz ove kratke analize proizlazi zahtjev za rješenjem koje će budućim M2M sustavima minimalno omogućiti detekciju radio ometanja.

Sigurnosni problem 2: Ranjivost GPRS/EDGE/UMTS/HSPA mobilnih komunikacija (MitM napadi)

Ometanje radio signala često se i uspješno koristi za realizaciju *Man-in-the-Middle* (MitM) napada, kako na WLAN mreže tako i na moderne celularne mreže (3G-4G). Posljedice ovog napada mogu biti katastrofalne u smislu narušavanja povjerljivosti i integriteta podataka, obzirom da MitM napadač preusmjerava sav promet između M2M uređaja i M2M servera preko sebe.

U kontekstu celularnih mreža, ometanjem 3G-4G (UMTS, HSPA) signala većina modernih mobilnih uređaja će se prebaciti na 2G-2.5G signale i mreže (GSM, GPRS, EDGE). Kao što je demonstrirano u [11], napadač može ovo iskoristiti na način da instalira lažnu 2.5G baznu stanicu. Napadač zatim iskoristi poznate sigurnosne propuste u GPRS i EDGE tehnologiji. Konkretno, kod GPRS-a i EDGE-a, mobilni telefon ne autentificira baznu stanicu na koju se spaja. Osim toga, prema specifikacijama, mobilni uređaji moraju podržavati GEA0 enkripcijski algoritam (esencijalno znači "ne koristi enkripciju"). Vrstu enkripcije, prema GPRS i EDGE specifikacijama uvijek i isključivo bira bazna stanica. Iz svega navedenog proizlazi da napadač može preuzeti potpunu kontrolu nad podatkovnim prometom danog mobilnog telefona (odnosno M2M uređaja). Ovo je vrlo važno zapažanje s obzirom da postoje mnoga uvjerenja da je M2M komunikacija sigurna samim time što se odvija putem sigurnih 3G-4G celularnih mreža. Stoga su nužne dodatne mjere i koraci za ispravnu zaštitu M2M komunikacija – konkretno zaštita podataka (povjerljivosti i integriteta) na višim razinama, iznad prijenosne razine.

Sigurnosni problem 3: Fizička ranjivost M2M uređaja

Priroda M2M sustava je takva da će veliki broj M2M uređaja često biti postavljen u nekontroliranom okruženju u kojem će često biti izloženi fizičkim napadima (npr. automati ili dislocirani M2M mjerni uređaji u našim scenarijima). Sigurnosne implikacije fizički kompromitiranih M2M uređaja mogu biti vrlo ozbiljne. Osim izravne fizičke štete, napadač može kompromitirati podatke pohranjene u memoriji uređaja (prikupljena očitanja, enkripcijski ključevi) ili one pohranjene u UICC (*Universal Integrated Circuit Card*) i SIM karticama (autentifikacijski ključevi, digitalni certifikati) na M2M uređajima. Na ovaj način napadač može posredno ostvariti neovlašten pristup kako M2M uslugama tako i samoj poslovnoj M2M aplikaciji. Nadalje, napadač može prebaciti SIM i/ili UICC karticu na drugi uređaj, primjerice na običan mobilni telefon.

Ovaj aspekt sigurnosti M2M uređaja, fizička sigurnost, značajan je i slučaju zastare i bacanja ili otuđivanja (prodaje) korištenog M2M uređaja. Slično kao u slučaju izravnog fizičkog napada, ukoliko odbačeni M2M uređaj nije adekvatno deaktiviran (pobrisana memorija, SIM i/ili UICC kartica deaktivirana) moguće je iskoristi sadržaj istoga za ostvarivanje neautoriziranog pristupa M2M podacima i uslugama.

Fizički napadi uključuju i dislociranje (statičkih) M2M uređaja, te manipulaciju njegovim osjetnicima (senzorima) i mjernim komponentama s ciljem provociranja krivih očitavanja. Dakle, nužno je razviti rješenja koja će znati prepoznati ovakvu vrstu fizičkih manipulacija. To, primjerice, može biti detekcija neautoriziranog pomicanja M2M uređaja pomoću akcelerometara koji bi upozorili operacijski sustav uređaja da je došlo po neplaniranog pomicanja, a operacijski sustav može nakon dodatnih provjera pokrenuti postupak deaktivacije (brisanja) M2M uređaja.

Sigurnosni problem 4: Zaštita privatnosti na komunikacijskim kanalima

Standardne metode za enkripciju odnosno zaštitu povjerljivosti podataka generalno ne osiguravaju potpunu zaštitu privatnosti. Iako će M2M sustavi koristiti adekvatne enkripcijske algoritme kao što je AES za zaštitu M2M podataka, AES enkripcija sama po sebi ne osigurava potpunu privatnost podataka. Primjerice, u nekim rješenjima m-zdravstva, M2M uređaj koji mjeri vitalne znakove života neke osobe, te svoja očitanja komunicira putem radio kanala u realnom vremenu pri čemu su komunikacijski kanal, odnosno podatkovni paketi enkriptirani te je zaštićen njihov integritet. Međutim, pasivnim osluškivanjem transmitiranih poruka odnosno analizom prometa (*traffic analysis*) potencijalno je moguće zaključiti npr. ritam i/ili intenzitet otkucaja srca. Vremenski raspored paketa (vremenski razmak između susjednih paketa) kao i njihova veličina može biti koreliran sa ritmom i intenzitetom rada srca. Iako napadač ne može direktno dekriptirati pakete, iz njihovih karakteristika mogu se saznati potencijalno korisne informacije. Na primjer, u radu [12] grupa autora je pokazala kako precizno identificirati jezik konverzacije koja se odvije putem enkriptirane VoIP (Skype) komunikacije.

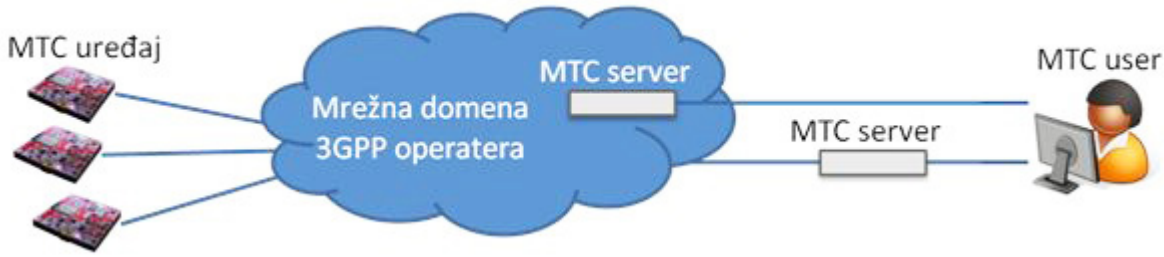
Sličan problem narušavanja privatnosti moguć je i u *smart metering* scenariju. Zamislimo da skupina M2M uređaja komunicira detaljna očitanja potrošnje električne energije (na razini trošila) u danom kućanstvu. S pozitivne strane, prikupljena mjerenja mogu biti osnova za optimiziranje potrošnje električne energije (za dano kućanstvo) kao i optimiziranje i planiranja rada električne mreže (za distributera) – *smart grid* koncept. S negativne strane, navedena detaljna očitanja u formi potrošnje po trošilu (umjesto samo kumulativne potrošnje), omogućavaju distributeru izradu detaljanog profila potrošnje danog kućanstva (koji uređaj i kada je bio uključen). Ovo je primjer vrlo ozbiljnog (kritičnog) narušavanja privatnosti.

3 M2M standardi: sigurnosni aspekti

U tijeku su mnoge standardizacijske aktivnosti vezane za buduće M2M komunikacije. Između ostalih, dio aktivnosti odnosno tehničkih specifikacija pokriva problematiku sigurnosti. U slijedećoj sekciji ukratko ćemo predstaviti najvažnije aktivnosti na tom području od strane 3GPP alijanse i ETSI standardizacijskog tijela, a u nastavku ćemo opisati neka sigurnosna rješenja koja je razvila istraživačka grupa autora članka – djelomično u suradnji i pod pokroviteljstvom kompanije Ericsson Nikola Tesla.

3.1 3GPP aktivnosti

Tipična M2M/MTC arhitektura prema 3GPP-u prikazana je na slici 4.



Slika 3: M2M arhitektura prema 3GPP

3GPP arhitektura sastoji se od tri glavna dijela odnosno domene: domena MTC/M2M uređaja, domena transportne mreže, i aplikacijska M2M domena. Po pitanju transportne mreže, 3GPP-ove standardizacijske aktivnosti usko su vezane uz 3GPP mobilne celularne mreže. Aplikacijska domena sastoji se od MTC poslužitelja koji mogu biti pod kontrolom operatera transportne mreže ili nekog drugog neovisnog operatera. 3GPP je izdao dvije tehničke specifikacije koje pokrivaju sigurnosne aspekte: TR 33.868 – s fokusom na razne sigurnosne aspekte MTC komunikacija [8] i TR 33.812 – koja predstavlja studiju izvedivosti sigurne daljinske inicijalizacije i promjene operatera M2M uređaja [7].

Generalni sigurnosni aspekti (3GPP TR 33.868)

U dokumentu TR 33.868 3GPP daje listu ključnih sigurnosnih problema kao i opis rješenja za iste. Ključni sigurnosni problemi prema 3GPP prikazani su u tablici 1. Osim navedenog u tabeli 1, generalano 3GPP naglašava važnost implementacije ispravne kontrole pristupa transportnoj 3GPP mreži. Također se veliki naglasak stavlja na sigurnosna rješenja koja su energetski efikasna, obzirom su MTC uređaji često baterijski napajani.

Predložena rješenja za sigurnosne probleme iz tablice 1 zasnivaju se na primjeni ili proširenju postojećih 3GPP sigurnosnih mehanizama i protokola. Na primjer, u scenariju u kojem MTC server i transportna 3GPP mreža pripadaju istom operateru, 3GPP predlaže primjenu *Generic Bootstrapping Architecture* (GBA) [13] za inicijalnu autentifikaciju M2M uređaja te uspostavu enkripcijskih i autentifikacijskih ključeva koji će se koristiti za end-2-end zaštitu između MTC servera i MTC uređaja, kao i za zaštitu integriteta relevantnih poruka između transportne mreže i MTC entiteta. GBA omogućuje međusobnu autentifikaciju MTC uređaja i MTC poslužitelja/aplikacija, koja je zasnovana na kriptografskim ključevima koji se generiraju primjenom postojećih 3GPP autentifikacijskih mehanizama kao što je 3GPP AKA (*Authentication and Key Agreement*) [14]. AKA je standardan mehanizam za izvođenje novih autentifikacijskih ključeva na temelju postojeće 3GPP autentifikacijske infrastrukture i digitalnih vjerodajnica (autentifikacijskog materijala) koji se nalaze na UICC karticama instaliranim u mobilnim (odnosno u našem slučaju MTC) uređajima.

U slučaju kada MTC server nije u ingerenciji operatera transportne mreže, sučelje između 3GPP transportne mreže i MTC servera može se zaštiti primjenom mehanizama kao što je NDS/IP (*Network Domain Security/IP network security*), odnosno IPSec protokola [8]. U ovom rješenju, transportna 3GPP mreža i MTC Server uspostavljaju IPSec vezu preko IPSec poveznika (*gateway*).

Tablica 1: Sigurnosne prijetnje prema 3GPP TR 33.868.

1. Prozivanje M2M uređaja (*device triggering*)	U mnogim M2M aplikacijama koristiti će se tzv. poll model za komunikaciju između MTC uređaja i MTC poslužitelja: uređaj će slati očitanja/podatke poslužitelju tek na zahtjev. Ovo je zanimljivo u situacijama u kojima MTC korisnik ne želi da MTC uređaj bude stalno povezan sa MTC serverom ili MTC uređaj jednostavno nije kontinuirano vezan na pristupnu mrežu. Sigurnosni problem: Napadač šalje lažne (*triger*) poruke za buđenje i spajanje MTC uređaja - npr. lažne SMS poruke.
2. Sigurna veza (*secure connection*)	Odnosi se na mogućnost uspostave sigurne veze između MTC uređaja i odgovarajućeg MTC servera.
3. Neautentificirana Reject poruka (*Reject message without integrity protection*)	Lažna bazna stanica može poslati lažne poruke tipa „*IMSI unknown in HLR*“ ili „*PLMN not allowed*“ u *Reject* porukama i time onemogućiti MTC uređaju pristup mobilnoj mreži – DoS napad.
4. Kontrola zagušenja (*congestion control*)	U svrhu sprječavanja zagušenja transportne mreže signalnim prometom, celularne mreže imaju mogućnost ograničenja/blokiranja pristupa mreži. Postojeća rješenja su zasnovana na dodijeljenim indikatorima prioriteta koje mobilni uređaj mora predati mreži. U uvjetima zagušenja, uređajima koji imaju niski prioritet blokira se pristup mreži. Sigurnosni problem se može javiti kada indikatori prioriteta nisu kriptografski zaštićeni. U tom slučaju napadač može npr. povećati indikatore prioriteta MTC uređaja (koji se nalaze u paketima za zahtjev pristupa mreži). Posljedica ovog je da će se M2M uređaji spajati (i povećavati signalni promet) na već zagušenu mrežu.
5. Sigurnost vanjskog sučelja (*external interface security*)	Aplikativna domena u MTC može biti pod kontrolom operatera neovisnog od operatera transportne 3GPP mreže. U tom slučaju sučelje (komunikacijski kanal) između transportne mreže i aplikativne domene može biti nezaštićeno a time i cijeli promet na tom kanalu. Stoga se potencijalni napadač može npr. lažno predstaviti kao MTC server te slati lažne zahtjeve odgovarajućim MTC uređajima. MTC uređaji će pokrenuti proceduru za povezivanje na transportnu mrežu. Osim potrošnje baterije na MTC uređajima, veliki broj istovremenih zahtjeva za povezivanje može izazvati ozbiljna zagušenja u celularnoj mreži. Mogući su i drugi ozbiljni sigurnosni problemi (npr. curenje privatnih informacija kao što su identiteti uređaja).
6. Ograničavanje UICC kartice (odnosno USIM aplikacije) za korištenje sa točno određenim MTC uređajem	MTC korisnik može dogovoriti određenu povoljniju tarifu sa 3GPP operatorom – npr. jeftiniji prijenos M2M podataka u odnosu na klasične podatkovne tarife. U ovom slučaju MTC korisnik može pokušati prebaciti UICC karticu na drugi uređaj (npr. svoj laptop) s ciljem ostvarivanja podatkovne usluge po povoljnijoj tarifi. Stoga je nužno predložiti rješenje koje će vezati jedan USIM sa samo jednim ili legalnom grupom MTC uređaja.
7. Narušavanje privatnosti	Neki tipovi MTC uređaja mogu se lako povezati sa osobom (MTC korisnik) koja konzumira podatke s tog uređaja. Tako je moguće npr. povezati MTC uređaje koji prikupljaju očitanja na određenoj lokaciji s korisnikom tih informacija – što predstavlja potencijalnu povredu privatnosti korisnika.

Daljinska administracija MTC uređaja (3GPP TR 33.812)

Osim generalnih sigurnosnih aspekata M2M komunikacija, 3GPP opisuje detaljnu studiju izvedivosti daljinske administracije MTC uređaja u smislu jednostavne inicijalizacije uređaja, promjene pretplate i operatera, nadogradnje softvera. Ovo je vrlo važan praktičan aspekt obzirom da će MTC uređaji biti postavljeni na udaljenim lokacijama. Nemogućnost daljinske administracije MTC uređaja zahtijevala bi fizičko prisustvo osobe na tim lokacijama pri svakoj promjeni pretplate, operatera, inicijalizaciji MTC uređaja novim autentifikacijskim ključevima, nadogradnji softvera. U tehničkom izvješću TR 33.812, 3GPP opisuje dvije kategorije rješenja za daljinsku administracije MTC uređaja: rješenje zasnovano na UICC kartici i rješenje zasnovano na specijalziranom TRE (Trusted Enviroment) modulu (UICC-free rješenje). TRE je okruženje koje omogućuje hardversku i softversku zaštitu

autentifikacijskih podataka i funkcija, odnosno Machine Communication Identity Module – MCIM. MCIM omogućava MTC uređaju pristup 3GPP mreži – MCIM je sličan USIM i ISIM aplikacijama koje se pohranjuju na UICC karticu i omogućavaju mobilnim uređajima pristup 3GPP mrežama. Prema definiciji USIM i ISIM aplikacije se pohranjuju na UICC karticu, dok MCIM može biti pohranjen na UICC ili u TRE.

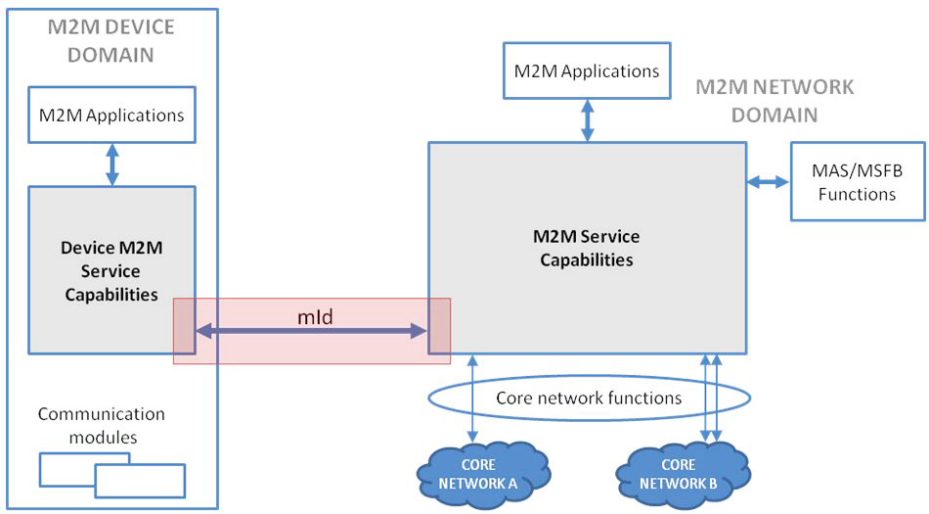
U studiji 3GPP TR 33.812 opisano je nekoliko mogućnosti za zaštitu procesa daljinske administracije USIM/ISIM/MCIM aplikacija u kontekstu 3GPP sustava.

- Rješenje zasnovano na TRE modulu instaliranom na MTC uređaju.
  a. TRE validira MTC uređaje i autentificira korisnike.
  b. Može pohraniti više MCIM modula koji se mogu administrirati daljinski.
- Rješenje zasnovano na UICC, bez podrške za daljinsku administraciju.
  a. Svaki MTC uređaj opremljen je zamjenjivom UICC karticom.
  b. Inicijalizacija/promjena pretplate/operatera obavlja se zamjenom kartica (postojeći M2M sustavi u osnovi koriste ovu metodu).
- Rješenje zasnovano na UICC s podrškom za daljinsku administraciju (koristi se standardizirana OTA (Over-the-Air, npr. TS 102 225) procedura za daljinsku administraciju/nadogradnju MTC uređaja). Razlikujemo dva slučaja:
  a. UICC kartica na MTC uređaju pohranjuje jedan OTA ključ koji inicijalno zna prvi mrežni operater (MNO1) preko kojeg je vezan MTC uređaj. Kada MTC korisnik inicira promjenu operatera MNO1 u MNO2, prvi operater MNO1 jednostavno isporučuju OTA ključ novom operateru MNO2 i o tome obavještava MTC uređaj (mijenja njegov IMSI).
  b. UICC kartica pohranjuje listu OTA ključeva (proizvođač UICC inicijalizira karticu). Prvi mrežni operater MNO1 zna prvi OTA ključ sa liste. Pri promjeni operatera, MNO1 obavještava MTC uređaj (mijenja njegov IMSI i upućuje ga da koristi sljedeći OTA ključ pohranjen na UICC kartici). Novi operater MNO1 kontaktira proizvođača UICC kartice od kojeg dobiva novi OTA ključ kojim može daljinskim administrirati MTC uređaj (stari operater MNO1 ne zna novi OTA ključ).

3.2 ETSI standardizacijske aktivnosti

Za razliku od 3GPP grupe, koja je fokusirana na M2M komunikacije u celularnim mobilnim mrežama, ETSI definira generalnu sistemsku arhitekturu za podršku M2M komunikacijama, gdje transportne mreže mogu biti ne samo celularne već WLAN, WiMAX, klasične žičane mreže (Internet). ETSI standardizira skup M2M servisnih komponenti (*M2M Service Capabilities*) koje su neovisne o poslovnim aplikacijama, transportnim mrežama i vrstama M2M uređaja. M2M servisne komponente mogu pristupati i koristiti funkcije centralne mreže (core network) te omogućavaju M2M aplikacijama pristup raznim M2M funkcijama kroz skup standardiziranih sučelja. Na ovaj način ETSI nastoji pojednostavniti proces razvoja i instalacije M2M aplikacija. ETSI opisuje M2M funkcionalnu arhitekturu u tehničkoj specifikaciji TS 102 690 [5].

U ovom članku, naš fokus je usmjeren na M2M sigurnosne servise (*M2M Security Capabilites*) definirane u dijelu tehničke specifikacije TS 102 690. Konkretno, ETSI definira podršku za međusobnu autentifikaciju, zaštitu integriteta i zaštitu povjerljivosti na sučelju između M2M uređaja i mrežne domene (sučelje označeno kao mId na slici 4, unutar crvenog okvira).



Slika 4: Funkcionalna arhitektura M2M servisnih komponenti (prema ETSI).

Definirane su sljedeće M2M servisne komponente vezane uz sigurnost:

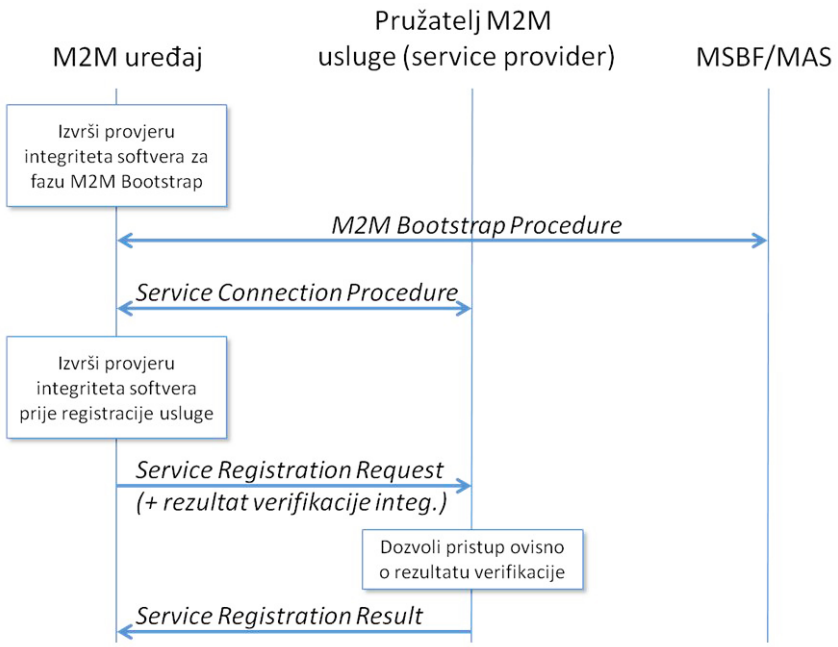
» NSEC (*M2M Network Security Capability*) – sigurnosne funkcionalnosti u mrežnoj domeni
  a. Sigurna inicijalizacija M2M servisa (M2M Service Bootstrap – slika 5).
  b. Realizacija odgovarajuće hijerarhije kriptografskih ključeva (slika 6).
  c. Autentifikacija i uspostava izvedenih sesijskih ključeva.
  d. Provjera integriteta softvera na M2M uređaju.

» DSEC (*M2M Device Security Capability*) – sigurnosne funkcionalnosti u domeni M2M uređaja:
  a. Sigurna inicijalizacija M2M servisa (*M2M Service Bootstrap*).
  b. Realizacija odgovarajuće hijerarhije kriptografskih ključeva.
  c. Autentifikacija i uspostava izvedenih sesijskih ključeva.
  d. Provjera integriteta softvera na M2M uređaju – čiji rezultat može prijaviti NSEC komponenti.
  e. Pohrana konekcijskih ključeva Kmc (*M2M Connection Keys* - slika 6).

Osim toga, u funkcionalnoj arhitekturi, ETSI definira sve funkcije nužne za upravljanje M2M servisnim komponentama mrežne domene. Posebno relevantne funkcije za sigurnost su MSBF (*M2M Service Bootstrap Function*) i MAS (*M2M Authentication Server*), locirane u mrežnoj domeni kao što je prikazano na slici 4.

M2M Service Bootstrap Function

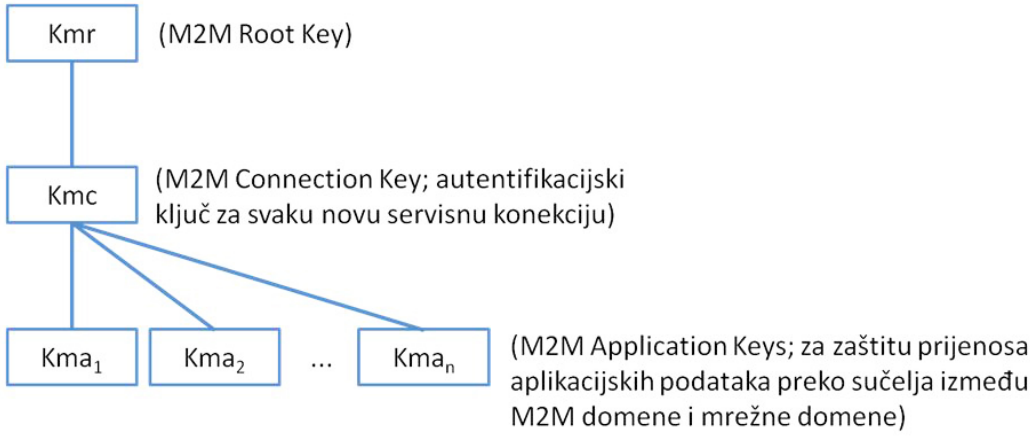
M2M uređaj mora biti inicijaliziran odgovarajućim digitalnim vjerodajnicama (permanentnim autentifikacijskim ključevima i identifikatorima) koji će biti osnova za uspostavu sigurne komunikacije, međusobne autentifikacije, naplate usluga i slično, između servisnih komponenti M2M uređaja i pružatelja M2M usluga (*M2M Service Provider*).



Slika 5: Proces inicijalizacije M2M servisa

U tu svrhu koristi se *M2M Service Bootstrap* procedura između M2M uređaja, odnosno određenog D/G M2M čvora (*D/G M2M Node*) na tom uređaju, s jedne strane, te MSBF i MAS s mrežne strane (slika 5).

D/G M2M čvor predstavlja logičku reprezentaciju jednog skupa M2M komponenti na M2M uređaju; važno je naglasiti da jedan uređaj može podržavati više D/G M2M čvorova istovremeno. Svaki D/G M2M čvor označen je jedinstvenim identifikatorom – *M2M-Node-ID*. Kao što je prikazano na slici 5, ova procedura je (opcijski) uvjetovana uspješnom provjerom integriteta softvera na M2M uređaju. Rezultat *M2M Service Bootstrap* procedure jesu permanentni ključevi (*M2M Root Key* - slika 6) i identifikatori vezani uz jedinstven D/G M2M čvor, odnosno jedinstvena i sigurna veza između D/G M2M čvora i poslužitelja M2M usluge. Moguće je, izvršavanjem više *M2M Bootstrap* procedura sa istim ili različitim pružateljima M2M usluga, istovremeno instancirati više D/G M2M čvorova na istom M2M uređaju.

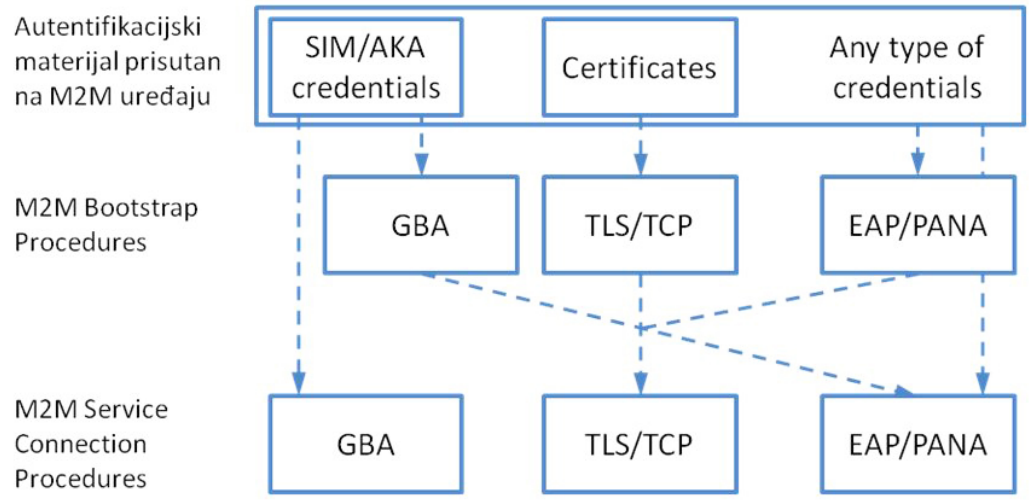


Slika 6: Hijerarhija ključeva za ETSI servisnu razinu

M2M Bootstrap procedura se ne izvršava ukoliko je M2M uređaj inicijaliziran putem npr. UICC kartica od strane pružatelja M2M usluga. U protivnom, ovisno o tome postoji li poslovna veza između operatera pristupne mreže i pružatelja M2M usluge, M2M Bootstrap procedura se može realizirati na dva načina: uz pomoć pristupne mreže i neovisno o pristupnoj mreži.

U prvom slučaju, operater pristupne mreže i pružatelj M2M usluge dijele poslovnu vezu te se servisne komponente M2M uređaja mogu inicijalizirati pomoću kriptografskog materijala (digitalnih vjerodajnica) same pristupne mreže (koji se normalno koriste za kontrolu pristupa toj mreži). Primjerice, mogu se koristiti SIM i AKA vjerodajnice koje se nalaze na UICC kartici za potrebe kontrole pristupa celularnoj mreži. ETSI definira niz procedura i protokola za ovu svrhu koji su zasnovani na GBA (*Generic Bootstrapping Architecture* [13]) arhitekturi i na EAP (*Extensible Authentication Protocol* [15]) protokolu (slika 7).

Ukoliko operater pristupne mreže i pružatelj M2M usluge nisu u poslovnoj vezi (neovisni su), ETSI propisuje primjenu EAP/PANA [16] i TLS protokola u sljedećim kombinacijama (slika 7, srednji red): EAP-IBAKE preko EAP/PANA, EAP-TLS preko EAP/PANA i TLS/TCP protokol [5]. Koji autentifikacijski mehanizam će se koristiti ovisi o tome koji tip digitalnih vjerodajnica (*X.509 certifikates*, SIM, *pre-shared keys*, OTP, SIM, AKA, i dr.) se nalazi instaliran na M2M uređajima prije pokretanja *M2M Bootstrap* procedure (slika 7 – prvi red).



Slika 7: Protokoli i okviri za autentifikaciju i uspostavu dijeljenih ključeva (*M2M Root i M2M Connection Keys*) između M2M uređaja i mrežne domene.

M2M Service Connection procedura

Po uspješnoj inicijalizacijskoj proceduri, M2M uređaj (odnosno M2M čvor na tom uređaju) inicijaliziran je Kmr ključem – *M2M Root Key* (slika 6). Ovaj ključ je permanentan i koristi za međusobnu autentifikaciju i uspostavu svih izvedenih ključeva između M2M uređaja i pružatelja M2M usluge (*M2M Service Provider*). M2M uređaj sada može zatražiti uspostavu M2M servisne veze između inicijaliziranog D/G M2M čvora i

odgovarajućeg mrežnog čvora u mrežnoj domeni pružatelja M2M usluga (slika 5). ETSI definira *M2M Service Connection* proceduru za navedenu svrhu. Rezultat ove procedure je sigurna veza između M2M servisnih komponenti M2M uređaja i M2M servisnih komponenti mrežne domene – slika 4.

M2M Service Connection procedura sastoji se od nekoliko faza (slika 5):

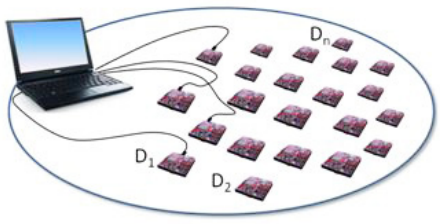
- Međusobna autentifikacija D/G M2M čvora na M2M uređaju i odgovarajućeg pružatelja M2M usluge (za ove potrebe koristi se ključ Kmr – *M2M Root Key* – kojim je M2M uređaj inicijaliziran u prethodnoj fazi).
- Uspostava M2M konekcijskog ključa Kmc (*M2M Connection Key*) i opcijski jednog ili više aplikacijskih ključeva Kma (*M2M Application Key*). Ovi ključevi se izvode iz Kmr (kako je prikazano na slici 6), te se koriste za zaštitu kanala između M2M uređaja (odnosno M2M servisnih komponenti) i mrežnih M2M servisnih komponenti (vidi sliku 4). Dok je Kmr permanentan ključ, različiti Kmc ključ se generira za svaki novi zahtjev za uspostavu servisne veze između D/G M2M čvora i odgovarajućeg mrežnog M2M čvora.
- Slanje izvještaja o rezultatima verifikacije integriteta softvera na M2M uređaju. Ovisno o rezultatu, M2M uređaju će biti dopušteno povezivanje na mrežnu domenu i M2M servise u ingerencije odgovarajućeg pružatelja M2M usluge.

Za potrebe autentifikacije i izvođenja ključeva Kmc i Kma na osnovu ključa Kma, ETSI definira niz procedura i mehanizama koje su slične onima za *M2M Bootstrap* funkcije (slika 7 – posljednji red).

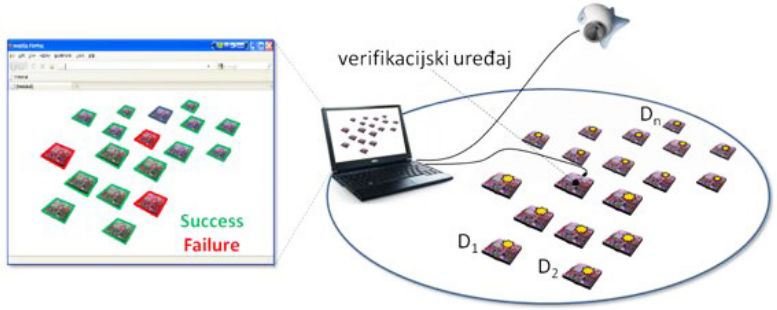
Važno je naglasiti da prema ETSI specifikacijama, svi uređaji u domeni M2M uređaja (slika 2) ne trebaju podržavati i implementirati gore navedene M2M servisne komponente (uljučujući sigurnosne komponente). Takvi uređaji mogu ostvariti vezu s aplikacijskom M2M domenom putem posredničkih M2M uređaja koji implementiraju ETSI servisne komponente. Uređaji u domeni M2M uređaja umrežuju se kroz *M2M Area Network* koja koristi postojeće PAN (*Personal Area Networks*) tehnologije kao što su *IEEE802.15.1, IEEE802.15.4, Zigbee, ISA 100.11a, i dr. ili LAN mreže PLC, Wireles M-BUS* i druge.

4 Naša rješenja

U ovom dijelu kratko ćemo opisati sigurnosne mehanizme, primjenjive na M2M komunikacije, koje je razvila istraživačka grupa autora ovog članka, djelomično pod pokroviteljstvom kompanije Ericsson Nikola Tesla. Konkretno, fokusirat ćemo se na problem sigurne i jednostavne inicijalizacije velikog broja M2M uređaja i te posebno na problem dizajna energetski efikasnih enkripcijskih metoda prilagođenih M2M uređajima. U uvjetima kada ICT sektor „pridonosi“ 2-2.5% ukupnom svjetskom zagađenju, što je ekvivalentno zrakoplovnoj industriji, energetska efikasnost je nužna odlika budućih komunikacijskih sustava [17].



Slika 8: Inicijalizacija M2M uređaja putem kabela.



Slika 9: Arhitektura predloženog višekanalnog mehanizma za inicijalnu uspostavu sigurnosnih asocijacija.

4.1 Višekanalni protokoli za inicijalizaciju M2M uređaja

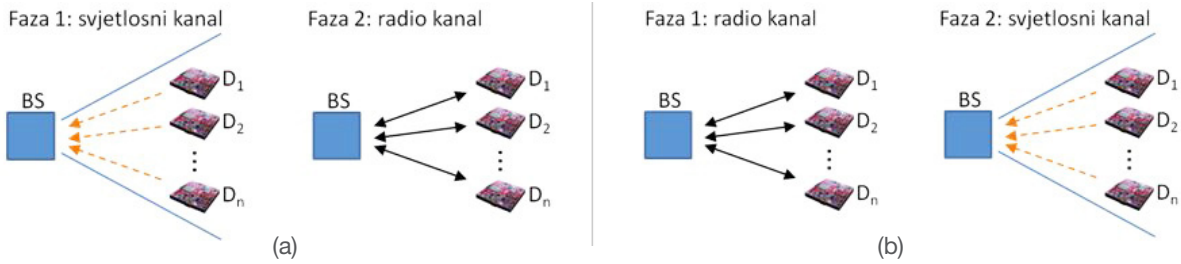
Osnovni preduvjet uspostave sigurne M2M mreže (*M2M Area Network*) i M2M komunikacija je upisivanje inicijalnog kriptografskog materijala (digitalnih vjerodajnica) u M2M uređaje. Ovaj problem se u praksi često zanemaruje ili se smatra trivijalnim. Čak i u 3GPP i ETSI specifikaciji jednostavno se pretpostavlja prisustvo određenog kripto-materijala u M2M uređajima prije M2M Bootstrap procedure. Danas, nažalost, postoji vrlo malo praktičnih i skalabilnih metoda za ubacivanje inicijalnog kripto-materijala u M2M uređaje. Postojeća rješenja uključuju tvornički inicijalizirane uređaje (tajni ključevi se snime u uređaje u postupku proizvodnje), inicijalizaciju putem npr. USB kabela (slika 8), jednostavno slanje ključeva preko nezaštićenog radio kanala

ili pak zahtijevaju korištenje specijaliziranih uređaja (npr. Faradejev kavez). Ova rješenje su nesigurna (npr. tvornička inicijalizacija), ne skaliraju dobro s brojem uređaja (inicijalizacija putem kabela) ili su jednostavno presložena za krajnjeg korisnika. Višegodišnje iskustvo sa WiFi mrežama naučilo nas je da korisnici često nemaju dovoljno znanja da bi podesili sigurnost u mrežama od svega nekoliko prijenosnih računala (da ne spominjemo desetke i stotine M2M uređaja).

U [18, 19] razvili smo nekoliko metoda za inicijalno upisivanje kripto-ključeva u M2M uređaje na siguran i jednostavan (intuitivan) način za krajnjeg korisnika. Predložene metode omogućavaju jednostavnu i brzu inicijalizaciju stotine i tisuće M2M uređaja. Naše inicijalizacijske metode zasnovane su na tzv. višekanalnim (*multichannel*) protokolima kod kojih se komunikacija odvija preko dvosmjernog radio kanala i jednosmjernog optičkog/svjetlosnog kanala. Na slici 9 prikazana je tipična postavka za predložene metode. Pretpostavlja se da je korisnik opremljen standardnom opremom kao što su laptop i kamera (obična web kamera), te da je svaki M2M uređaj opremljen LED diodom. Jednosmjerni svjetlosni kanal realizira se paljenjem i gašenjem LED dioda (*on/off* modulacija) na strani M2M uređaja, koje bilježi laptop preko kamere (slika 9).

Inicijalizacijska metoda 1: simetrična kriptografija

Prva inicijalizacijska metoda koristi simetričnu kriptografiju, zbog čega je prilagođena za inicijalizaciju M2M uređaja vrlo ograničene procesorske snage. U ovoj metodi, slika 10(a), korisnik posloži M2M uređaje (označene kao D_1,D_2,..D_n) u fokus kamere koja je dio bazne stanice BS. Baznu stanicu BS čine računalo, monitor, kamera i tzv. verifikacijski M2M uređaj koji računalu služi kao posrednik za komunikaciju s ostalim M2M uređajima putem radio kanala (slika 9). Cilj metode je uspostava jedinstvenog tajnog ključa između BS i svakog pojedinačnog M2M uređaja D_i.



Slika 10: Faze višekanalnog mehanizma za inicijalizaciju M2M uređaja zasnovanog na (a) simetričnoj kriptografiji, i (b) asimetričnoj kriptografiji.

Kao što prikazuje 10(a), proces inicijalizacije se odvija u dvije faze. U prvoj fazi M2M uređaji generiraju tajni ključ koji komuniciraju putem zaštićenog svjetlosnog kanala (blinkanjem LED dioda) baznoj stanici BS; na slici je taj proces je prikazan isprekidanim strelicama. BS snima (potencijalno nesinkronizirane) LED diode na svim M2M uređajima istovremeno te interpretira/demodulira transmitirane ključeve. U dugoj fazi inicijalizacije, BS inicira provjeru tajnih ključeva primljenih putem LED kanala preko standardnog dvosmjernog radio kanala (dvosmjerne pune strelice na slici 10(a). Provjera se putem standardnih autentifikacijskih protokola (npr. ISO/IEV 9798-2) pri čemu BS koristi verifikacijski M2M uređaj za komunikaciju s ostalim M2M uređajima. Svaki uspješno provjereni ključ indiciran je na monitoru (slika 9) tako da korisnik može završiti inicijalizaciju odgovarajućeg M2M uređaja jednostavnim pritiskom tipke na tom uređaju. Po uspješnoj inicijalizaciji svih M2M uređaja, BS odnosno inicijalizacijsko računalo dijeli ključeve sa svim M2M uređajima i u biti je posrednik u uspostavi sigurnosnih asocijacija između bilo kojeg para ili grupe M2M uređaja. Naknadna komunikacija se odvija putem standardnog radio kanala.

Važno je uočiti da se kod ove metode tajni ključevi šalju preko nezaštićenog svjetlosnog kanala. Stoga sigurnost metode ovisi o dostupnosti svjetlosnog kanala napadaču, odnosno može li napadač vidjeti LED diode na M2M uređajima. U nekim uvjetima, npr. kontrolirana i zatvorena soba kojoj napadač nema ni fizički ni vizualni pristup, svjetlosni LED kanal je siguran. U drugim uvjetima, moguće je prekriti kameru i M2M uređaje odgovarajućim zastorom koji ne propušta svjetlo. Istovremeno, radio signal ne možemo koristiti za inicijalan transfer tajnih ključeva obzirom da se radio signali rasprostiru kroz zidove i prepreke. U drugoj inicijalizacijskoj metodi, zasnovanoj na asimetrično kriptografiji, nije potrebna takva fizička zaštita LED kanala.

Inicijalizacijska metoda 2: asimetrična kriptografija

Ova metoda je puno fleksibilnija od prve i koristi se za inicijalizaciju M2M uređaja koji podržavaju asimetričnu kriptografiju. Proces je prikazan na slici 10(b). Kao i prije, cilj je uspostava sigurnosne asocijacije između svakog M2M uređaja i bazne stanice. U prvoj fazi, BS i M2M uređaji razmjene svoje javne ključeve preko nesigurnog javnog radio kanala, primjenom odgovarajućeg protokola. U drugoj fazi, M2M uređaji na osnovu podataka iz prethodne faze, formiraju kratak autentifikacijski string (*Short Authentification String* (SAS)) kojim autentificiraju razmijenjene javne ključeve s BS-om. M2M uređaji transmitiraju autentifikacijski string SAS

putem jednosmjernog svjetlosnog LED kanala. Uspješnom provjerom autentifikacijskog stringa, BS potvrđuje autentičnost javnih ključeva razmijenjenih s M2M uređajima, što se u konačnici indicira korisniku putem monitora (slika 9). Za razliku od prethodne metode, kod ove metode nije nužna fizička zaštita svjetlosnog kanala, LED kanal je javan i napadač mu može imati pristup. Dakako, nužno je osigurati autentičnost svjetlosnog kanala u smislu da napadač ne može mijenjati podatke transmitirane na takvom kanalu (npr. primjenom lasera). Reference [18] i [19] opisuju kako osigurati autentičnost svjetlosnog kanala pomoću jednostavnih kodova (Machester i Berger kodovi).

Obije opisane inicijalizacijske metode zahtijevaju korištenje dodatnog hardvera (iako standardnog). U [19] smo opisali novu inicijalizacijsku metodu koja također koristi svjetlosni kanal ali ne zahtjeva nikakave dodatne pomoćne uređaje (kamere, računala i sl.). Umjesto kamere, podatke na svjetlosnom kanalu interpretira sam čovjek (putem vida). Specifičnim kodiranjem svjetlosnog kanala postigli smo to da se čovjekova zadaća svede na jednostavnu usporedbu stanja LED dioda na M2M uređajima. Ova metoda ima minimalne hardverske zahtjeve na strani M2M uređaja: jedna LED dioda. S druge strane, ista ne skalira dobro s brojem M2M uređaja kao prethodne dvije metode.

4.2 GreenAE: energetski efikasna autentifikacijsko-enkripcijska metoda

U ovoj sekciji istražujemo mehanizme koji osiguravaju povjerljivost, cjelovitost (integritet) i autentičnost podataka u M2M komunikacijama. Pri tome stavljamo naglasak na sigurnosne mehanizme koji su karakterizirani malom potrošnjom energije i malim memorijskim zahtjevima. Ovo su vrlo važne karakteristike budući da će M2M uređaji tipično imati ograničene hardverske i baterijske resurse.

Najpoznatije suvremene metode za osiguravanje povjerljivosti i autentičnosti jesu **autentifikacijsko-enkripcijski (AE)** algoritmi (modovi rada): CCM (*Counter with CBC-MAC*) [20] i OCB (*Offset Codebook Mode*) [21]. CCM se koristi za zaštitu WLAN mreža (IEEE 802.11i) i WPAN mreža (IEEE 802.15.4), a OCB se navodi kao alternativa. CCM i OCB su autentifikacijsko-enkripcijske metode, što znači da istovremeno osiguravaju povjerljivost i autentičnost podataka.

CCM (*Counter with CBC-MAC*) enkriptira podatke u tzv. CTR (*counter*) načinu rada, dok se autentičnost osigurava standardnim CBC-MAC algoritmom. Dakle, za svaki podatkovni blok koji treba zaštititi, CCM dva puta poziva/izvršava korištenu blok šifru (AES). S obzirom da radi u CTR modu, CCM koristi samo enkripcijski smjer AES šifre za postupak enkripcije i dekripcije podataka.

S druge strane, **OCB (*Offset Codebook Mode*)** je iznimno efikasna metoda zaštite podataka kod koje se svaki podatkovni blok provlači samo jednom kroz blok šifru (npr. AES). OCB istovremeno (u jednom prolazu preko podataka) osigurava i povjerljivost i autentičnost podataka. Za razliku od CCM moda, OCB koristi oba smjera blok šifre enkripcijski i dekripcijski. Osim toga, kod OCB moda blokovi se mogu enkriptirati i dekriptirati neovisno jedni o drugima – paralelno. Još jedna važna razlika između dva AE moda rada jest činjenica da je CCM otvoren za korištenje svima, dok je korištenje OCB ograničeno patentnim/licencnim pravima.

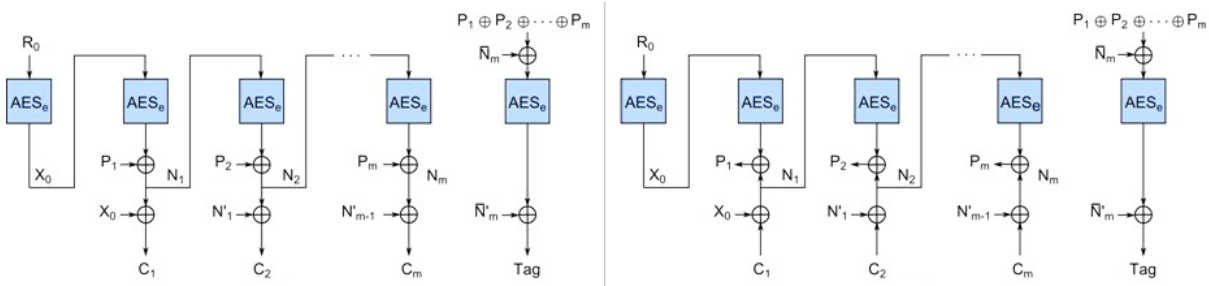
Naša preliminarna studija dviju popularnih AE metoda pokazuje da iste nisu optimalni izbor za primjenu u M2M uređajima ograničenih resursa [19]. Ovdje smo razmatrali sljedeće kriterije optimalnosti: energetska efikasnost, memorijski zahtjevi te licencna prava. Na osnovu ove analize, predložili smo alternativnu, novu autentifikacijsko-enkripcijsku (AE) metodu **GreenAE** koja kombinira najbolje karakteristike CCM i OCB metoda, dok odbacuje one koje nisu relevantne za M2M sustave, kako je prikazano u tablici 2.

Tablica 2: Osnovne karakteristike GreenAE metode

	"one-pass" (energija)	samo AES enkripcijski smjer (energija i memorija)
CCM	Ne	Da
OCB	Da	Ne
Green AE	Da	Da

Kao što je vidljivo iz tablice 2 (i slike 11), GreenAE metoda enkriptira svaki podatkovni blok samo jednom (one-pass metoda), slično OCB modu. Na ovaj način se štedi energija zbog brže enkripcije. S druge strane, slično CCM modu, GreenAE koristi samo enkripcijski smjer primijenjene blok šifre (AESe na slici 11). Ovo je vrlo važan aspekt predložene metode u slučaju AES-a. Naime, AES je nesimetrična blok šifra, što znači

da AES enkripcija i AES dekripcija nisu identične radnje. Važnije, AES dekripcija je kompleksnija od AES enkripcije; ovisno o implementaciji dekripcijski smjer troši 20-30% više energije [19]. Zahvaljujući ovoj karakteristici, osim manje potrošnje, GreenAE zahtjeva i manje memorije za pohranu AES šifre (pohranjuje se samo AES enkripcijski algoritam). S negativne strane, GreenAE enkripcijska metoda ne može se paralelizirati (kao što je to slučaj sa OCB metodom). Međutim, ovaj kompromis je opravdan s obzirom na prirodu M2M komunikacija koju karakterizira povremena razmjena male količine podataka (nije potrebno podržati visoke brzine prijenosa , npr. Gbps).



Slika 11: GreenAE metoda: (a) enkripcijski smjer, i (b) dekripcijski smjer.

Detalji GreenAE enkripcijske metode prikazani su na slici 11. $P_1,P_2,..P_n$ su podatkovni blokovi (poruka) za koje treba osigurati povjerljivost i autentičnost. $C_1,C_2,..C_n$ su odgovarajući šifrirani blokovi, Tag je autentifikacijski string, R_0 je slučajni broj (*random nonce*), dok je N'_i ekvivalentan N_{i-1} rotiran ulijevo za 1. Pošiljatelj emitira slijedeću poruku ($R_0,C_1,C_2,..C_n$,Tag), koju primatelj dekriptira dijeljenim tajnim AES ključem i provjerava njenu autentičnost koristeći autentifikacijski string *Tag*. U [19] detaljno analiziramo sigurnost GreenAE metode i diskutiramo načine njene efikasne primjene te konkretno pokazujemo kako se može amortizirati trošak slanja slučajnog broja R_0.Opisani su i drugi mehanizmi uštede energije kao npr. *Green Encryption/Decryption Engine*.

5 Zaključak

Dan je pregled aktivnosti vezanih uz sigurnost u budućim M2M sustavima. Najprije su predstavljene osnovne sigurnosne prijetnje i njihove implikacije: izloženost M2M uređaja fizičkim napadima, ugrožavanje dostupnosti uređaja (npr. radio ometanjem), maliciozna zagušenja transportnih mreža, narušavanje privatnosti M2M korisnika te narušavanje povjerljivosti i autentičnosti podataka. Motivirani vizijom o 50 milijardi M2M uređaja do 2020. godine, alijansa 3GPP i standardizacijski institut ETSI pokrenuli su snažne standardizacijske aktivnosti koje između ostalog pokrivaju i sigurnosnu problematiku. Pri tome je 3GPP usko fokusiran na M2M komunikacije putem isključivo mobilnih celularnih mreža, dok ETSI definira generalnu sistemsku arhitekturu za podršku M2M sustavima, neovisno o transportnim mrežama. Obije grupe poseban naglasak stavljaju na sigurnost procesa daljinske administracije M2M uređaja, njihove fizičke sigurnosti, osiguravanje komunikacijskih kanala između domene M2M uređaja i mrežne domene. Karakter većine predloženih rješenja je primjena provjerenih sigurnosnih mehanizama poimenice GBA, AKA, OTA, ISIM i drugih iz sfere mobilnih mreža, odnosno TLS, EAP, PANA i drugih iz sfere IP i web sigurnosti. Važno je naglasiti da postojeće 3GPP i ETSI tehničke specifikacije ne pokrivaju lokalnu komunikaciju između M2M uređaja (tzv. *M2M Area Network*). Tu problematiku rješavaju, ali samo djelomično, standardi kao što su IEEE802.15.1, IEEE802.15.4, Zigbee, ISA 100.11a i drugi.

Konačno, u radu smo opisali neke od naših aktivnosti u području M2M sigurnosti. Konkretno, predstavili smo nekoliko mehanizama za jednostavnu i sigurnu inicijalizaciju velikih M2M mreža, kao i novu autentifikacijsko-enkripcijsku metodu GreenAE. Naša rješenja imaju odlike energetske učinkovitosti, jednostavnosti uporabe za krajnjeg korisnika te, kao najvažnije, sigurnosti.

6 Literatura

[1] D. Boswarthick, O. Elloumni and O. Hersent, “M2M Communications: A System Approach”, First Edition, John Wiley & Sons, (2012).

[2] ETSI, “Machine to Machine Communications”, presentation at Mobile World Congress, Barcelona, (2011). Available at http://www.etsi.org

[3] A. Walter-Krisch, “Heading towards 50 billion connections”, Ericsson, (Feb. 2011). Available at www.ericsson.com

[4] T. Taleb and A. Kunz, “Machine Type Communications in 3GPP Networks: Potential, Challenges, and Solutions”, IEEE Communications Magazine, (Mar. 2012).

[5] ETSI TS 102 690, “Machine-to-Machine communications (M2M); Functional architecture”, (Oct. 2011).

[6] ETSI TS 102 921, “Machine-to-Machine communications (M2M); mla, dla and mld interfaces”, (Feb. 2012).

[7] 3GPP TR 33.812, “Feasibility study on the security aspects of remote provisioning and change of subscription for Machine to Machine (M2M) equipment”, (Apr. 2010).

[8] 3GPP TR 33.868, “Security aspects of Machine-Type Communications”, (2011).

[9] Signal Jammer, http://shopsignaljammer.com, (May 2012).

[10] Gemalto, “OTA (Over-The-Air) ”, http://www.gemalto.com/techno/ota, (May, 2012).

[11] D. Perez and J. Pico, “A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communications”, Black Hat DC (2011).

[12] C. V. Wright, L. Ballard, F. Monrose and G. M. Masson, “Language identification of encrypted VoIP traffic: Alejandra y Roberto or Alice and Bob”, 16th Usenix Security Symposium, (2007).

[13] 3GPP TS 33.220, “Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)”, (2012).

[14] A. Niemi, J. Arkko, and V. Torvinen, “Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)”, IETF RFC 3310 (Sep. 2002).

[15] B. Aboba et al., “Extensible Authentication Protocol (EAP)”, IETF RFC 3748, (Jun. 2004).

[16] V. Fajarado, Y. Ohba, and R. Marin-Lopez, “State Machines for Protocol for Carrying Authentication for Network Access (PANA)”, IETF RFC, (Aug. 2009).

[17] R. Lu et al., “GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications”, IEEE Communications Magazine, (2011).

[18] T. Perković, I. Stančić, L. Mališa, and M. Čagalj, “Multichannel Protocols for User-friendly and Scalable Initialization of Sensor Networks”, 5th Int. ICST Conference on Security and Privacy in Comm. Networks (Securecomm), (2009).

[19] M. Čagalj, “Bootstrapping and Securing Next-Generation M2M Networks”, Project report – Ericsson Nikola Tesla, (Dec. 2011).

[20] D. Whiting, R. Housley, and N. Ferguson, “Counter with CBC-MAC (CCM)”, IETF RFC 3610, (Sep. 2003).

[21] P. Rogaway, M. Bellare, and John Black, “OCB: A block-cipher mode of operation for efficient authenticated encryption”, ACM Transactions on Information and System Security, (Aug. 2003).

7 Popis kratica

3GPP	3rd Generation Partnership Project
AE	Authenticated-Encryption

AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
CCM	Counter with CBC-MAC
D/G M2M	Device/Gateway M2M
DoS	Denial-of-Service
DSEC	M2M Device Security Capability
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data rates for GSM Evolution
ETSI	European Telecommunications Standards Institute
GBA	Generic Bootstrapping Architecture
GEA	GPRS Encryption Algorithm
GPRS	General Packet Radio Service
HLR	Home Location Register
IMSI	International Mobile Subscriber Identity
IPSec	Internet Protocol Security
ISIM	IP Multimedia Services Identity Module
LAN	Local Area Network
LED	Light-Emitting Diode
M2M	Machine-to-Machine
MAS	M2M Authentication Server
MCIM	Machine Communication Identity Module
MitM	Man-in-the-Middle
MNO	Mobile Network Operator
MSFB	M2M Service Bootstrap Function
MTC	Machine Type Communication
NDS/IP	Network Domain Security/IP network security
NSEC	M2M Network Security Capability
OCB	Offset Codebook Mode
OTA	Over-The-Air programming
OTP	One Time Password
PAN	Personal Area Network
PANA	Protocol for Carrying Authentication for Network Access
SAS	Short Authentication String
SIM	Subscriber Identity Module
TLS/TCP	Transport Layer Security/Transmission Control Protocol
TRE	Trusted Enviroment
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module

Adresa autora:

Mario Čagalj
e-mail: mario.cagalj@fesb.hr

Sveučilište u Splitu, FESB
R. Boškovića 32
HR-21000 Split
Hrvatska

Uredništvo je primilo rukopis 21. svibnja 2012.

Marko Lukičić

Ericsson Nikola Tesla d.d., Zagreb, Hrvatska
Ericsson Nikola Tesla d.d., Zagreb, Croatia

M2M KOMUNIKACIJE U PRIMJENI NAPREDNIH ELEKTROENERGETSKIH MREŽA

M2M COMMUNICATIONS IN SMART GRIDS

Sažetak

Iako su na prvi pogled dva nespojiva područja, energetika i komunikacije svakako konvergiraju k istoj paradigmi s ciljem ostvarenja danas još uvijek uglavnom konceptualnih modela, poput naprednih elektroenergetskih mreža (Smart grid), ali i inteligentnih gradova, zgrada, kućanstava i drugog. Pri tome komunikacija među strojevima (Machine-to-Machine - M2M), odnosno uređajima, kao nova vrsta komunikacije, predstavlja komunikacijsku okosnicu za preobrazbu spomenutih konceptualnih modela, ali i pilot projekata u njihovu stvarnu realizaciju i širu primjenu.

Ovaj rad daje osvrt na M2M vrstu komunikacije i njene ključne razlike u odnosu na dosadašnju, tradicionalnu komunikaciju usmjerenu ka čovjeku. Kroz identifikaciju ključnih domena naprednih elektroenergetskih mreža, razmotrena je primjena M2M komunikacije za svaku od domena zasebno i predložena arhitektura inteligentnog upravljanja elektroenergetskom ili komunalnom mrežom zasnovana na M2M vrsti komunikacije.

Abstract

Although at first glance it may look like two completely incompatible areas, energy and communications surely converge to the same paradigm – the paradigm of smart grids. Communications between machines (Machine-to-Machine - M2M), or devices - as a new type of communication – is the foundation for the implementation and wider application of smart grids (including smart metering, smart cities, smart buildings, smart homes, etc.).

This paper provides an overview of the M2M communications. Key differences from the previous, traditionally man-focused communications, is given as well. Through the identification and characterization of key smart grid domains, the application of M2M communications in smart grids is considered and an architecture of smart metering based on M2M communications proposed.

KLJUČNE RIJEČI:	KEY WORDS:
M2M komunikacija	M2M communication
Napredne elektroenergetske mreže	Smart grids
Konceptualni model	Conceptual model

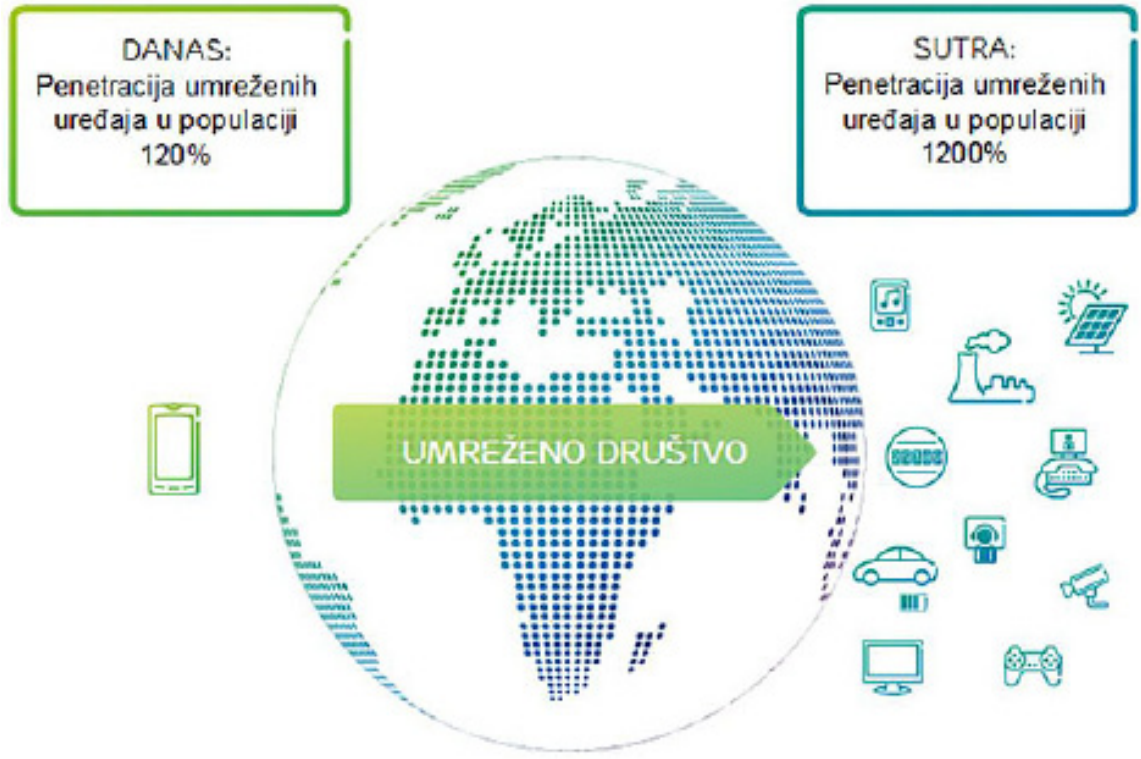
1 Uvod

Uspostavom globalne telekomunikacijske pokrivenosti, završena je velika faza tehnološkog razvoja civilizacije. Sada, kada bismo se retrospektivno osvrnuli na njen završetak, mogli bismo reći je tu fazu moguće obilježiti jednom riječi: pokrivenost. U telekomunikacijskom kontekstu, pokrivenost će podrazumijevati geografsko područje unutar kojega stanice mogu komunicirati konzumiranjem telekomunikacijskih usluga poput nepokretne telefonije, mobilne telekomunikacije, širokopojasnih usluga i plaćenih TV (pay TV) usluga, podatkovnih usluga i drugog.

Iako u ovim počecima ne izrazito primjetno, ali sasvim sigurno, uspostavom globalne pokrivenosti nedavno su potaknuti novi razvojni smjerovi koji već oslikavaju blago prepoznatljive konture nove faze tehnološkog razvoja. Uzimajući u obzir zajedničke dimenzije u kojima ti smjerovi egzistiraju, moguće je prepoznati povezivost i upravljivost (uz adekvatnu sigurnost) kao ključna obilježja nove faze tehnološkog razvoja civilizacije.

Povezivost se u prvome redu nadovezuje na pokrivenost. Bitno je napomenuti da je povezivost na elementarnoj razini već postignuta prošlom fazom, s jedne strane razvojem mobilnih komunikacijskih uređaja, tablet računala i drugih uređaja, a s druge strane razvojem komunikacijskih rješenja poput, u prošlom broju Revije predstavljenog Ericssonovog Business Communication Suita. Ipak, primjetno je da ovakva povezivost, u prvome redu ,stavlja čovjeka u ulogu sudionika u komunikaciji.

Kada se govori o povezivosti u okviru nove faze razvoja onda bi se za potrebe razlikovanja njenog shvaćanja u odnosu na prethodnu faze mogao iskovati termin Povezivost2.0 koji iza sebe skriva zanimljiv trend: iskorak od mobilnog interneta prema ugradbenom internetu (slika 1). Naime, Ericsson procjenjuje da će do 2020. godine u svijetu postojati 50 milijardi umreženih uređaja. Drugim riječima, sve što će imati koristi od povezivosti, to će do 2020. godine i biti povezano. Ovakva, sveobuhvatnija povezivost ne isključuje čovjeka kao sudionika u komunikaciji već, dapače, generalizira definiciju sudionika u komunikaciji na način da ona sada obuhvaća sve što može biti povezano (osim ljudi i vozila, medicinske i druge osjetnike, uređaje za zabavu, strojeve, alate, postrojenja, kućanske alate i drugo).



Slika 1: Od mobilnog interneta prema ugradbenom internetu.

Ovakvom generalizacijom definicije sudionika u komunikaciji, stavljen je novi izazov pred novu razvojnu fazu. Ukoliko u nekoj komunikaciji sudjeluje barem jedan sudionik zasnovan na siliciju, tada će se ostvariti puni

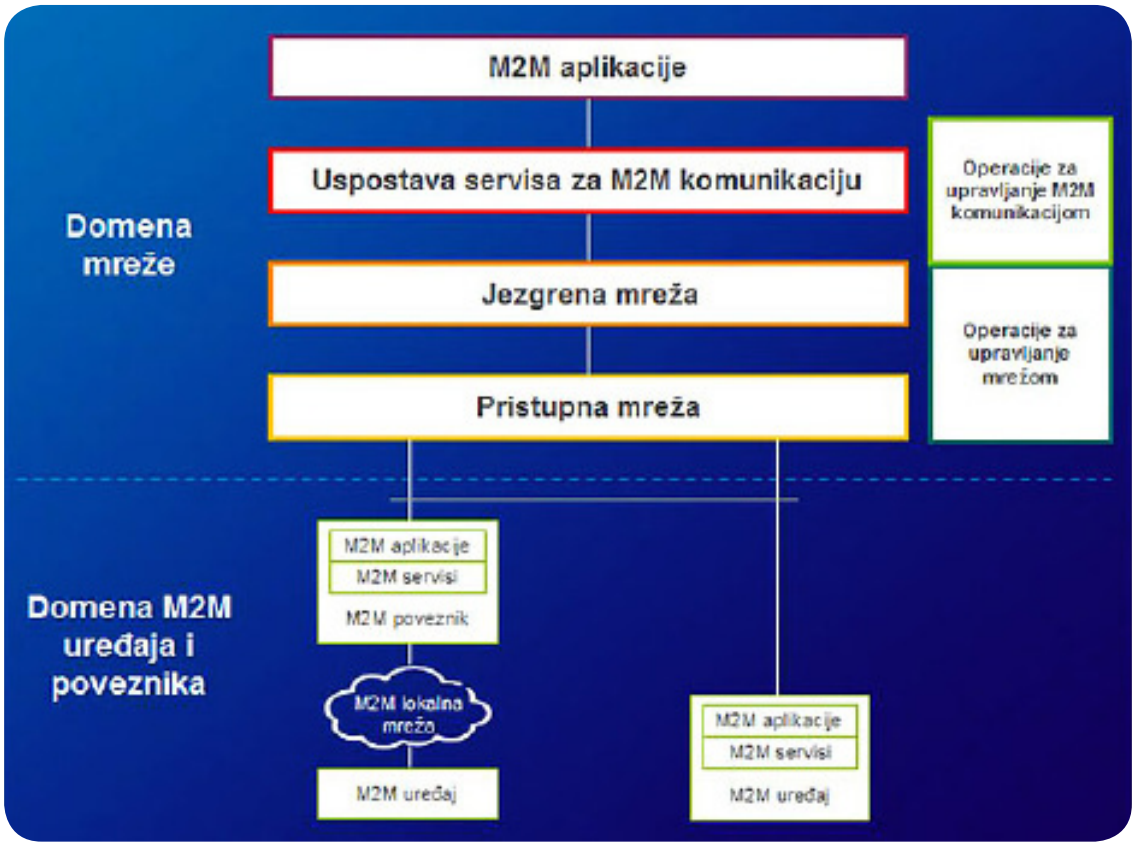
potencijal uspostavljene komunikacije tek ukoliko je ta komunikacija nadograđena sigurnim servisima za upravljanje tim sudionikom. Ovaj kritičan zahtjev postavljen pred povezivost iziskuje u prvome redu uspostavu standardiziranih servisa te potpornih protokola i tehnologija za udaljeno upravljanje uređajem, odnosno sudionikom, ali i za upravljanje uređajem kao pretplatnikom u samoj telekomunikacijskoj mreži.

Kompanija Ericsson Nikola Tesla je rano prepoznala razvojne smjerove nove faze tehnološkog razvoja te ih je podržala inovativnim rješenjima poput Ericsson Mobile Health sustava za udaljeni nadzor pacijenata, sudjelovanjem u međunarodnim projektima poput europskog HeERO pilot projekta čiji je cilj unaprjeđenje prometne i javne sigurnosti putem telekomunikacijske usluge e-Poziva, i brojnim drugim aktivnostima. U isto vrijeme, malo bi bilo reći da je i Ericsson korporacija prepoznala rane konture nove faze razvoja, već ona sudjeluje u njenom oblikovanju inovativnim rješenjima poput Device Connection Platforme, rješenja za uspostavu M2M komunikacije, povezivosti temeljenog na računarstvu u oblaku i drugih.

2 Machine-to-Machine komunikacija

S obzirom na činjenicu da u svijetu postoji mnogo više strojeva (pod strojem se u kontekstu M2M komunikacije podrazumijeva bilo koja stvar s mehaničkim, elektroničkim ili električnim značajkama koja sudjeluje u komunikaciji) nego ljudi i isto toliko puta više potencijalnih dodatnih vrijednosti od njihova međupovezivanja, zadnjih je godina M2M vrsta komunikacije pridobila pažnju pružatelja telekomunikacijskih usluga. Uspostavom M2M komunikacije omogućuje se međupovezivanje, umrežavanje i udaljeno upravljanje strojevima uporabom već pristupačnih, skalabilnih i pouzdanih tehnologija. Na temelju takve povezivosti, pružatelji telekomunikacijskih usluga mogu ponuditi nove usluge poput udaljenog očitavanja potrošnje električne energije i upravljanja energetskom učinkovitosti domaćinstava.

Za razliku od čovjek-prema-čovjeku vrste komunikacije, koja uglavnom uključuje glasovnu komunikaciju, poručivanje i pristup Internetu, M2M komunikacija zamišljena da povećava efikasnost i smanjuje troškove, prije svega povećanjem razine automatizacije razmijene i dijeljenja podataka između strojeva i pozadinskih potpornih sustava. Upravo će stoga uspostava standardiziranih servisa te potpornih protokola i tehnologija predstavljati glavne izazove u uspostavi nesmetanih tokova podataka u M2M komunikaciji [1].



Slika 2: Komponente arhitekture sustava za uspostavu M2M komunikacije (ETSI).

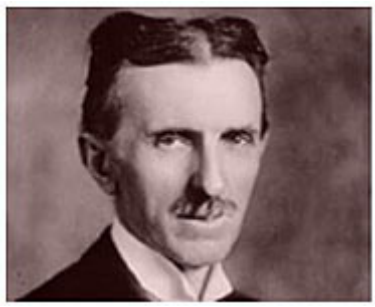
Europski institut za telekomunikacijske standarde (European Telecommunications Standards Institute - ETSI) predlaže sljedeće komponente arhitekture sustava za uspostavu M2M komunikacije (slika 2) [2]:

- M2M uređaj koji kroz vlastitu M2M aplikaciju koristi M2M servise iz sloja za uspostavu M2M usluga,
- M2M lokalna mreža za osiguranje povezivosti između M2M uređaja i M2M poveznika (Karakteristične tehnologije za uspostavu M2M lokalne mreže su: WiFi, bluetooth, IC…),
- M2M poveznik kao posrednik između M2M uređaja i mrežne domene (Poveznik može ostvarivati specifične funkcionalnosti za upravljanje M2M uređajima na operativnoj razini poput provjere statusa pojedinog M2M uređaja, ponavljanja upita upućenog M2M uređaju u slučaju izostanka odgovora, i drugo.),
- pristupna mreža koja dozvoljava domeni M2M uređaja i poveznika komunikaciju s jezgrenom mrežom. (Tipični primjeri pristupne mreže su: xDSL, HFC, satelit, GERAN, UTRAN, eUTRAN, W-LAN, WiMAX…),
- jezgrena mreža koja putem IP ili drugih protokola osigurava upravljanje mrežom i uslugama, povezivanje s drugim mrežama, roaming (uporaba uređaja u tuđim mrežama), kontrolu kvalitete usluge i drugo,
- uspostava servisa za M2M komunikaciju (sustav koji, putem otvorenih sučelja za programiranje, pruža zajedničke funkcionalnosti i usluge M2M aplikacijama),
- M2M aplikacije putem kojih se krajnjim korisnicima pružaju specifične usluge zasnovane na M2M komunikaciji.

S obzirom na svoju namjenu da osigura povezivost u sveobuhvatnom smislu te riječi, platforme za uspostavu M2M komunikacije postaju neizostavna komponenta za povezivanje bilo kojeg uređaja za koji postoji potreba za komunikacijom s drugim uređajima.

3 M2M komunikacija u inteligentnim elektroenergetskim mrežama

Tradicionalne, postojeće nacionalne elektroenergetske infrastrukture građene su na principima i modelima predviđanja potražnje za električnom energijom koji datiraju još iz 19. stoljeća kada su, temeljem radova u kojima Nikola Tesla opisuje izmjeničnu struju te principa rada indukcijskih motora, izgrađene prve elektrane izmjenične električne struje [4,5]. Iako su te infrastrukture godinama zadovoljavale naše potrebe, porast potražnje za električnom energijom je činjenica koja tu infrastrukturu gura prema njezinim limitima te svakodnevno povećava vezane rizike u njihovoj veličini, broju i složenosti. Predviđanja pokazuju da će se ukupna svjetska potrošnja električne energije u periodu od 2008. godine do 2035. godine povećati za 53 posto. (prema International Energy Outlook 2011, U.S. Energy Information Administration) [3].Nedavna su zamračenja Americi [6] i Italiji [7] ukazala da nemogućnost ocjene i razumijevanja stanja elektroenergetskog sustava te kašnjenje u provođenju odgovarajućih korektivnih akcija nakon manjeg ispada u distribuciji električne energije, može dovesti do masovnog zamračenja. Iako se procjenjuje da su današnji energetski sustavi 99,97 posto pouzdani, ispadi u dostavi električnom energijom još uvijek, samo u Americi, uzrokuju i godišnji trošak u iznosu od 150 milijardi dolara (oko 500 dolara na svakog muškarca, ženu i dijete) [8].



Na kraju krajeva, ova centrala i nije tako važna. Ona je samo praktična primjena teorija koje već dugo poznajemo. Umjesto da si čestitamo trebali bismo se sramiti što je nismo sagradili prije. Pravi je posao tek pred nama. Moramo savladati udaljenost, osjetila registriraju samo ono što je u blizini.

Dodatne izazove pred energetske infrastrukture stavljaju i potrošači. U svojim nastojanjima da iskoriste sav potencijal koristi koje im nude sustavi poput električnih automobila, pametnih kuća i drugi, ali i da svoju poziciju u energetskom sustavu učine mnogo aktivnijom mijenjajući pri tome svoju ulogu s tradicionalnog potrošača na dinamičkog potrošača-proizvođača, potrošači očekuju odgovarajuću tehnološku i operativnu podršku distributera električnom energijom. Oni ne očekuju više da će im potrošena električna energija biti naplaćena, nego da će im se i proizvedena električna energija dana u elektroenergetsku mrežu platiti po unaprijed reguliranim i dogovorenim tarifama.

I konačno, bitno je spomenuti europski trend deregulacije energetskog sektora kojim države, u nastojanju da de-monopoliziraju i uspostave konkurentno energetsko tržište, iziskuju od aktera u energetskom tržištu od uspostave novih poslovnih modela pa sve do eventualnih prilagodbi pripadajućih elektroenergetskih infrastruktura [9,10,11].

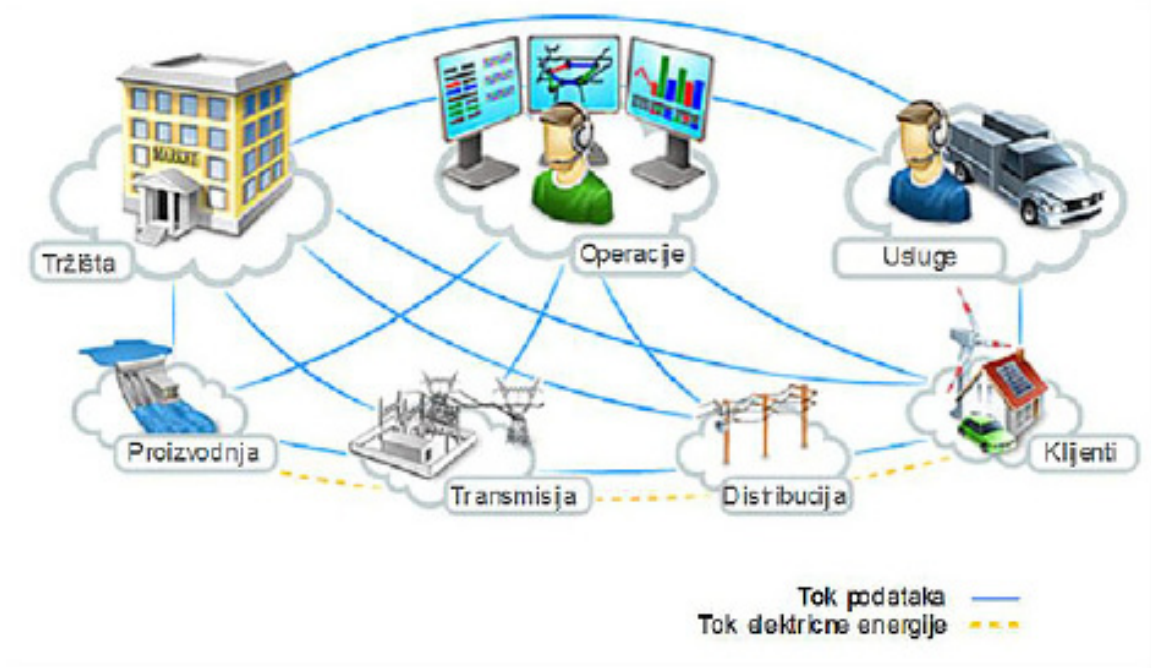
Rješavanje svih navedenih izazova vodi ka spajanju principa i koncepata dva izuzetna čovjeka koji su uprli temelje kako u energetici, tako i u komunikacijama: Nikole Tesle i Larsa Magnusa Ericssona. Upravo iz objedinjavanja njihovih vizija proizlazi modernizacija energetskog sustava postavljanjem u mrežu aktivnih elemenata za daljinsko praćenje i upravljanje elektroenergetskim sustavom te tokovima i potrošnjom električne struje, a s konačnim ciljem uspostave inteligentne mreže (Smart Grid) sposobne za adaptivnu i optimalnu proizvodnju, transmisiju, distribuciju i potrošnju električne energije.

Napredne elektroenergetske mreže su primjer primjene M2M komunikacije koja se provodi osjetnicima i drugim aktivnim elementima instrumentalizirane elektroenergetske mreže, a kojima se upravlja i u stvarnom vremenu prati niz pokazatelja energetskog sustava poput potrošnje električne energije, gubitaka u distribuciji električnom energijom, ispada u distribuciji, radnog učinka pojedinih dijelova mreže i mnogih drugih. Ti elementi, povezani u komunikacijsku mrežu s operativnim sustavima podrške, omogućuju slanje informacija u centralni informacijski sustav te nadzor i upravljivost cjelovitom elektroenergetskom mrežom sa jednog mjesta. Posjedovanje tih podataka u operativnim sustavima podrške će omogućiti uštede u proizvodnji, transmisiji, distribuciji i potrošnji električne energije, a daljnja integracija tih sustava s poslovnim sustavima podrške i postizanje veće poslovne efikasnosti te poboljšanje kvalitete usluga.

4 Konceptualni model inteligentnog upravljanja energetskom mrežom

Institut inženjera elektrotehnike i računarstva (Institute of Electrical and Electronics Engineers - IEEE, www.ieee.org) i Američki nacionalni institut za standarde i tehnologije (National Institute of Standards and Technology - NIST, www.nist.gov) zajedničkim su naporima pokrenuli razvoj tehnoloških standarda za uspostavu naprednih elektroenergetskih mreža [12,13]. Ti dokumenti sadrže konceptualni model naprednih elektroenergetskih mreža zasnovan na sljedećim domenama:

- masovna proizvodnja,
- transmisija,
- distribucija,
- klijenti,
- usluge,
- operacije,
- tržišta.



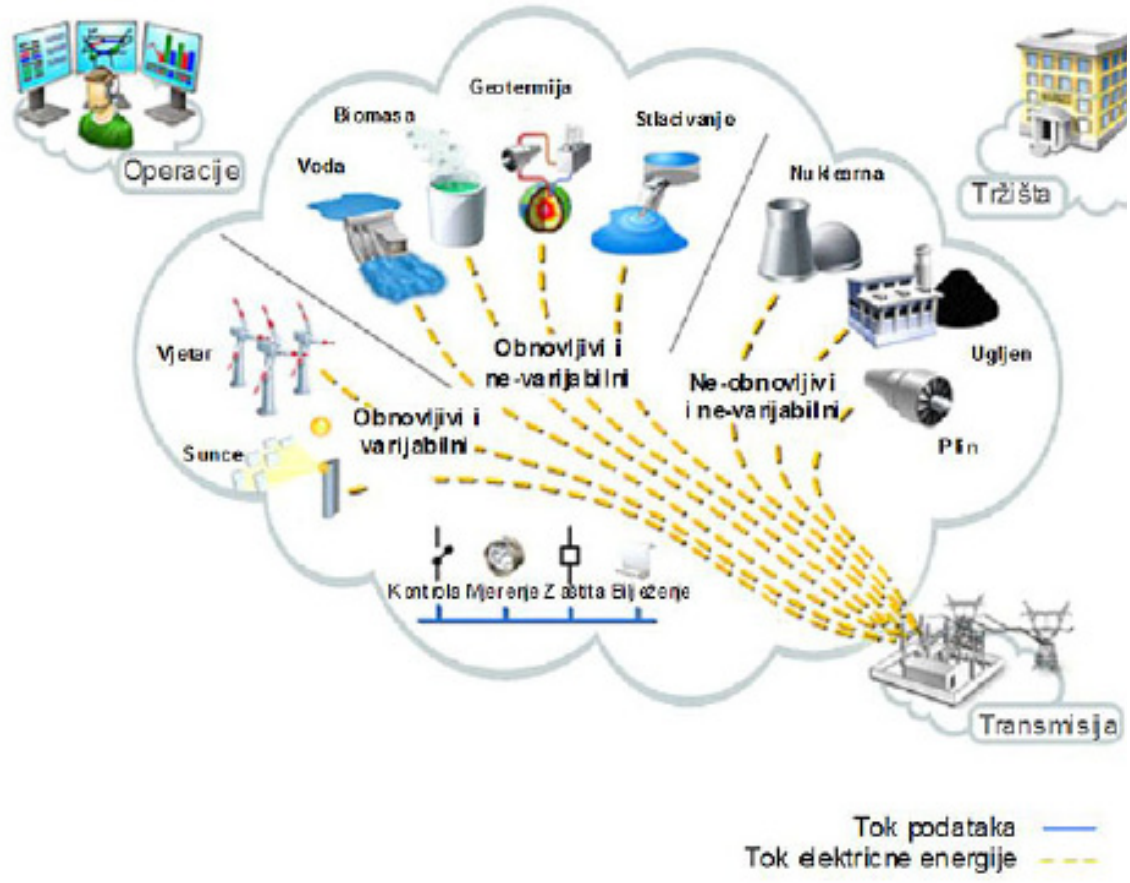
Slika 3: Konceptualni model inteligentnih energetskih mreža.

Slika 3 prikazuje tokove električne energije i uspostavljene komunikacijske kanale za razmjenu informacija među domenama okvirnog modela naprednih elektroenergetskih mreža. Svaka od domena sadrži odgovarajuće aktivne elemente napredne elektroenergetske mreže međusobno povezane dvosmjernim M2M komunikacijskim vezama i energetskim tokovima. IEEE dalje svaku od domena, koju predlaže NIST, detaljizira na fundamentalnim razinama: razini energije, komunikacijskoj razini i informacijsko-informatičkoj razini.

4.1 Masovna proizvodnja električne energije

Domenu masovne proizvodnje električne energije u prvom redu čine veliki generatori. S obzirom na dostupne izvore, dijelimo ih na generatore obnovljive i ne-obnovljive energije, a s obzirom na kontinuitet na varijabilne i ne-varijabilne (slika 4). Tipični obnovljivi varijabilni izvori energije su vjetar i sunce. Obnovljivim i nevarijabilnim izvorima se smatraju voda, biomasa, geotermija i stlačivanje, a neobnovljivim i nevarijabilnim nuklearno gorivo, ugljen i plin.

Bitna karakteristika naprednih elektroenergetskih mreža je mogućnost trenutačnog odgovora proizvodnje električne energije na trenutačnu potražnju i visoka preciznost u predviđanju buduće potražnje za električnom energijom. Faktori poput godišnjih doba, klimatskih promjena, vikenda i praznika, katastrofa, političkih uzroka različitih operativnih scenarija i kvarova bitno će utjecati na trenutačnu proizvodnju kao i na predviđanje potrošnje električne energije [14]. Od 90tih godina prošloga stoljeća se umjetne neuronske mreže, primjenom faktora poput ranije navedenih [15], uspješno primjenjuju u predviđanju potražnje električne energije.



Slika 4 – Domena masovne proizvodnje električne energije.

Za provođenje trenutačne prilagodbe proizvodnje u skladu s potražnjom električne energije i predviđanje buduće potražnje za električnom energijom potrebno je pojednostaviti, ubrzati i učiniti što efikasnijim upravljanje cjelokupnom masovnom proizvodnjom električne energije. To se, prije svega, postiže centraliziranim upravljanjem proizvodnjom električne energije kroz uspostavu četiri temeljna potporna mehanizma. Mehanizam za kontrolu proizvodnje osigurava praćenje pokazatelja poput radnog učinka

pojedinog generatora energije. Ti pokazatelji daju informaciju o korištenim kapacitetima, ali i opterećenjima pojedinih pogona te time olakšavaju odlučivanje prilikom prilagodbe proizvodnje električne energije ili preusmjeravanja proizvodnje s jednog generatora na drugi. Trenutačnu razliku između potražnje i proizvodnje osigurava mehanizam za mjerenje. No, isti mehanizam je iskoristiv za i procjenu i praćenje gubitaka u proizvodnji te identifikaciju kvarova. Upravo u slučajevima kvarova će zaštitni mehanizmi biti od presudne važnosti u lokalizaciji kvarova i sprečavanju njihova širenja i potencijalnih katastrofa. I konačno, mehanizam za bilježenje stanja cjelokupnog sustava proizvodnje će kontinuirano nuditi dragocjene podatke za daljnju analitiku s ciljem optimizacije i razvoja domene proizvodnje električne energije.

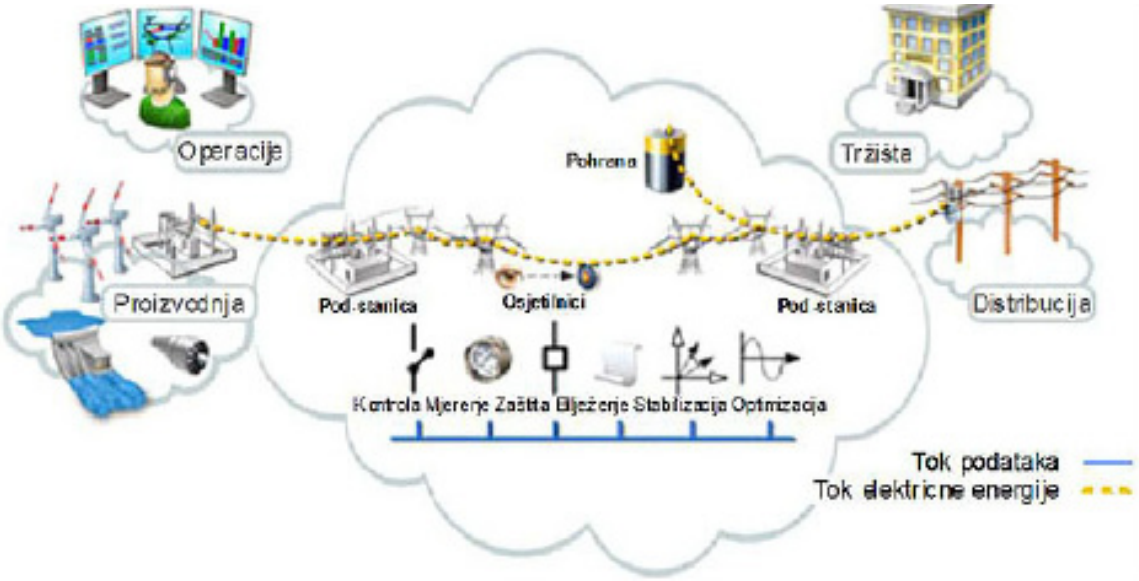
Svi navedeni mehanizmi imaju istu infrastrukturnu pretpostavku za njihovu realizaciju: uspostavljenu komunikaciju između aktivnih i pasivnih elemenata elektrana (poput osjetnika ali i kompresora, rotora, turbina, kondenzatora, generatora pare, vodocijevnog sustava i drugog) i centralnog sustava za nadgledanje i upravljanje cjelokupnom domenom. Platforma za M2M komunikaciju će osigurati komunikaciju s tim uređajima. Dok će s jedne strane omogućiti praćenje i operativno upravljanje uređajima, poput jednostavnog dodavanja i aktiviranja novog ili deaktiviranja postojećeg uređaja bilo gdje u domeni masovne proizvodnje električne energije, s druge će strane ista platforma integracijom omogućiti pristup prikupljanim podacima i operativno te poslovno upravljanje uređajima kroz operativne i poslovne sustave podrške proizvođača električne energije. Sada se, slijedom ispunjene infrastrukturne pretpostavke, uspostavljaju temeljni potporni mehanizmi a time i centralizirano mjesto za trenutačnu prilagodbu proizvodnje potražnji za električnom energijom te precizno predviđanje i planiranje buduće potražnje za električnom energijom.

4.2 Transmisija

Domena transmisije električne energije je zadužena za masovni prijenos električne energije na velike udaljenosti putem transmisijskih prijenosnih linija. Domena transmisije povezuje masovnu proizvodnju električne energije s centrima potrošača energije napredne elektroenergetske mreže. Osnovne komponente domene su transformatorske stanice, rasklopna prijenosna postrojenja te zračni vodovi i kabeli. U kontekstu naprednih elektroenergetskih mreža, svakako su sastavni dio domene transmisije i pogoni za privremeno skladištenje energije i drugi alternativni distribuirani izvori energije.

Temeljni mehanizmi prisutni u masovnoj proizvodnji električne energije su, u njihovom općenitom smislu, prisutni i u domeni transmisije (slika 5). Ipak, uz njih postoje još dva mehanizma za stabilizaciju i optimizaciju čija je osnovna zadaća:

- angažiranje proizvodnih objekata u području transmisije i aktivacija spojnih vodova s drugim mrežama,
- osiguravanje energije za pokriće gubitaka u prijenosnoj mreži i energije za uravnoteženje,
- kontinuitet i pouzdanost sustava opskrbe električnom energijom te ispravna koordinacija sustava proizvodnje, prijenosa i distribucije, te
- održavanje parametara kvalitete električne energije.

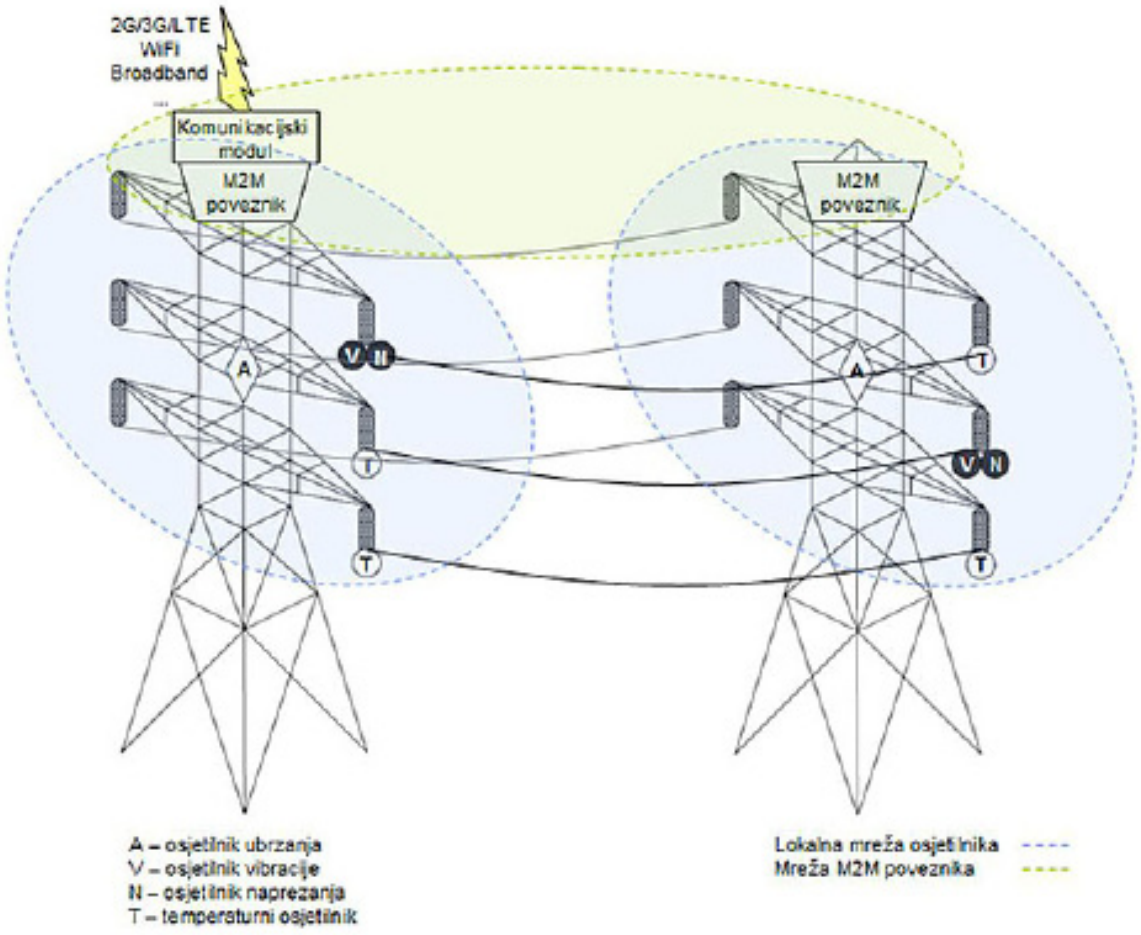


Slika 5: Transmisija električne energije.

Danas postoji niz razvijenih i dostupnih osjetnika i drugih aktivnih i pasivnih elemenata koji su u stanju pratiti mehaničke varijable, prije svega prijenosnih linija ali i ostalih komponenata domene transmisije. Temeljem tih varijabli je moguće predvidjeti i identificirati iznimne uvjete rada uzrokovane pojavama poput meteoroloških događaja te slučajnih ili namjernih infrastrukturnih oštećenja.

Obzirom da potporna infrastruktura vodova i kablova koristi slične građevinske karakteristike kao zgrade, predlaže se uporaba osjetnika iz iste aplikativne domene koji su na temelju pokazatelja, poput ubrzanja, naprezanja i pomaka, u stanju pružiti odgovarajuću razinu osmotrivosti sustava za potrese, nalete vjetra i druge događaje [16,17]. Aplikacijom temperaturnih osjetnika na spojnim točkama vodova postiže se otkrivanje problema pregrijavanja, često povezanih s prekomjernim opterećenjem transmisijskih linija. Osim spomenutih, moguće je postavljanje i drugih osjetnika s ciljem poboljšanja tehničkih karakteristika mreže i smanjenja gubitaka električne energije ostvarenih u prijenosnoj mreži.

Povezivanjem osjetnika i drugih aktivnih i pasivnih elemenata s operativnim i poslovnim sustavima podrške operatora prijenosnog sustava M2M komunikacijom, podupiru se nastojanja za efikasnim upravljanjem tokovima električne energije u prijenosnoj mreži s ciljem kvalitetne opskrbe električnom energijom. Važno je uočiti da je uspostava i povezivanje M2M komunikacije s operativnim i poslovnim sustavima podrške u domeni transmisije slična njenoj uspostavi i integraciji u domeni masovne proizvodnje. Ipak, primjetna je razlika u mrežnoj pokrivenosti pojedinih domena. Dok u slučaju domene masovne proizvodnje topologija mreže poprimati mrežasti oblik, gdje svaki od čvorova predstavlja postrojenje za proizvodnju energije, u slučaju domene transmisije električne energije topologija poprima linijski oblik prateći tako infrastrukturu vodova i kablova. Zbog toga će u nekim slučajevima za potrebe optimizacije protoka podataka biti preporučeno postavljanje lokalnih podatkovnih i komunikacijskih procesora koji će u ulozi M2M poveznika upravljati poljem osjetnika te grupirati i procesirati prikupljene podatke prije njihova slanja u domenu M2M mreže (slika 6).



Slika 6: Primjer povezivanja osjetnika u M2M lokalnu mrežu i M2M poveznika u pristupnu mrežu.

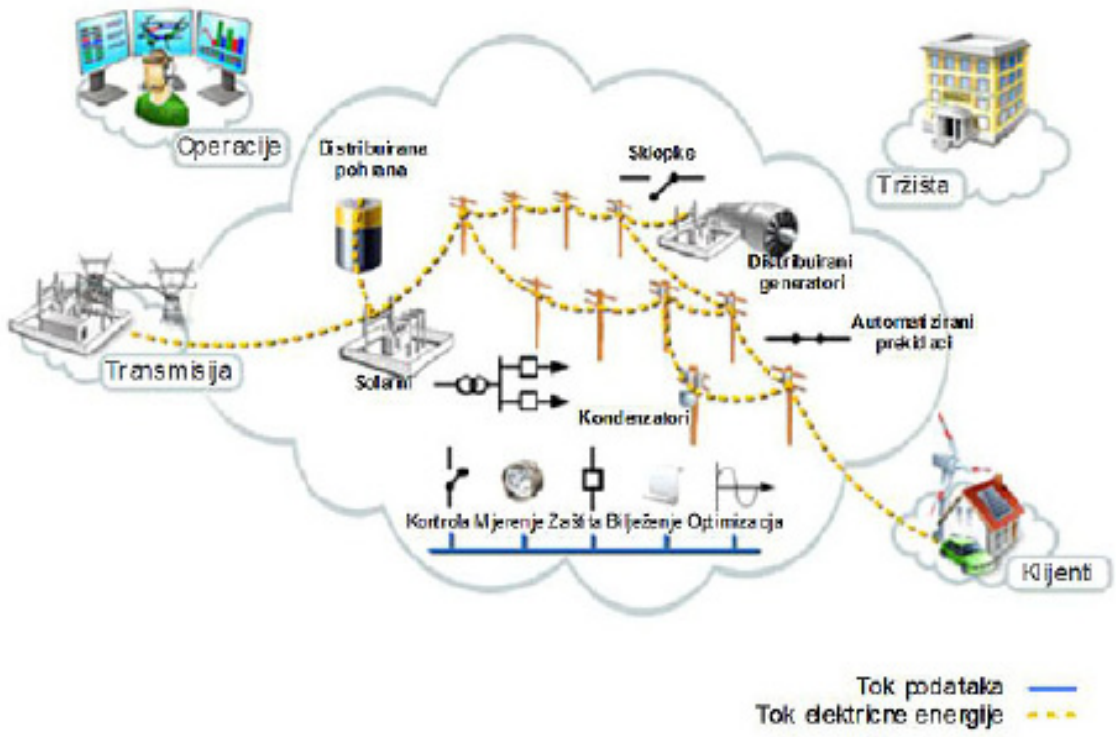
4.3 Distribucija

Domena distribucije raspodjeljuje električnu energiju prema i od krajnjih korisnika, odnosno klijenata. Distribucijska mreža povezuje inteligentna brojila i druge inteligentne uređaje, te ih upravlja i kontrolira putem dvosmjerne bežične ili žičane komunikacijske mreže poput mobilne 2G/3G mreže ili same elektroenergetske mreže (komunikacija elektroenergetskim vodovima - Power Line Communication). Domena može sadržavati i postrojenja za distribuiranu pohranu energije ali i druge alternativne izvore energije poput solara, vjetrenjača i drugih generatora. Sanduci kondenzatora, rastavne sklopke, automatizirani prekidači i transformatorske stanice samo su neki od primjera aktivnih i pasivnih elemenata distribucijske mreže, zaduženi za upravljanje mrežom te kvalitetnu raspodjelu i dostavu električne energije krajnjim korisnicima (slika 7).

Ipak, povezivanje kritičnih elemenata distribucijske mreže omogućiti će udaljeno nadgledanje tek temeljnih pokazatelja mreže bez pružanja dubokog uvida u pojedine oscilacije u ravnoteži raspodjele električne energije. Izostanak takvog dubljeg uvida u stanje mreže i upravljanja njenim elementima glavne su prepreke finijoj optimizaciji mreže i raspodjeli električne energije na temelju trenutačnih zahtjeva i potražnje, odnosno uspostavi mehanizama:

- kontrole i ranog otkrivanja izvanrednih stanja mreže,
- mjerenja energetske opskrbe i potrošnje,
- zaštite mreže i uzbunjivanja u slučaju slabe energetske učinkovitosti, kvarova i neočekivanih događaja te
- bilježenja energetske opskrbe s ciljem pružanja podrške u planiranju potrošnje i drugih mjera poboljšanja energetske učinkovitosti.

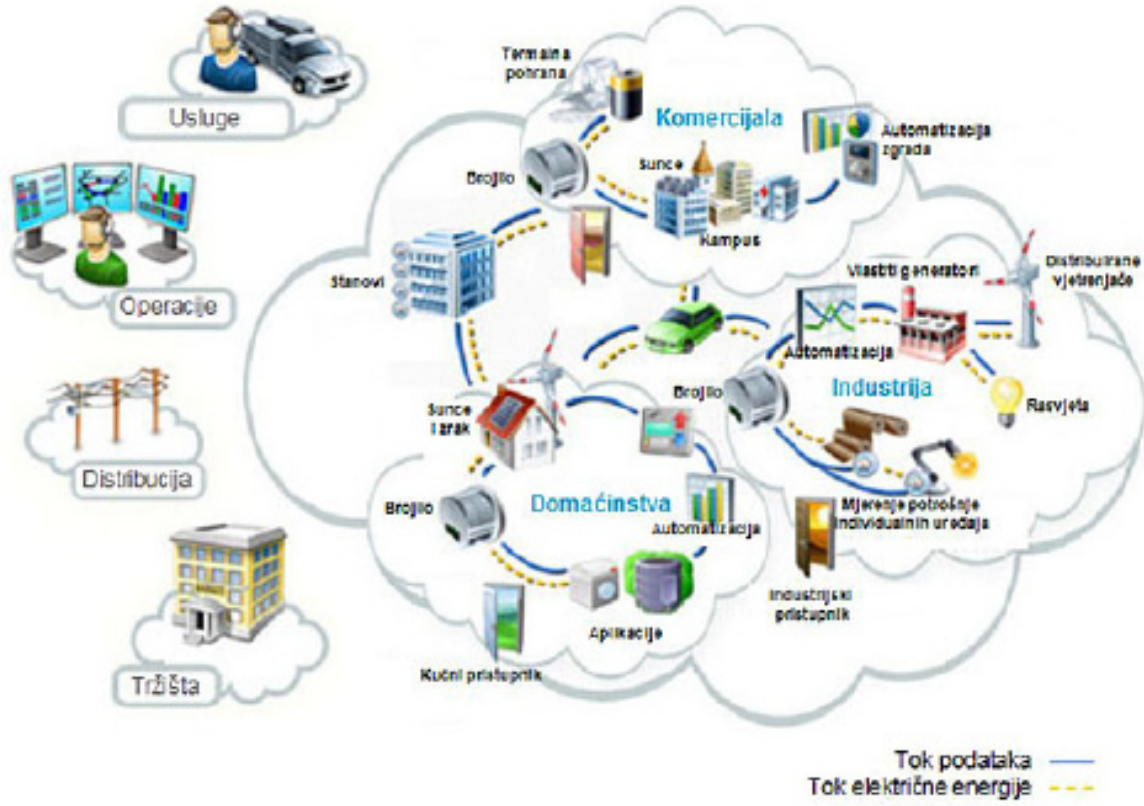
Integracija s drugim domenama poput operacija, transmisije i tržišta bit će kritična za postizanje automatizacije s ciljem trenutačne prilagodbe parametara distribucijskog sustava putem operativnih ili poslovnih sustava podrške novonastalim situacijama dodirnih domena. Ovdje se pod parametrima distribucijskog sustava se ne podrazumijevaju samo parametri distribucijske mreže i raspodjele električne energije, već i parametri distribucijskog sustava u općenitom smislu. Primjer takvih parametara može biti: cijena električne energije, promjene u tarifama i drugo.



Slika 7: Distribucija električne energije.

4.4 Klijenti

Domena klijenata, odnosno potrošača/proizvođača električne energije kao krajnjih korisnika distribucijske mreže, zadnjih je godina izuzetno dinamična s gledišta stvaranja novih domenskih aktera i elemenata (poput pojave električnih automobila, inteligentnih zgrada, privatnih generatora električne energije i distribuiranih postrojenja za pohranu energije…) te evolucije postojećih elemenata s obzirom na promjenu njihove uloge u domeni i načina na koji koriste/proizvode električnu energiju (slika 8). Dobar primjer su domaćinstava koja uporabom vlastitih solara i vjetrenjača žele aktivno sudjelovati kako u potrošnji tako i u proizvodnji električne energije u ulozi generatora energije domene distribucije.



Slika 8: Domena klijenata, odnosno krajnjih korisnika distribucijske mreže.

Zajednički element svih aktera domene klijenata je inteligentno brojilo. Njegova osnovna zadaća je precizna evidencija potrošene ali i proizvedene energije predane u distribucijsku mrežu, upravljanje smjerom toka električne energije i pružanje informacija o obrascima potrošnje energije te trenutnoj i akumuliranoj potrošnji električne energije pojedinog klijenta. Za tu je potrebu neizostavna M2M komunikacija koja korištenjem M2M platforme osigurava nesmetani dvosmjerni tok podataka između inteligentnih brojila i operativnih i poslovnih sustava podrške operatera distribucijskog sustava električne energije.

M2M komunikacija između brojila i M2M platforme operatora distribucije električne energije se uobičajeno ostvaruje jednim od sljedeća dva načina.

1. Kao komunikacijski kanal između brojila i M2M platforme se koristi neka od javnih pokretnih mreža. Prednost ovakvog povezivanja je u jednostavnosti povezivanja brojila u M2M komunikacijsku mrežu te u činjenici da operatora distribucijskog sustava time izbjegava održavanja komunikacijskog kanala. S druge strane, u najmanju ruku, zbog potrebne izmjene SIM modula u inteligentnim brojilima, prelazak na drugog operatera pokretnih komunikacija je zahtjevan. Iako postoje prototipovi softverskih SIM modula koji bi trebale omogućiti promjenu domaće javne pokretne mreže bez izmjene SIM modula, ovakva rješenja još uvijek nisu niti standardizirana niti prihvaćena.
2. Komunikacija elektroenergetskim vodovima predstavlja žičanu alternativu mobilnim pokretnim mrežama. Komunikacija se odvija na dvije razine. Prvu predstavlja komunikacija između M2M platforme i koncentratora putem optičkih i drugih dostupnih komunikacijskih kanala. Drugu razinu

predstavlja komunikacija od koncentratora do lokalnih inteligentnih brojila putem energetskih vodova. Prednost ovog pristupa je korištenje već dostupnih vodova za potrebe razmjene podataka. Ipak, korištenje vodova u komunikacijske svrhe je podložnije pogreškama uslijed komunikacije od pokretnih mreža.

Važno je napomenuti da svaki klijent, neovisno radi li se o kućanstvu, industriji, kompaniji i slično, iza inteligentnog brojila sadrži vlastitu privatnu domenu uređaja odnosno potrošača i proizvođača električne energije. Primjer takvih uređaja može biti frižider s ugrađenim sustavom za pohranu energije koji će se za vrijeme jeftinije struje puniti električnom energijom i prazniti za vrijeme skuplje. Aplikacije za upravljanje električnom energijom mogu automatizirano uključivati pojedine programe kućanskih aparata, poput programa perilice rublja, za vrijeme jeftinijih tarifa. Slijedom istih aplikacija distributeri električne energije mogu ponuditi promotivne tarife, poput sniženja cijene električne energije potrošene perilicom suđa u određenom vremenskom intervalu i time vršiti balansiranje opterećenja mreže . U privatnoj domeni klijenata se mogu još nalaziti i različiti uređaji za inteligentno upravljanje domaćinstvom, uređaji za zabavu i multimediju te generatori električne energije, solari i vjetrenjače.

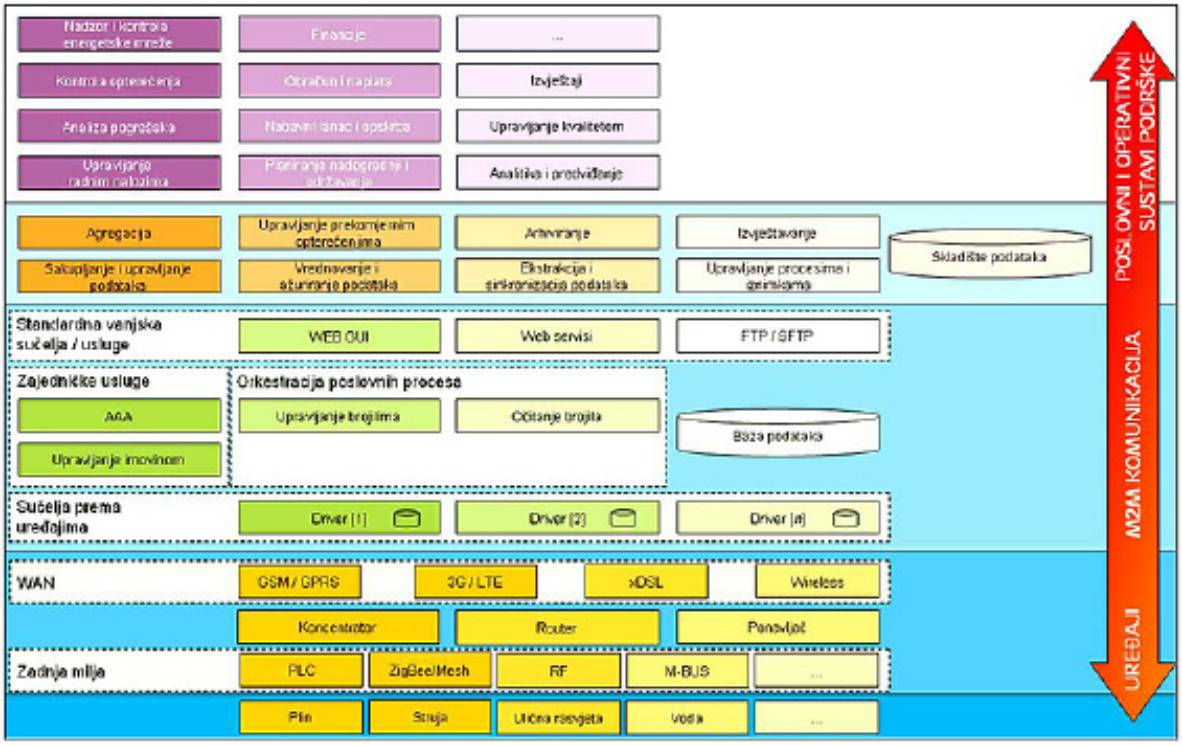
4.5 Operacije

Nadgledanje i upravljanje svih energetskih tokova između pojedinih domena se nadzire u operacijama (slika 9). Pri tome se M2M komunikacija koristi za uspostavu potrebne dvosmjerne komunikacije korištene u povezivanju podstanica, mreža klijenata i inteligentnih uređaja s operativnim i poslovnim sustavima podrške operacija.

Slika 9: Operacije.

Temeljnu informacijsku infrastrukturu operacija čini centralni sustav za upravljanje brojilima potrošnje električne energije MDMS (Meter Data Management System).

Operativni sustavi podrške operacije sadrže alate za nadzor, kontrolu i upravljanje energetskim tokovima te udaljeno upravljanje i očitanje stanja brojila potrošnje električne energije putem M2M komunikacijske mreže. Kontrola opterećenja i analitika pogreška ključni su alati u raspoređivanju tokova energije i planiranju održavanja i nadogradnji, dok izvještavanje i analitika imaju presudnu važnost u planiranju daljnjeg razvoja i uravnoteživanju energetskih tokova s očekivanom potražnjom i mogućom proizvodnjom električne energije. Integracija operativnih i poslovnih sustava podrške bit će važna prvenstveno u automatizaciji obračuna i naplate, upravljanju radnim nalozima, kontroli te predviđanju preopterećenja i analizi pogrešaka (slika 10).

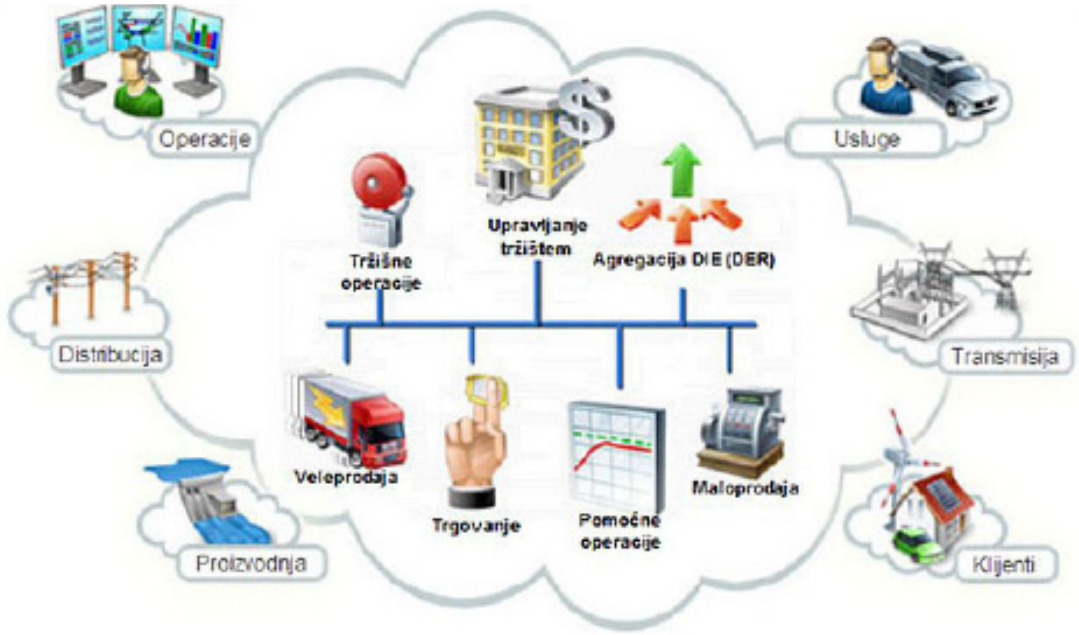


Slika 10: M2M komunikacija kao okosnica arhitekture napredne elektroenergetske ili komunalne mreže.

4.6 Tržišta

Uobičajeni sudionici domene tržišta su samostalne, neovisne i neprofitne javne organizacije čija je osnovna zadaća provođenje regulacije energetskih djelatnosti s ciljem učinkovitog i racionalnog korištenja energije, razvijanja konkurentnog poduzetništva u području energetike, stvaranja pozitivnih uvjeta za investiranje u energetski sektor i očuvanja okoliša (slika 11).

S obzirom da će ovakve, regulatorne agencije vršiti nadzor nad primjenom tarifnih sustava i propisanih naknada, nadzor nad energetskim subjektima, nadzor kvalitete usluge energetskih subjekata uz prikupljanje i obradu podataka, ali i pružanje usluga uravnoteženja električne energije u elektroenergetskom sustavu, bit će potrebno povezivanje na M2M komunikacijsku infrastrukturu s ciljem povezivanja informacijskih sustava i razmjene podataka dionika iz svih drugih domena.



Slika 11: Domena tržišta.

4.7 Usluge

Konačno, uspostavom napredne elektroenergetske mreže stvaraju se uvjeti za razvoj, do sada tek slabo primjetne, domene usluga. Mogućnost povezivanja informacijskih sustava pružatelja usluga iz ove domene s udaljenim uređajima drugih domena podržava osmišljavanje novih energetskih usluga udaljenog nadzora i upravljanja domaćinstvima i zgradama (slika 12). Tipični primjeri takvih usluga biti će web aplikacije za upravljanje vlastitom energetskom efikasnosti, sučelja za razmjenu podataka između potrošača i komunalnih kompanija, upravljanje rasvjetom, grijanjem i hlađenjem zgrada i kućanstava, isporuka jeftinije električne energije klijentima kroz podugovaranje i upravljanje dobavljačima električne energije i drugi. Moguće je pružanje usluga drugim domenama energetskog sektora poput usluga upravljanja potražnjom za električnom energijom, usluga upravljanja javnom rasvjetom, usluga upravljanja ispadima električne energije i uslugama instalacije i održavanja.

Slika 12: Domena usluga.

5 Zaključak

Dostupnost telekomunikacijskih usluga, odnosno globalna pokrivenost njima, pokrenula je trend razvoja i ugradnje komunikacijskih modula u sve što može imati koristi od komunikacijske povezivosti. Korporacija Ericsson predviđa da će do 2020. godine biti u upotrebi gotovo 50 milijardi takvih uređaja što čini i više od deset puta veću penetraciju umreženih uređaja u globalnoj populaciji od one danas. Drugim riječima, do 2020. godine će M2M komunikacija postati najzastupljeniji oblik komunikacije.

Jednako kao što telekomunikacija ulaze u novu eru, eru komunikacije strojeva, tako su i tradicionalni principi, modeli i energetske infrastrukture stavljene pod pritisak s ciljem izgradnje naprednih i inteligentnih elektroenergetskih mreža sposobnih adaptivno i optimalno upravljati proizvodnjom, raspoređivanjem i potražnjom za električnom energijom.

Američki nacionalni institut za standarde i tehnologije (NIST) je u sklopu nastojanja razvoja tehnoloških standarda za inteligentne energetske mreže identificirao sedam ključnih domena: masovna proizvodnja, transmisija, distribucija, klijenti, usluge, operacije i tržišta. U daljnjoj razradi tih domena na energetsku, komunikacijsku i informacijsko-informatičku razinu, Institut inženjera elektrotehnike i računarstva (IEEE) prepoznaje dvosmjerne M2M komunikacijske tokove informacija razmjenjivanih između pojedinih elemenata tih domena.

Ericsson Nikola Tesla je, kao specijalizirani isporučitelj telekomunikacijske opreme ali i kao predvodnik informacijsko komunikacijskih tehnologija, prepoznao ovo uzajamno podupiranje energetike i telekomunikacija te ih podržao vlastitim razvojnim ali i komercijalnim projektima. U isto vrijeme, korporacija Ericsson već sudjeluje u razvojnim projektima poput Device Connection Platform, rješenja za uspostavu M2M povezivosti, temeljenog na računarstvu u oblaku, ali i u većem broju projekata implementacije Smart Metering sustava diljem svijeta.

6 Literatura

[1] D. Niyato, L. Xiao, P. Wang, Machine-to-Machine Communications for Home Energy Management System in Smart Grid. Communications Magazine, IEEE, Volume: 49(4), p.p. 53-59, April 2011.

[2] Machine-to-Machine communications (M2M); Functional architecture. European Telecommunications Standards Institute. 2011. ETSI TS 102 690 V1.1.1 (2011-10).

[3] International Energy Outlook 2011. U.S. Energy Information Administration. September 2011. DOE/EIA-0484(2011).

[4] N. Tesla, A New System of Alternating Current Motors and Transformers. American Institute of Electrical Engineers, May 1888.

[5] T. P. Hughes, Networks of Power: Electrification in Western Society, 1880–1930. Baltimore: Johns Hopkins University Press. ISBN 0-8018-4614-5. March 1993. p.p. 119–122.

[6] U.S.-Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, April 2004.

[7] Interim Report of the Investigation Committee on the 28 September 2003 Blackout in Italy, UCTE, 27 October 2003.

[8] The Smart Grid: An Introduction. Prepared for the U.S. Department of Energy by Litos Strategic Communication unter contract No. DE-AC26-04NT41817, subtask 560.01.04.

[9] Final Guidelines of Good Practice on Regulatory Aspects of Smart Metering for Electricity and Gas. European Regulators Group for Electricity & Gas. Bruxelles, 8 February 2011. Ref: E10-RMF-29-05.

[10] Directive 2006/32/EC of the European parliament and of the Council of 5 April 2006 on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC.

[11] 3rd Energy Package. URL: http://www.europarl.europa.eu/sides/getDoc.do?type=IMPRESS&reference=20080616FCS31737&language=EN

[12] Institute of Electrical and Electronics Engineers, Approved IEEE Smart Grid Standards. http://smartgrid.ieee.org/standards/approved-ieee-smart-grid-standards

[13] National Institute of Standards and Technology, NIST & the Smart Grid. www.nist.gov/smartgrid/nistandsmartgrid.cfm

[14] G. Dudek, Artificial Immune System for Short-Term Electric Load Forecasting, Rutkowski et al. (eds.). ICAISC 2008, LNAI 5097, pp. 1007–1017, 2008.

[15] E. A. Feinberg, D. genethliou, Load Forecasting, in Applied Mathematics for Restructured Electric Power Systems: Optimization, Control and Computational Intelligence, J. H. Chow, F. F. Wu, J. J. Momoh (eds.),.Springer, 2005. p.p. 269-285.

[16] J.P. Lynch, A. Sundararajan, K.H. Law, A.S. Kiremidjian, T. Kenny, E. Carryer, Embedment of Structural Monitoring Algorithms in a Wireless Sensing Unit. Structural Engineering and Mechanics, Vol. 15, No. 3, p.p. 285-297, 2003.

[17] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A Survey on Sensor Networks. IEEE Communications Magazine, vol. 40, p.p. 102 – 114, August, 2002.

7 Popis kratica

ETSI	European Telecommunications Standards Institute
IEEE	Institute of Electrical and Electronics Engineers
M2M	Machine-to-Machine
NIST	National Institute of Standards and Technology
TV	Televizija

Adresa autora:

Marko Lukičić
e-mail: marko.lukicic@ericsson.com
Ericsson Nikola Tesla d.d.
Krapinska 45
p.p. 93
HR-10002 Zagreb
Hrvatska

Uredništvo je primilo rukopis 7. svibnja 2012.

IV

Josip Dulj, Tomislav Blajić
Ericsson Nikola Tesla d.d., Zagreb, Hrvatska
Ericsson Nikola Tesla d.d., Zagreb, Croatia

M2M KOMUNIKACIJE KORIŠTENJEM POKRETNIH MREŽA

M2M COMMUNICATIONS OVER MOBILE NETWORKS

Sažetak

U današnje vrijeme razni uređaji zauzimaju sve važnije mjesto u svakodnevnom životu. Mobilni telefoni su prisutni u svim segmentima života te se danas koriste ne samo za komunikaciju već i kao sredstvo plaćanja, foto i video snimanje te kao pristup internetu, itd. Zajednička karakteristika ovih aktivnosti je da su inicirane od strane krajnjeg korisnika (čovjek).
Razvojem industrije i promjenom stila života dolazi do potrebe za optimizacijom i automatizacijom mnogih segmenata svakodnevice. Jedan od najstarijih primjera je hladnjak koji bi pazio na količinu namirnica te automatski kreirao izvještaj o namirnicama koje treba kupiti. Primjer novijeg datuma odnosi se na nadzor voznog parka gdje vozila šalju podatke o lokaciji, potrošnji goriva, mogućim kvarovima, itd. Zajednička karakteristika ovih aktivnosti je da uređaji sami iniciraju komunikaciju na osnovi ugrađenih algoritama te šalju informaciju na obradu, pa govorimo o komunikaciji između uređaja ili skraćeno M2M (Machine to Machine) komunikaciji.
Takva vrsta komunikacije ima svoje zahtjeve i specifičnosti na koje današnja tehnologija ima odgovore, a jedan od njih je korištenje tehnologija pokretnih mreža.

Abstract

Usage of various devices occupies an important place in today's everyday life. Mobile phones are present in all segments of life, used not only for communication but also as a means of payment, photo and video recording as well as Internet access, etc. As the common characteristic, these activities are initiated by end users (human).
With the development of industry and lifestyle comes the need for optimization and automation of many segments of life. One of the earliest examples is the fridge that would monitor the amount of food and automatically create a grocery shopping list. More recent example is related to car fleet monitoring, where the vehicles send data on the location, fuel consumption, possible failures, etc. As the common characteristic of these activities includes devices that initiate communication on their own, based on embedded algorithms, and sending the information to be processed, we talk about communication between machines (Machine to Machine communication, M2M).
This type of communication has its own requirements and specifics, for which today's technology has the answers. One of these answers is usage of the mobile networks technologies for M2M communication.

KLJUČNE RIJEČI:	KEY WORDS:
M2M	M2M
Komunikacija	Communication
Uređaj	Machine
Platforma	Platform
Pokretna mreža	Mobile network
Sigurnost	Security
IP usmjeravanje	IP routing
Kakvoća usluge	Quality of service

1 Uvod

Ideja M2M komunikacija već je dulje vrijeme prisutna u društvu, no tek nedavno dolazi u fokus kao važna tema i mogući izvor prihoda za mnoge mrežne operatore, čime raste interes vodećih proizvođača telekomunikacijske opreme kao i vodećih normizacijskih tijela. U tu je svrhu 7 normizacijskih tijela (ARIB, TTC, ATIS, TIA, CCSA, ETSI i TTA Korea) udružilo napore za pokretanje M2M normi čija je namjena polaganje globalnih temelja za M2M komunikaciju koji bi omogućili povrat uloženih sredstava. Tijekom 2012. godine očekuje se pokretanje globalne inicijative kako bi se pokrenuo tehnički dio koji bi pokrio izazove M2M komunikacije. Istovremeno i 3GPP, kao normizacijsko tijelo zaduženo za razvoj tehnologije zasnovane na GSM/WCDMA/LTE pokretnim sustavima, također djeluje na području M2M komunikacije s nizom tehničkih istraživanja i preporuka.

M2M komunikacija zasnovana na korištenju pokretnih mreža danas je raširena u svijetu i mnogi telekomunikacijski operatori nude takvu vrstu usluge krajnjim korisnicima. Krajnji korisnik je, u ovom slučaju, najčešće organizacija koja je vlasnik uređaja. Sjeverno američko tržište, čiji su predstavnici AT&T, Verizon i Sprint, vodeće je u ovom segmentu, a slijede ga globalni operatori kao što su Vodafone, T-Mobile, Telenor, itd.

Ericsson ima viziju od 50 milijardi umreženih uređaja do 2020. godine. Iako se ova brojka čini optimističnom, podaci ukazuju na taj trend - krajem 2010. godine je bilo oko 80 milijuna umreženih uređaja, dok ih se do 2015.g. očekuje oko 300 milijuna (uz predviđenu složenu godišnju stopu rasta (CAGR - Compound Annual Growth Rate) od 32 posto.

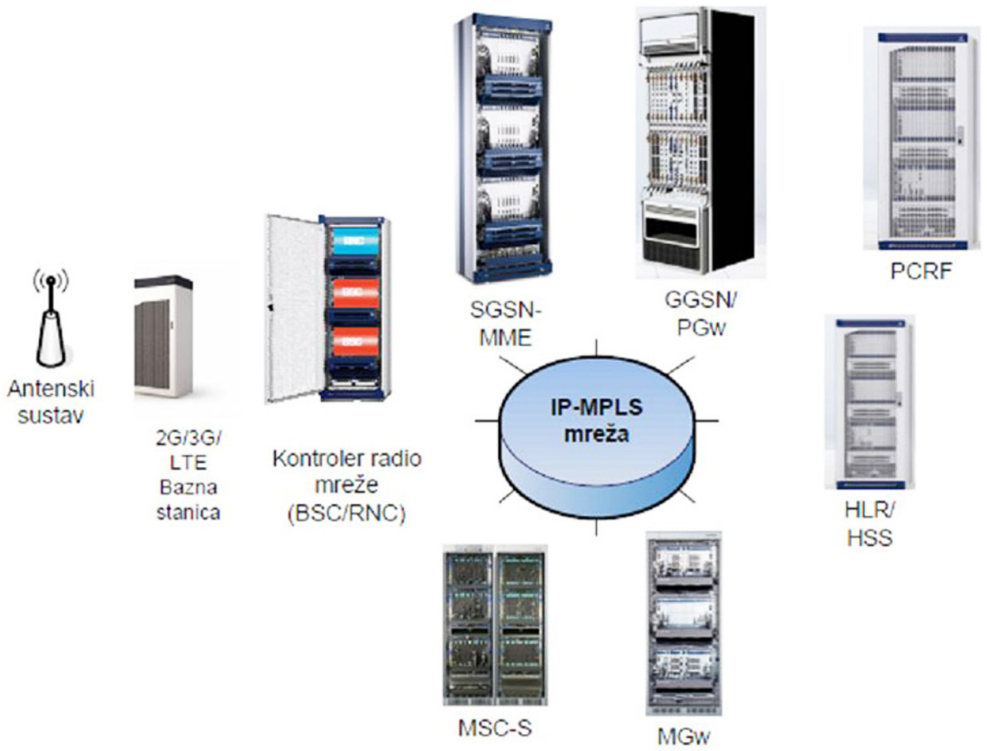
Sustav mrežne M2M komunikacije (slika 1) sadrži 4 osnovna elementa:

1. krajnje uređaje (hardverski moduli koji će biti instalirani u mreži i pružati informacije ovisno o namjeni),
2. platformu za upravljanje uređajima (potrebna kako bi se efikasno upravljalo uređajima te dobio pregled nad stanjem u mreži koja pruža povezivanje),
3. mrežno povezivanje (mreža koja daje IP vezu od/prema krajnjem uređaju) i
4. aplikaciju (centralno mjesto kamo uređaji šalju informacije na obradu)

Slika 1: Osnovni elementi mrežne M2M komunikacije

Gledano s tehnološkog stajališta pokretna mreža se nameće kao najbolji izbor za mrežno povezivanje, zato što posjeduje sljedeće bitne karakteristike:

- jednostavan i brz početak rada (uređaj treba imati SIM karticu i odmah je spreman je komunikaciju preko mobilne mreže),
- pokrivanje (današnje mobilne mreže signalom pokrivaju i najudaljenija područja te se uređaj može postaviti bilo gdje bez potrebe za izgradnjom pristupne linije),
- mobilnost, kao sastavni dio mobilne mreže (neke M2M usluge, poput prometnih, zahtijevaju mobilnost krajnjih uređaja što znači da je mobilna mreža savršeni izbor),
- građene su sukladno globalnim 3GPP normama i imaju riješenu IP komunikaciju od krajnjeg uređaja do interneta odnosno poslužitelja te
- pružaju izvrsne karakteristike u pogledu propusnosti i kašnjenja (HSPA i LTE mreže mogu zadovoljiti potrebe multimedijalnih aplikacija za visokom kvalitetom usluge).

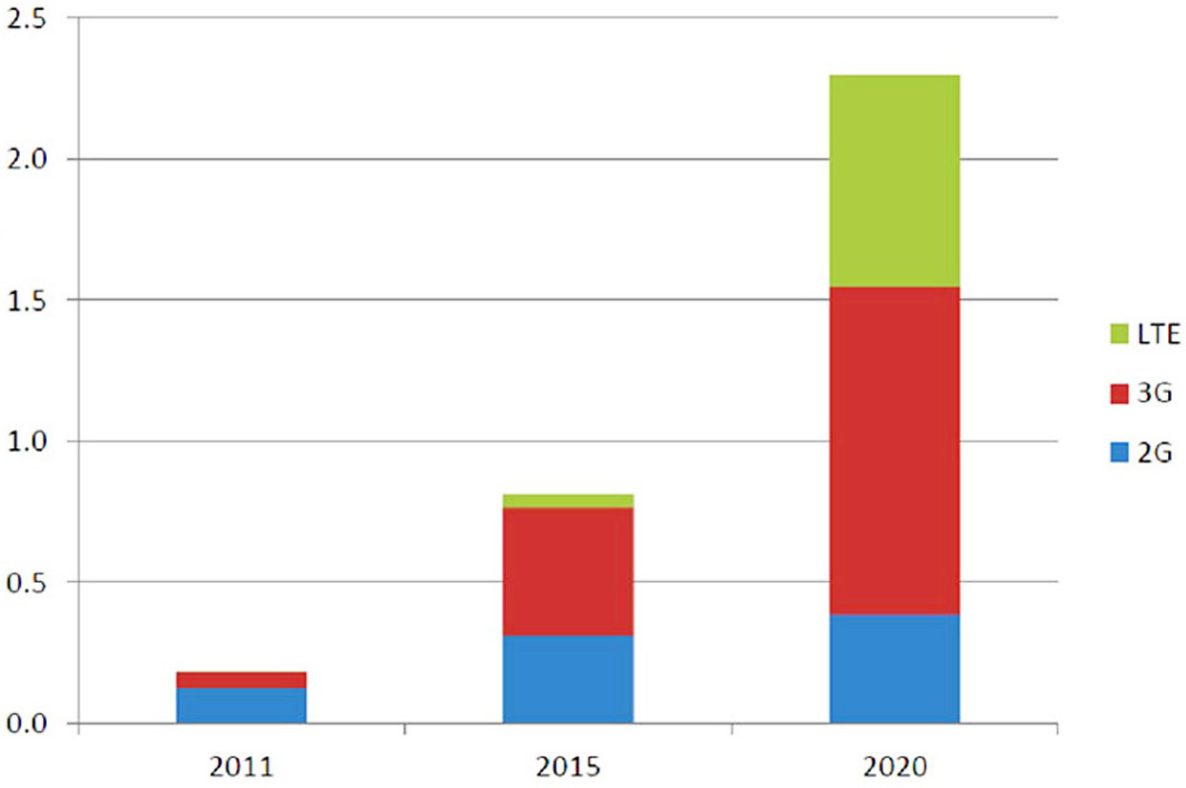


Slika 2: Osnovni elementi arhitekture pokretne mreže

Arhitektura pokretne mreže sa komponentama bitnim za M2M komunikaciju prikazana je na slici 2. Četiri bitna dijela međusobno su povezana IP tehnologijom:

- radio mreža – antenski sustav, bazne stanice (2G/3G/LTE) i kontrolori radio mreže (BSC/RNC),
- jezgrena mreža paketskog prijenosa – SGSN-MME, GGSN-PGw, PCRF,
- jezgrena mreža za prijenos govora – MSC-S, MGw te
- baza korisnika – HLR/HSS.

M2M komunikacija se većinom odvija paketskim prometom koristeći IP (IPv4 ili IPv6). Iako je moguća komunikacija preko govornog dijela mreže (komutacijom kanala) ne očekuje se da će ona zaživjeti zbog slabih mogućnosti za prijenos informacija. Izuzetak može biti SMS komunikacija za vrlo malu količinu informacija ili kao sredstvo buđenja uređaja (uređaj može biti u stanju mirovanja kako bi štedio energiju i/ili mrežne resurse). Druga moguća primjena odnosi se na mogućnost automatskog podešavanja postavki uređaja (OTA, Over the Air), npr. putem SMS poruke. OTA rješenje je dostupno i preko paketskog dijela mreže, ali u svrhu očuvanja postojećeg ulaganja u OTA rješenja, treba dozvoliti i ovu mogućnost.



Slika 3: Broj M2M konekcija, prema pristupnoj radijskoj tehnologiji (stanje 2011, predviđanje za 2015-2020.g., izvor [4])

2 M2M IZAZOVI

Brojka od 50 milijardi umreženih uređaja izgleda kao perspektivan poslovni potencijal za telekomunikacijske operatore, a u konačnici i za proizvođače opreme. Ipak potrebno je izdvojiti i neke bitne izazove koje treba sagledati u M2M poslovnom modelu:

Prihod – Količina prometa u M2M komunikaciji ovisi o namjeni samog uređaja. Primjerice, uređaj koji očitava stanje brojila šalje jako malu količinu podataka, jednom dnevno. S druge strane video nadzor šalje jako puno podataka. Tendencija je da će većina M2M komunikacije generirati mali promet pa je i prihod po uređaju malen. Prema dostupnim predviđanjima, prosječni prihod po korisniku (ARPU - Average revenue per user) u M2M komunikaciji bit će na razini jedne desetine današnjeg korisnika - čovjeka. Ovo za sobom povlači potrebu optimizacije resursa i procesa kako bi margina bila zadovoljavajuća.

Poslovni sustavi trebaju biti dimenzionirani za poveću količinu uređaja uz prilagođeni sustav podrške kupcima. Naime, krajnji kupac nije sam uređaj već poslovni subjekt koji posjeduje uređaje. To za sobom povlači jedan račun za sve uređaje u vlasništvu nekog poslovnog subjekta, koji također želi imati i kontrolu nad uređajima (npr. kada aktivirati pojedini uređaj, imati uvid u performanse uređaja bez kontaktiranja operatora u realnom vremenu, itd.). Ovo zahtijeva da poslovni subjekt ima pristup u poslovne sustave ili dijelove upravljanja i nadzora (O&M) same mreže što predstavlja sigurnosni problem, kao i integracijski izazov te sa sobom nosi vremensku i novčanu dimenziju.

Telekomunikacijska oprema: Operatori moraju biti spremni uložiti u dodatne softverske licence i hardver, zbog povećanja broja uređaja u mreži. S obzirom na već spomenuti prihod i ARPU, prema ovakvoj investiciji se treba postaviti pažljivo.

Na tragu ovakvih razmišljanja operateru se nameću dva rješenja za optimizaciju M2M poslovanja i prilagodbe M2M komunikaciji:

1. razvoj vlastite M2M platforme za upravljanje uređajima (Platforma mora biti prilagođena M2M procesima, mora biti skalabilna i imati mogućnost prilagodbe različitim poslovnim subjektima. Procjene su da je za razvijanje ovakve platforme potrebno 1-2 godine, što na brzo rastućem M2M tržištu može značiti nepovratni gubitak tržišnog udjela.), ili
2. kupnja, odnosno korištenje već razvijene platforme za M2M komunikaciju, čime se razvoj i održavanje platforme prebacuje na proizvođača opreme. (Ovakav pristup omogućava brzu tržišnu dostupnost (TTM - Time to Market) te pruža operatoru mogućnost da se usmjeri na razvoj posla i pridobivanja poslovnih subjekata. Ericsson u ovom segmentu nudi svoju platformu EDCP (Ericsson Connection Device Platform).

3 M2M KOMUNIKACIJA

Sa stajališta pokretne mreže M2M komunikacija se ne razlikuje bitno od trenutačnog korisničkog prometa. Pokretna mreža ne pravi razliku između M2M uređaja i ljudskog korisnika jer koristi iste mehanizme u oba slučaja. Ti mehanizmi se odnose na uspostavu IP veze između uređaja i aplikacijskog poslužitelja (session management) te mogućnost kretanja uređaja (mobility management).

Među osnovna svojstava pojedine radijske pristupne tehnologije u pokretnoj mreži, nužna za kvalitetnu uspostavu M2M usluga možemo ubrojiti:

» sigurnost (Security) (Na radijskom sučelju provodi se enkripcija podataka, dok je sama radijska pristupna mreža transparentna na metode zaštite podataka s kraja-na-kraj (end-to-end) primjenjive na aplikacijskom sloju (npr. IPsec).),

» kvalitetu usluge (QoS -Quality of Service) (U suradnji sa paketskom jezgrenom mrežom moguća je podrška za QoS razlikovanje pretplatnika ili tipova nositelja usluga. Svi postojeći QoS mehanizmi korišteni u današnjem širokopojasnom mobilnom pristupu za naplatu i kontrolu prometa, mogu su primijeniti na M2M komunikaciju kako bi optimizirali korištenje mrežnih resursa.) te

» odašiljanje (Broadcast) (Različite mogućnosti slanja poruka/podataka prema većem broju/svim uređajima unutar jedne/više ćelija, podržane su od strane različitih radijskih tehnologija; npr. CBS (Cell Broadcast) za GSM i WCDMA, MBMS (Multimedia Broadcast-Multicast Services) za WCDMA i LTE, ETWS (Earthquake Tsunami Warning System) za WCDMA i LTE).

Radijske pristupne mreže (RAN – Radio Access Network) pružaju temeljni prijenosni kanal između paketske jezgrene mreže (PS Core Network) i krajnjih M2M uređaja. Bez obzira je li je riječ o već prisutnim radijskim tehnologijama druge (GSM/GPRS) ili treće generacije (WCDMA/HSPA) ili tek nadolazećim (LTE), one su u stanju pružiti uslugu prikladnu za M2M komunikaciju.

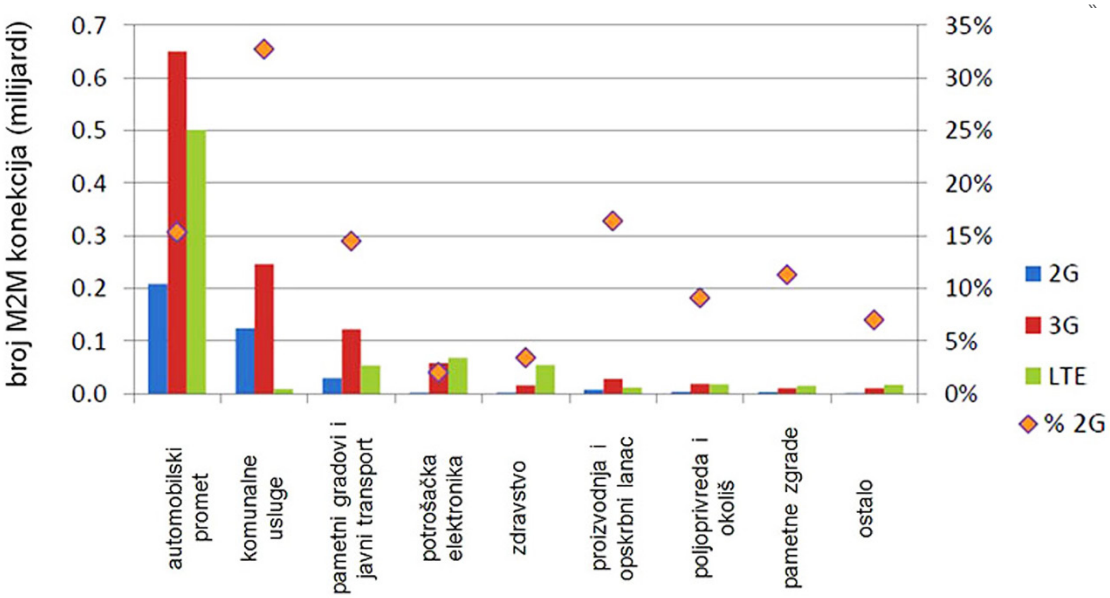
Primjenjivost pojedine radijske tehnologije ovisi i o karakteristikama pojedine M2M aplikacije. Pri tome, svaku aplikaciju može karakterizirati neki od sljedećih zahtjeva:

» podrška velikog broja aktivnih uređaja, ali uz vrlo male zahtjeve prema ukupnom kapacitetu, primjerice u slučaju komunalnih usluga (Premda i postojeće tehnologije mogu ispuniti današnje potrebe, LTE će svojim mogućnostima znatno pridonijeti podršci ovog aspekta u budućnosti, pogotovo u problematičnim slučajevima velikog broja istovremenih pokušaja pristupa sustavu. U slučaju prijenosa kratkih, ali neučestalih informacija nameće se potreba za optimizacijom signalizacijskih procedura kako bi se smanjilo opterećenje izazvano uglavnom kontrolnim prometom (control plane signalling).),

» podrška za rad i u uvjetima mobilnosti, kao u slučaju transportnih usluga (Jednosmjerna (unicast) dostava informacija u ovakvom okruženju je podržana i danas, ali samo odašiljački (broadcast) mehanizmi pomažu da se pritom zadrži malo opterećenje sustava. Pri tome najbolje performanse pokazuje ETWS pristup jer CBS ne osigurava kratka vremena kašnjenja, dok MBMS pristup još nije zadobio značajniju prihvaćenost, a i nije efikasan za manji broj korisnika.),

» potreba za niskom latencijom, primjerice u segmentu umreženih uređaja (HSPA zadovoljava većinu potreba, dok LTE osigurava stabilne niske vrijednosti kašnjenja , što je kritični faktor za neke igrače (gaming) aplikacije.),

» potreba za prijenosom veće količine podataka uzlaznom vezom, kao u slučaju video nadzora (GSM/GPRS tehnologija svojim kapacitetima nije u stanju podržati ovakve aplikacije, dok su performanse HSPA sustava zadovoljavajuće samo u slučaju manjeg broja korisnika/uređaja. LTE će uslijed velikog kapaciteta uzlazne veze biti u stanju podržati znatno zahtjevnije potrebe ovih aplikacija.).

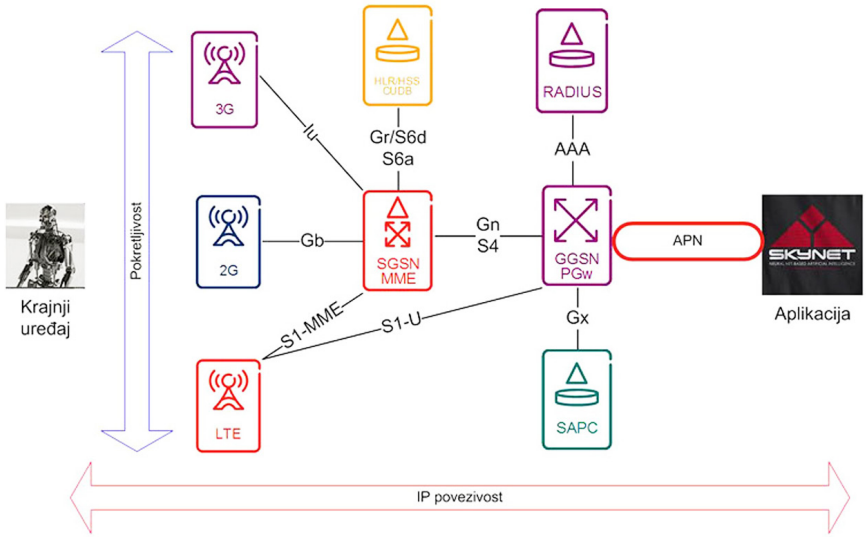


Slika 4: Broj M2M konekcija u ovisnosti o radio tehnologiji i aplikaciji (predviđanje za 2020.g., izvor [4])

Jezgrena mreža paketskog prijenosa u mobilnim mrežama sadrži:

- SGSN-MME čvor koji ima funkcije potrebne za posluživanje GPRS/EDGE/UMTS/HSPA/LTE prometa (Sa stajališta mreže nije potrebno, niti je tehnički izvedivo i opravdano, imati dedicirani SGSN-MME čvor za M2M komunikaciju.),
- GGSN-PGW čvor koji služi kao točka ulaza/izlaza mobilnog podatkovnog prometa iz mobilnih mreža (Ovaj čvor također posjeduje funkcije potrebne za posluživanje GPRS/EDGE/UMTS/HSPA/LTE prometa. Za razliku od SGSN-MME opcija sa dediciranim GGSN-PGW čvorom ima smisla u pogledu potrebnog kapaciteta i sigurnosti. GGN-PGw implementira i QoS mehanizme.),
- RADIUS čvor za autentikaciju i naplatu prometa (Ovaj čvor je opcijski, ali pruža nekoliko zanimljivih opcija za potrebe M2M komunikacije),
- SAPC čvor za napredne QoS mehanizme (Ovaj čvor je opcijski jer GGSN-PGW sadrži QoS mehanizme koji se nadopunjuju sa SAPC funkcionalnostima.) te
- HLR/HSS čvor kao centralnu bazu svih korisnika u pokretnoj mreži (ne samo za M2M).

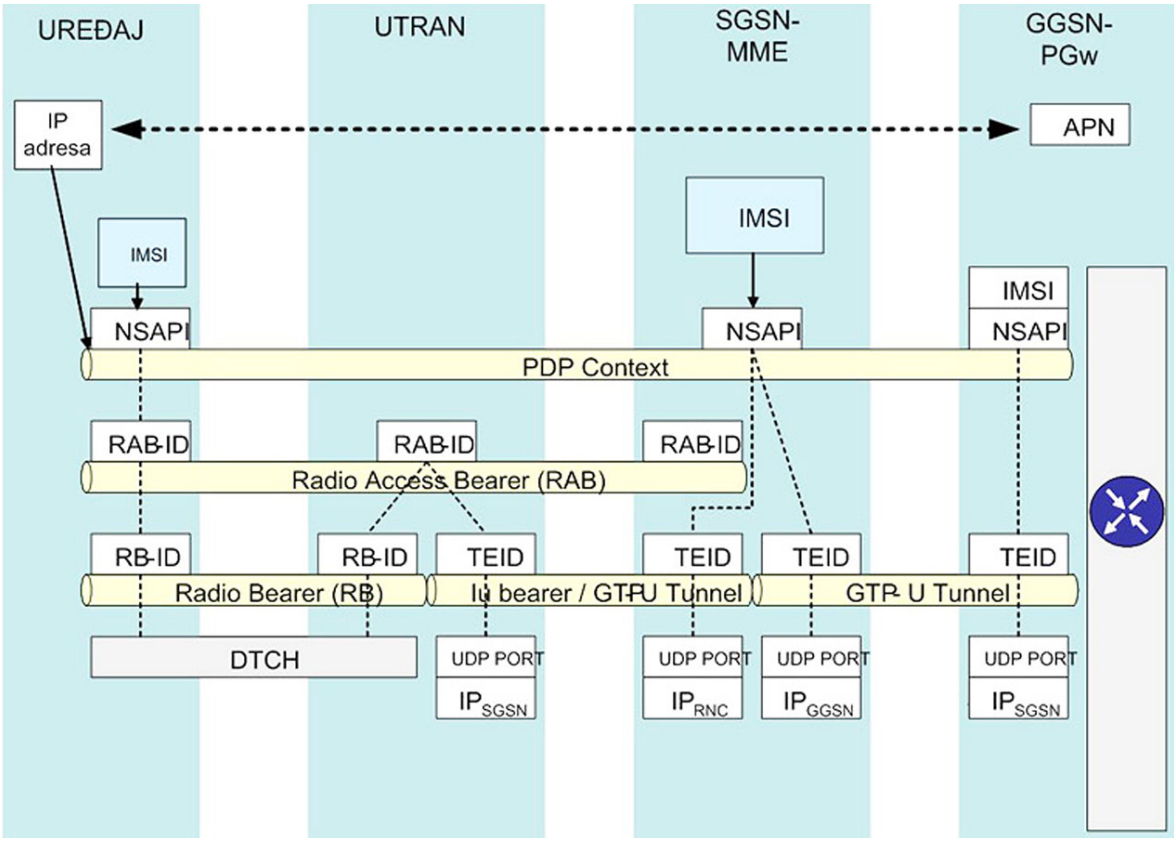
Elementi i sučelja pokretne mreže (sa naglaskom na paketski prijenos) koji sudjeluju u M2M komunikaciji su prikazani na slici 5.



Slika 5: Elementi i sučelja u M2M komunikaciji putem pokretnih mreža

3.1 IP adresiranje i usmjeravanje

Za komunikaciju s aplikacijskim serverom svaki uređaj mora imati dodijeljenu IP adresu. IP adresa se dodjeljuje prilikom uspostave PDP (Packet Data Protocol) konteksta. PDP kontekst je apstrakcija koja povezuje uređaj, SGSN-MME i GGSN-PGw čvorove, a u stvarnosti se bazira na nositeljima (bearer) u radio i jezgrenom dijelu mreže kako je prikazano slikom 6.



Slika 6: Realizacija PDP konteksta preko radijskih i jezgrenih nositelja (RAB)

Usmjeravanje prometa je vezano uz koncept konfigurabilnog mrežnog identifikatora - APN (Access Point Name). APN se može promatrati kao virtualna mreža koja ima svoja pravila usmjeravanja prometa, naplate prometa, postavki kvalitete usluge, pristupa internetu... Koristeći APN koncept mobilni operator može razdvojiti pojedine poslovne subjekte i svakom pružiti drugačije usluge.

Prilikom uspostave PDP-a uređaj šalje APN kojemu želi pristupiti i preko kojega će pristupiti aplikacijskom poslužitelju. Kako bi se povećala sigurnost i kontrola M2M komunikacije, APN se može kontrolirati na sljedeće načine:

- zahtijevani APN se u SGSN-MME čvoru uspoređuje sa podacima dobivenim iz HLR/HSS za taj uređaj pa ako se zahtijevani APN ne nalazi u podacima, uspostava PDP-a se obustavlja (postoje i drugačiji mehanizmi, ali za M2M komunikaciju je ovaj optimalan),
- RADIUS također može utjecati na izbor APN čime se zahtijevani APN može promijeniti

Postoji više načina dodjeljivanja IP adrese uređaju:

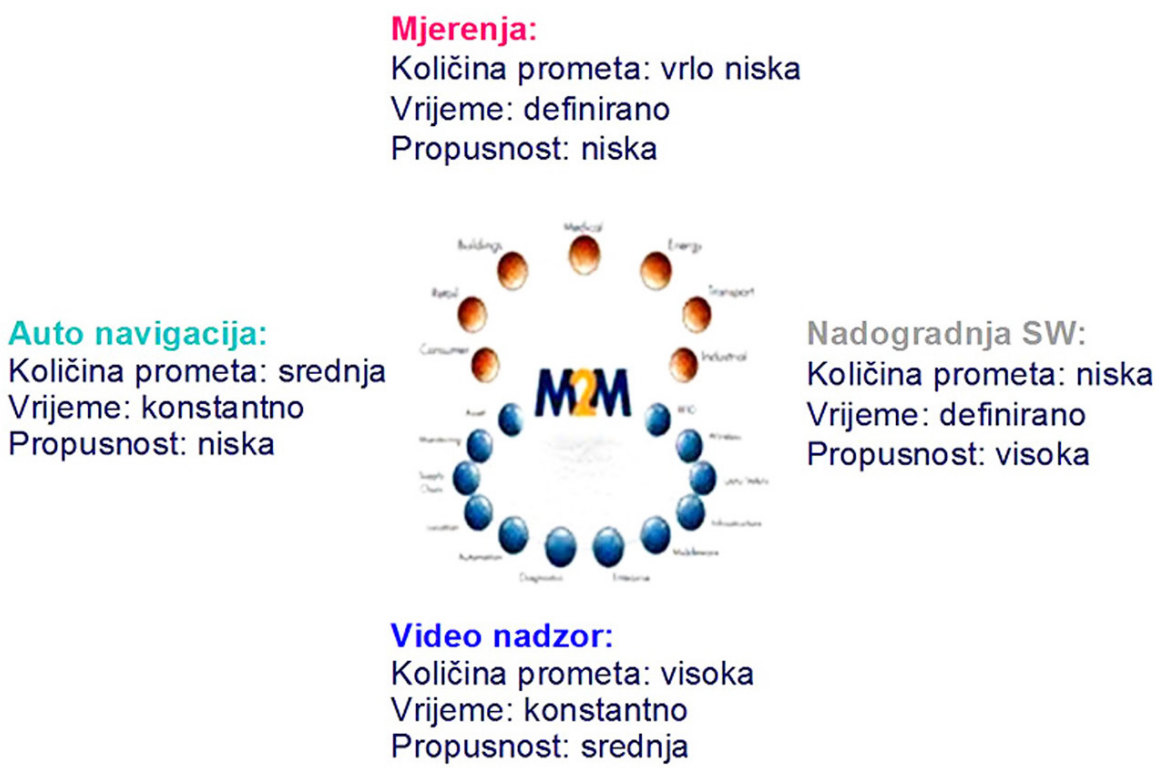
- statička IP adresa definirana u HLR čvoru (Ovaj podatak se prilikom registracije uređaja sprema u SGSN-MME te se kod aktivacije PDP-a šalje na GGSN-PGw.),
- dinamička IP adresa dodijeljena od strane GGSN-PGw čvora (Svaki APN ima svoj bazen IP adresa koji dodjeljuje uređaju prilikom uspostave PDP konteksta. Prednost ovog pristupa je što se adrese

koriste onoliko dugo koliko traje PDP ili preciznije, samo dok uređaj ima podatkovnu vezu, a zatim se oslobađaju kako bi ih drugi uređaj mogao koristiti.),

» dinamička IP adresa dodijeljena od strane RADIUS servera.

3.2 Kvaliteta usluge (QoS)

Svaka M2M komunikacija ima različite zahtjeve na kvalitetu usluge ovisno o vrsti informacije koja se prenosi, a ti zahtjevi su propusnost, vrijeme, količina prometa… Iako izravno nije vezana za kvalitetu usluge, mobilnost uređaja je nešto na što treba obratiti pažnju radi optimizacije signalizacijskih resursa u radijskom i jezgrenom dijelu mreže. Naime, nađe li se u mreži veliki broj uređaja s visokim stupnjem mobilnosti (npr. svaki automobil) količina signalizacije će višestruko narasti. Na samu mobilnost mobilni operator ne može (i zapravo ne bi smio) utjecati nikako, osim osiguravanjem mrežnih resursa kako bi mobilnost bila uspješna.



Slika 7: Mrežni zahtjevi pojedinih M2M aplikacija

Kvaliteta usluge se realizira na nekoliko načina:

» postavkama u HLR čvoru gdje se na razini uređaja definira maksimalna propusnost koja se onda provodi u radijskom i jezgrenom dijelu mreže,

» postavkama u GGSN-PGw čvoru gdje se može definirati maksimalna propusnost te također ograničiti vrsta informacije koju uređaj prenosi, kao i vrijeme kada uređaj smije prenositi informacije kako bi se spriječila mogućnost zlouporabe te

» postavkama u PCRF čvoru gdje se na inteligentan način koristeći trenutne podatke iz mreže može kontrolirati QoS preko Gx sučelja prema GGSN-PGw čvoru

3.3 Redundancija

Iznimno bitna karakteristika je mrežna redundancija. Tu se M2M komunikacija ne razlikuje od današnjih visoko postavljenih zahtjeva na redundanciju u mreži.

Redundancija se postiže na nekoliko načina od kojih su najbitniji:

- SGSN-MME pool (Svi SGSN-MME čvorovi u mreži su povezani sa svim čvorovima u radio mreži. Ako jedan od SGSN-MME čvorova u mreži postane nedostupan zbog bilo kojeg razloga, radio pristupna mreža može slati promet jednom od preostalih SGSN-MME čvorova.),
- GGSN-PGw raspodjela prometa (APN koncept može biti distribuiran na vise GGSN-PGW čvorova. U slučaju ispada jednog GGSN-PGW čvora, promet će biti usmjeren na jedan od preostalih GGSN-PGW čvorova koji služe zahtijevani APN.),
- HLR/HSS, PCRF te RADIUS geografska redundancija (Baze podataka kao HLR/HSS, PCRF i RADIUS se mogu implementirati u parovima te jedan drugome biti redundancija u slučaju ispada.).

3.4 Podaci za naplatu

Telekomunikacijski operator mora biti u mogućnosti naplatiti korištenje svoje mreže za M2M komunikaciju. U tu svrhu koristi zapise o pozivima (CDR – Call Data Records) u kojima se nalaze sve bitne informacije o M2M komunikaciji, npr:

- vremenski okviri M2M komunikacije,
- identitet uređaja,
- količina prometa,
- postavke kvalitete usluge i
- lokacija uređaja

Podaci za sve uređaje istog vlasnika (poslovnog subjekta) obrađuju se uz ispostavljanje samo jednog računa za sve uređaje.

CDR zapisi nalaze se na SGSN-MME (za 2G i 3G komunikaciju) te na GGSN-PGw čvorovima (za 2G, 3G i LTE komunikaciju).

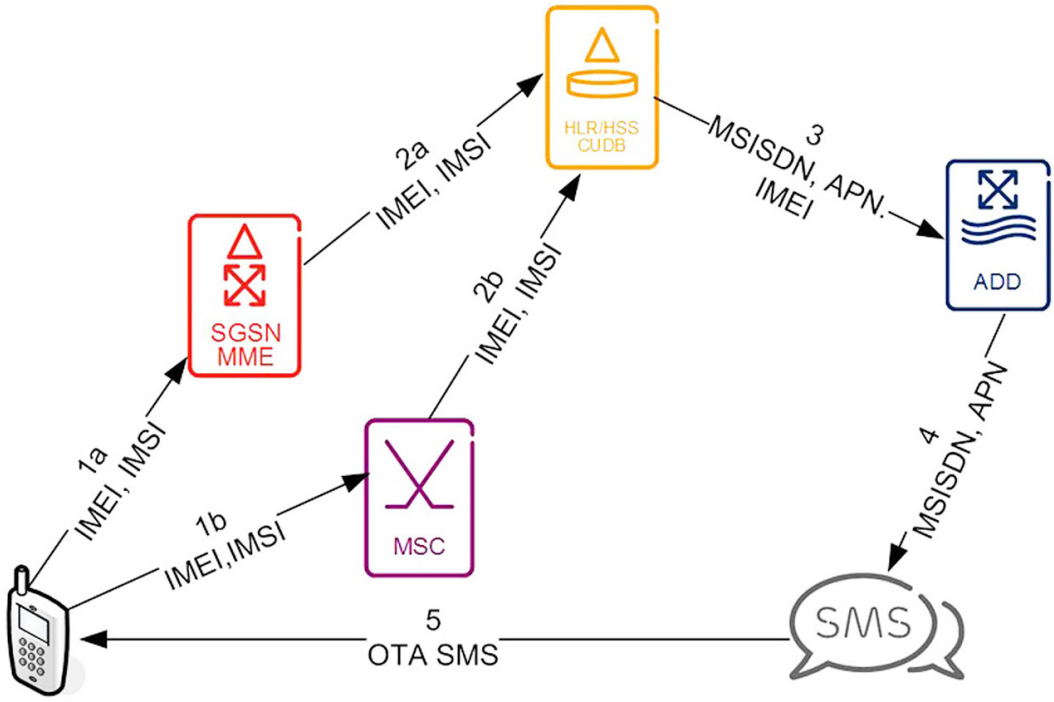
3.5 RADIUS funkcionalnosti

RADIUS funkcionalnost daje poslovnom subjektu mogućnost da u realnom vremenu nadzire uređaj i poduzima akcije. RADIUS čvor se može nalaziti kod telekomunikacijskog operatora (uobičajeno za današnju komunikaciju), ali i u vlasništvu samog poslovnog subjekta što daje sljedeće prednosti:

- Poslovni subjekt može sam definirati IP adresni prostor koji koriste uređaji što mu daje slobodu u postavkama IP usmjeravanja.
- Poslovni subjekt može utjecati na izbor APN-a, naime RADIUS ima mogućnost da uređaju promijeni APN prilikom uspostave veze.
- RADIUS može primati obavijesti o količini prometa koju uređaj generira. Takve obavijesti se šalju sa GGS-PGw čvora u definiranim vremenskim okvirima. Na osnovu tog podatka poslovni subjekt ima uvid u rad uređaja te može poduzeti korektivnu akciju prekida veze u slučaju da uređaj generira previše prometa.
- Budući da RADIUS sudjeluje u uspostavljanju i raskidu veze te može primati i poruke tokom veze, integracijom RADIUS-a sa vanjskim sustavom pruža se uvid u M2M komunikaciju u realnom vremenu.

3.6 Konfiguracija uređaja

APN postavke uređaja se mogu mijenjati izravno na uređaju koristeći metodu automatske detekcije uređaja ADD (Automatic Device Detection). Princip je prikazan na slici 8.



Slika 8: ADD princip promjene APN postavki uređaja

Postoje dva načina na koji se ADD izvršava, ovisno da li je pokrenut iz MSC ili SGSN čvorova, ali je princip rada potpuno isti.

Prilikom registracije u mreži (Location Update ili Routing Area Update) uređaj šalje svoje identifikacijske oznake od kojih su za ADD najvažniji IMEI i IMSI:

- IMSI jednoznačno identificira SIM/USIM karticu (odnosno korisnika),
- IMEI jednoznačno identificira uređaj

Ti podaci se prosljeđuju HLR/HSS čvoru. HLR/HSS čvor će provjeriti kombinaciju IMEI i IMSI te, ako se radi o novoj kombinaciji, poslati podatke prema ADD. Jedan od podataka koji se šalje ADD postupkom je i APN za koji treba podesiti uređaj. Ovisno o uređaju (IMEI) ADD će generirati konfiguracijsku poruku u obliku SMS-a koji će biti proslijeđen do uređaja. Uređaj prepoznaje ovaj SMS kao konfiguracijski te se, uz pristanak krajnjeg korisnika, postavke na uređaju podese automatski.

3.7 M2M SIM/USIM

Temelj pristupa uređaja pokretnoj mreži je SIM/USIM (Subscriber Identity Module / Universal Subscriber Identity Module) kartica u uređaju. Podaci zapisani na SIM/USIM kartici omogućavaju izmjenu sigurnosne informacije između uređaja. I dok se danas SIM/USIM uzimaju zdravo za gotovo (u komunikaciji, primjerice, mobilnim telefonima), SIM/USIM za M2M komunikaciju ipak ima nekoliko specifičnosti.

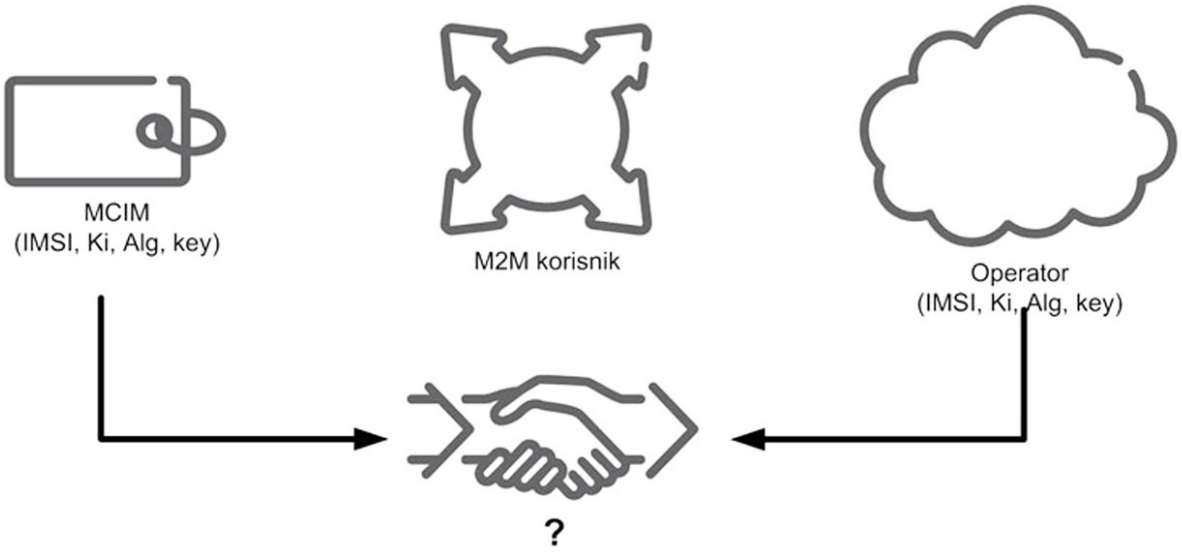
Jedan od bitnih zahtjeva je mogućnost promjene operatora. U današnje vrijeme promjena operatora nužno znači promjenu SIM/USIM kartice (čak i kada se zadržava postojeći pretplatnički broj) jer je SIM/USIM usko vezan uz operatora. U slučaju M2M komunikacije promjena operatora bi značila promjenu velikog broja SIM/USIM kartica što je dugotrajan i skup proces.

Na istom tragu, ali s drugog sigurnosnog stajališta, je ne samo promjena operatora već i definiranje inicijalnog operatora. Naime, kako bi se smanjila mogućnost prijevare, moguće je da će SIM/USIM biti proizvodno fizički vezan za uređaj kao dio samog uređaja, tj. neće se moći odvojiti od uređaja. Ovim se načinom želi obeshrabriti mogući pokušaj krađe SIM/USIM jer bi odvajanjem od uređaja postao neupotrebljiv. Budući da uređaj tokom proizvodnje nije pridijeljen niti jednom operatoru, mora postojati mogućnost početnog pridjeljivanja uređaja i njegovog pripadajućeg SIM/USIM-a operatoru.

Inicijalne postavke kao i promjena operatora znače promjenu podataka koji su do sada bili vezani uz SIM/USIM, kao IMSI i autentikacijski vektori koji su vezani uz operatora te upotrebljeni autentikacijski algoritmi.

U tu svrhu je unutar 3GPP normizacijskog tijela pokrenuta tema vezana uz MCIM modul (Machine Communication Identity Module) namijenjen za M2M komunikaciju, a koji bi obavljao funkcije koje SIM/USIM ima danas u mobilnim telefonima.

Pri tome se nameće pitanje kako MCIM modulu pridijeliti autentikacijske podatke prilikom proizvodnje, a da bi se uspješno mogao koristiti u pokretnoj mreži, jer tijekom proizvodnje još nije odlučeno kojem će operatoru MCIM pripadati (Slika 9). Autentikacijski podaci su IMSI, ključ (Ki), algoritam za kodiranje ključa (Alg) te algoritamski ključ (key).



Slika 9: Povezivanje MCIM modula, M2M korisnika i operatora

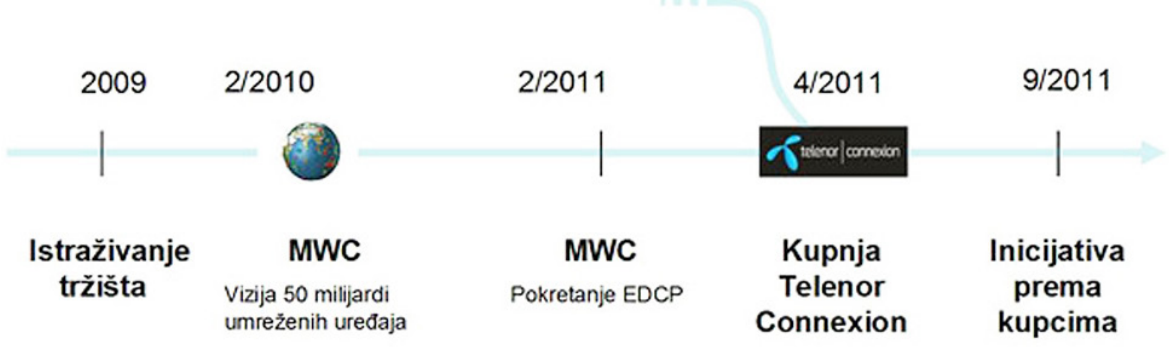
3GPP je dao neke mogućnosti u tehničkom izvještaju 3GPP TR 33.812 koji uključuje nove funkcionalne čvorove koji bi riješili ovu problematiku. To su:

- Connectivity Credential Issuing Function (CCIF) koji bi inicijalno u procesu proizvodnje MCIM pridijelio privremeni IMSI i privremeni Ki kao i adresu DRF,
- Discovery and Registration Function (DRF), čvor koji bi nakon što mu inicijalno pristupi M2M uređaj vratio adresu DPF koji se nalazi kod operatora, koji će dati resurse pokretne mreže za M2M komunikaciju te
- Download and Provisioning Function (DPF), čvor koji ce MCIM instalirati prave autentikacijske podatke

Budući je ovaj standard tek u izradi treba o oprezom uzeti ova nastojanja i vidjeti kako dalje.

4 ERICSSON DCP

Ericsson je vrlo aktivan na području M2M komunikacija sa svojom EDCP (Ericsson Device Connection Platform) ponudom.



Slika 10: Razvoj EDCP platforme

EDCP je kolekcija mrežnih čvorova (GGSN, HLR/HSS, sustav za nadzor….) na jednom mjestu, čija se infrastruktura iznajmljuje operatorima kako bi oni na brz i efikasan način pružili uslugu M2M komunikacije vlasniku M2M uređaja. EDCP također pruža sučelje prema operatoru i poslovnom subjektu kako bi oni imali uvid u stanje M2M komunikacije.

EDCP se sa mrežom operatora povezuje preko postojeće GRX (GPRS Roaming Exchange) i međunarodne signalizacijske mreže.

Prednost EDCP je u činjenici da su sva sučelja i procesi optimizirani za M2M komunikaciju te operator ne mora voditi brigu o održavanju i nadogradnji sustava. Taj dio je u Ericssonovoj nadležnosti pa se operator može posvetiti razvijanju vlastitog M2M posla.

EDCP je redundantno implementirana u Švedskoj i Nizozemskoj. Jedan od zadnjih značajnih kupaca koji će koristiti EDCP je Swisscom koji predviđa da će već kroz nekoliko godina imati 100 milijuna uređaja.

5 Reference

[1] 3GPP TR 33.812 V9.2.0

[2] Packet Core M2M Technical Solution Description, 4/221 02-FGB 101 256

[3] Ericsson Device Connection Platform 1.0, Service description,

[4] “The future of M2M is 3G (and 4G)“, Machina Research, studeni 2011

6 Popis kratica

ADD	Automatic Device Detection
APN	Access Point Name
ARIB	Association of Radio Industries and Businesses
ARPU	Average Revenue Per User
ATIS	Alliance for Telecommunications Industry Solutions
BSC	Base Station Controller
CAGR	Compound Annual Growth Rate
CBS	Cell broadcast
CCIF	Connectivity Credential Issuing Function
CCSA	China Communications Standards Association
CDR	Call Data Record
DPF	Download and Provisioning Function
DRF	Discovery and Registration Function
EDCP	Ericsson Device Connection Platform
EDGE	Enhanced Data rates for GSM Evolution
ETSI	European Telecommunications Standards
ETWS	Earthquake Tsunami Warning System
GGSN-PGw	Gateway GPRS Support Node - Packet Data Network Gateway
GRX	GPRS Roaming Exchange
HLR/HSS	Home Location Register Home Subscriber Server
HSPA	High Speed Packet Access
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IPsec	Internet Protocol Security
LTE	Long Term Evolution
M2M	Machine To Machine
MBMS	Multimedia Broadcast Multicast Service
MCIM	Machine Communication Identity Module
MGw	Media Gateway
MSC-S	Mobile Switching Center - Serving

OTA	Over The Air
PCRF	Policy Control and Charging Rules Function
PDP	Packet Data Protocol
QoS	Quality of Service
RAN	Radio Access Network
SAPC	Service Aware Packet Charging
SGSN-MME	Serving GPRS Support Node - Mobility Management Entity
SIM	Subscriber Identity Module
SMS	Short Message Service
TIA	Telecommunications Industry Association
TTA Korea	Telecommunications Technology Association of Korea
TTC	Telecommunication Technology Committee
TTM	Time To Market
USIM	Universal Subscriber Identity Module
WCDMA	Wideband Code Division Multiple Access

Adrese autora:

Josip Dulj
e-mail: josip.dulj@ericsson.com

Tomislav Blajić
e-mail: tomislav.blajic@ericsson.com

Ericsson Nikola Tesla d.d.
Krapinska 45
p.p. 93
HR-10002 Zagreb
Hrvatska

Uredništvo je primilo rukopis 28. lipnja 2012.