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

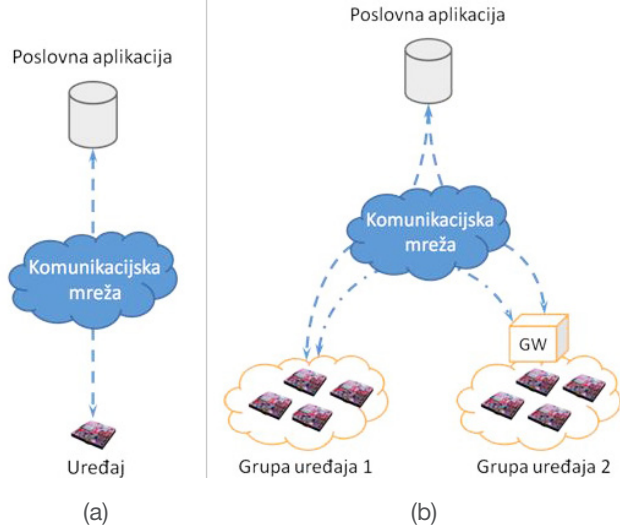
It is our goal in this paper to present some of the major security concerns and issues within the framework of Machine-to-Machine (M2M) communications. One of the key elements for a successful deployment and adoption of such systems is to ensure trustworthiness, authenticity, and privacy of data being 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.

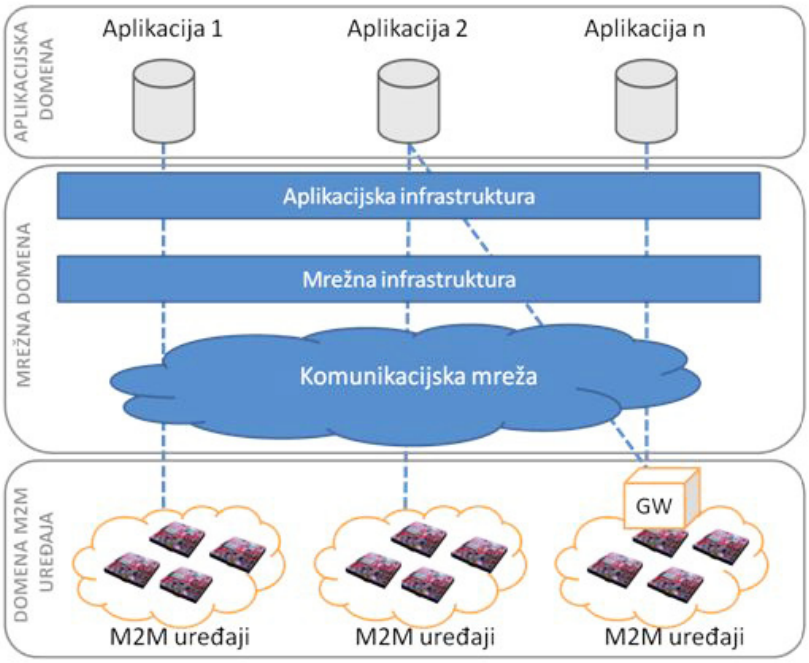
Na slici 1(a) prikazan je uređaj u M2M komunikaciji s odgovarajućom poslovnom aplikacijom. Nadzor i upravljanje razinom tekućine u danom spremniku je primjer aplikacije gdje M2M uređaj periodično komunicira (npr. putem SMS poruka) svoja očitanja backend aplikaciji. Slika 1(b) prikazuje složeni scenarij 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.

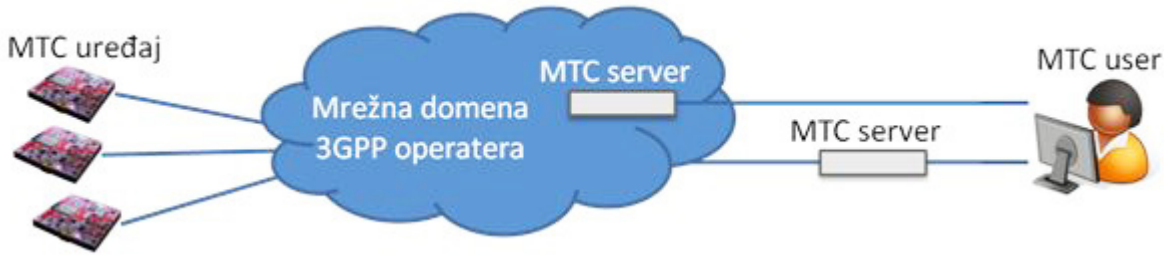
Sličan problem narušavanja privatnosti moguć je i u *smart metering* scenariju. Zamislimo da skupina M2M uređaja komunicira detaljna očitanja potrošnje električne energije (na razini trošila) u danom kućanstvu. S pozitivne strane, prikupljena mjerenja mogu biti osnova za optimiziranje potrošnje električne 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.

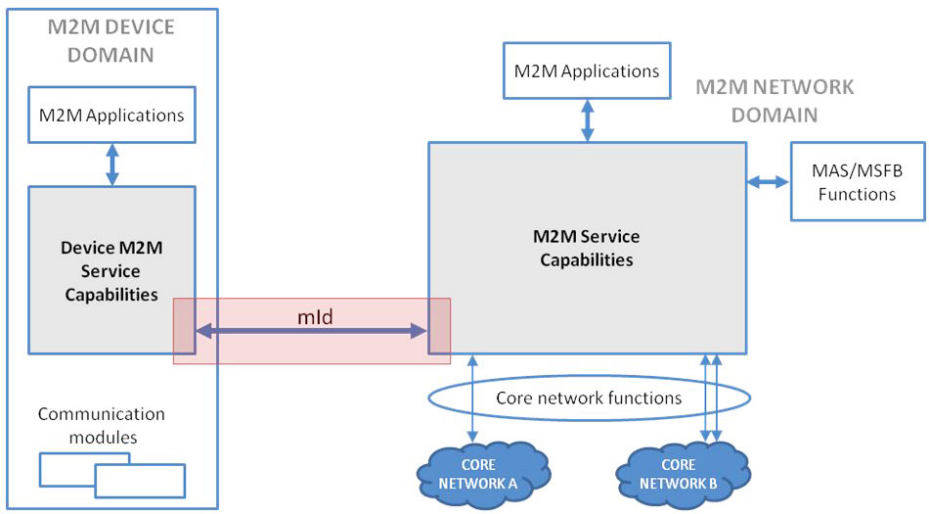
U studiji 3GPP TR 33.812 opisano je nekoliko mogućnosti za zaštitu procesa daljinske administracije USIM/ISIM/MCIM aplikacija u kontekstu 3GPP sustava.

- 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:

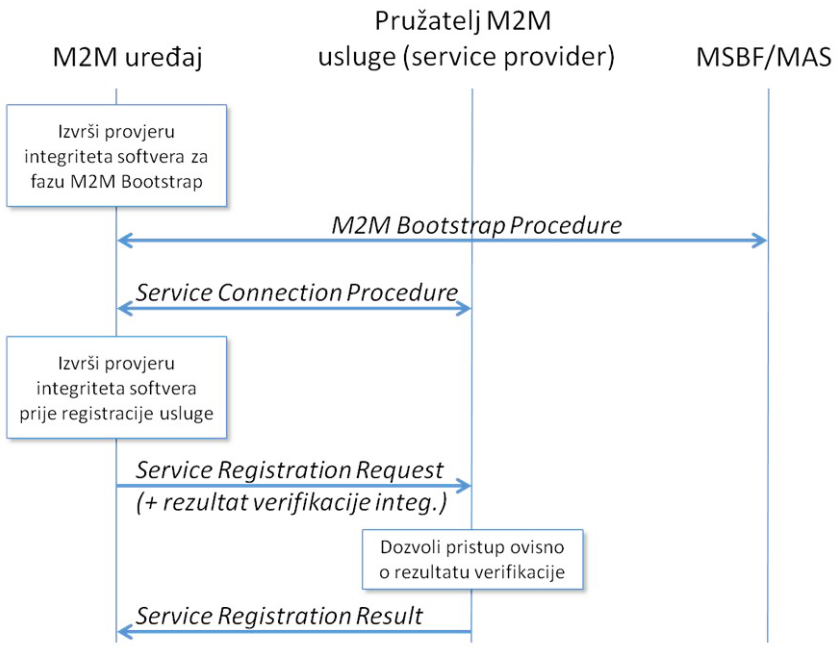
» NSEC (*M2M Network Security Capability*) – sigurnosne funkcionalnosti u mrežnoj domeni
  a. Sigurna inicijalizacija M2M servisa (M2M Service Bootstrap – slika 5).
  b. Realizacija odgovarajuće hijerarhije kriptografskih ključeva (slika 6).
  c. Autentifikacija i uspostava izvedenih sesijskih ključeva.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

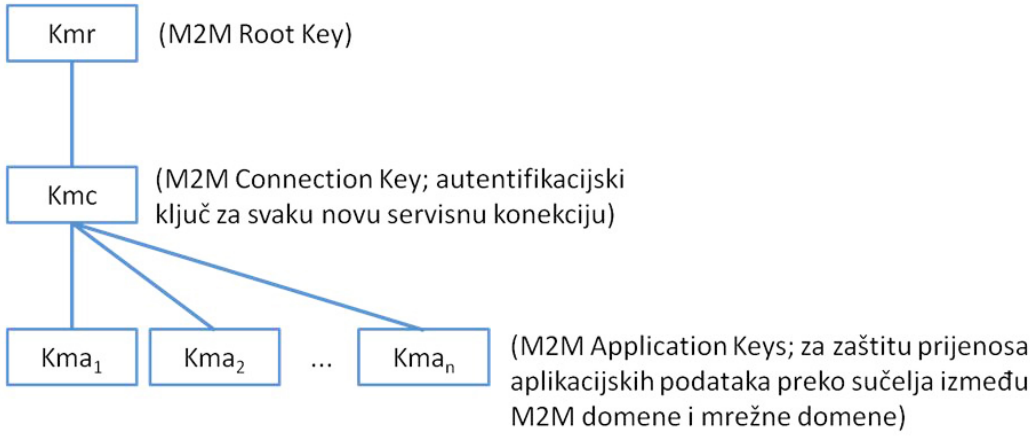
M2M uređaj mora biti inicijaliziran odgovarajućim digitalnim vjerodajnicama (permanentnim autentifikacijskim ključevima i identifikatorima) koji će biti osnova za uspostavu sigurne komunikacije, međusobne autentifikacije, naplate usluga i slično, između servisnih komponenti M2M uređaja i pružatelja M2M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

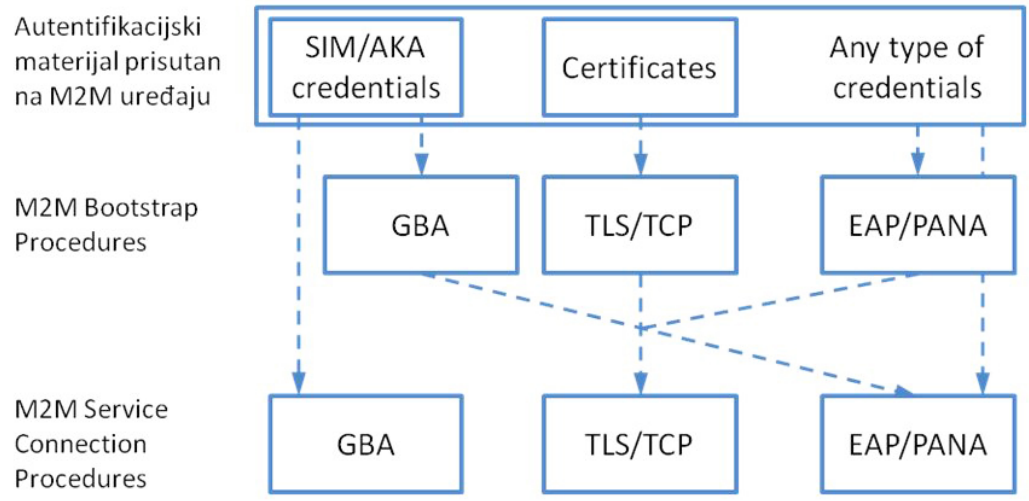


Slika 6: Hijerarhija ključeva za ETSI servisnu razinu

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):

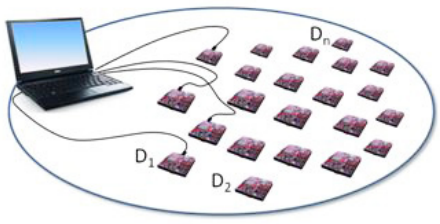
- Međusobna autentifikacija D/G M2M čvora na M2M uređaju i odgovarajućeg pružatelja M2M usluge (za ove potrebe koristi se ključ Kmr – *M2M Root Key* – kojim je M2M uređaj inicijaliziran u prethodnoj fazi).
- Uspostava M2M konekcijskog ključa Kmc (*M2M Connection Key*) i opcijski jednog ili više aplikacijskih 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).

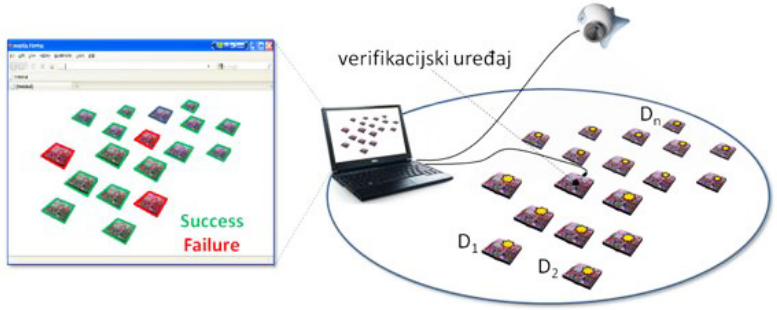
Važno je naglasiti da prema ETSI specifikacijama, svi uređaji u domeni M2M uređaja (slika 2) ne trebaju podržavati i implementirati gore navedene M2M servisne komponente (uljučujući sigurnosne komponente). Takvi uređaji mogu ostvariti vezu s aplikacijskom M2M domenom putem posredničkih M2M uređaja koji 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

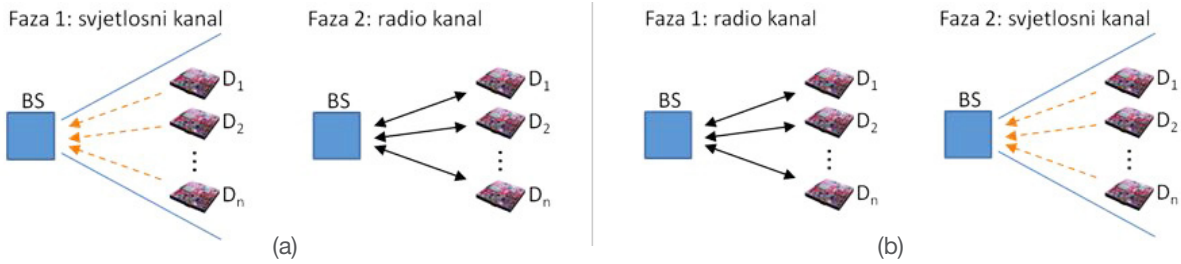
Osnovni preduvjet uspostave sigurne M2M mreže (*M2M Area Network*) i M2M komunikacija je upisivanje inicijalnog kriptografskog materijala (digitalnih vjerodajnica) u M2M uređaje. Ovaj problem se u praksi često zanemaruje ili se smatra trivijalnim. Čak i u 3GPP i ETSI specifikaciji jednostavno se pretpostavlja 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.

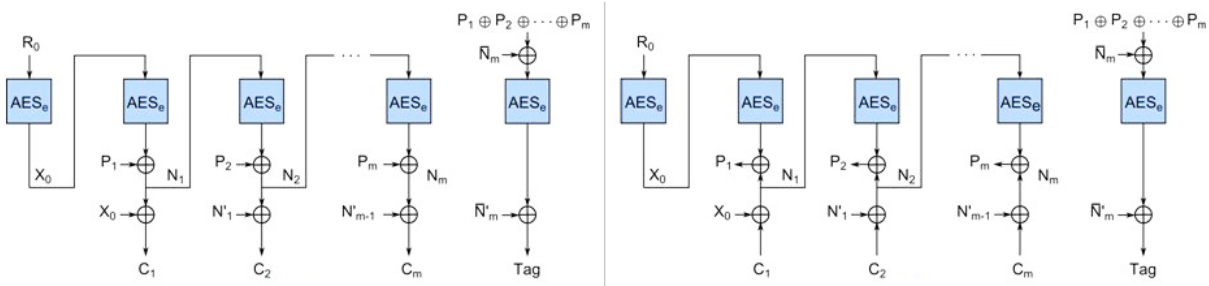
Naša preliminarna studija dviju popularnih AE metoda pokazuje da iste nisu optimalni izbor za primjenu u M2M uređajima ograničenih resursa [19]. Ovdje smo razmatrali sljedeće kriterije optimalnosti: energetska efikasnost, memorijski zahtjevi te licencna prava. Na osnovu ove analize, predložili smo alternativnu, 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.