UDC: 004.42:004.72.057.4 Info M str. 4-10

PROBLEMI AUTENTIFIKACIJE I AUTORIZACIJE U IOT OKRUŽENJU
PROBLEMS OF AUTHENTICATION AND AUTHORIZATION IN THE IOT ENVIRONMENT

Bojan Marčeta
Univerzitet u Beogradu, Fakultet organizacionih nauka

REZIME: Ekspanzija uređaja koji su opremljeni raznim senzorima i imaju mogućnost komunikacije sa drugim uređajima, ili korisnicima, donosi i veliku zabrinutost, uglavnom po pitanju privatnosti i čuvanja podataka koji se prikupljaju. Upravo ta briga i jeste velika prepreka ka još široj primeni IoT paradigme. Periferni uređaji, uglavnom senzori, zbog ograničenih hardverskih mogućnosti, nemaju mogućnost implementacije ozbiljnijih sigurnosnih mehanizama. Imajući na umu ta ograničenja, potebno je pronaći adekvatne protokole ili arhitekture koji će ponuditi sigurnu komunikaciju između perifernih uređaja i korisnika. U ovom radu opisane su osnovne gradivne komponente IoT arhitekture, predstavljene su neke od slabosti IoT uređaja koje se pre svega odnose na bezbednosne rizike prilikom autentifikacije i autorizacije u IoT okruženju. Takođe, navedeni su i primeri upotrebe protokola i arhitektura koje garantuju ili povećavaju bezbednost podataka prilikom autentifikacije i autorizacije periferni uređaja.

KLJUČNE REČI: IoT, IoT bezbednost, autentifikacija, autorizacija

ABSTRACT: Expansion of devices that are equipped with sensors and have the ability to communicate with other devices or users brings great concern, mainly in terms of privacy and data storage that is being collected. This concern is a major obstacle to the wider adoption of the IoT paradigm. Peripheral devices, mainly sensors, due to limited hardware capabilities, do not have the ability to implement heavy-weight security mechanisms. Bearing in mind these limitations, it is necessary to find adequate protocols or architectures that will offer secure communication between peripheral devices and users. In this paper, the basic components of IoT architecture are described, some of the weaknesses of IoT devices are presented, which are primarily related to security risks during authentication and authorization in the IoT environment. Also, there are examples of using protocols and architectures that guarantee or increase data security during authentication and authorization process.

KEY WORDS: IoT, IoT security, authentication, authorization

1. UVOD

U vremenu u kome dominiraju mobilni telefoni i ostali prenosivi uređaji, internet je došao do faze razvoja koja se naziva *semantic web*. Ideja je da se online sadržaj učini razumljivijim i lakše dostupnim samim mašinama tj. uređajima, koje će, uz pomoć naprednih algoritama za pretragu sadržaja, imati mogućnost da samostalno prikupljaju, obrađuju i dele informacije sa drugim uređajima, i to bez interakcije sa korisnikom. Pored razvoja internet tehnologija, veliki napredak se desio i u oblasti senzorskih mreža i RFID uređaja. Spajanjem ovih tehnologija proširili su se vidici i otvorile su se nove mogućnosti. Nastala je ideja o kreiranju okruženja u kome bi objekti koji nas svakodnevno okružuju, opremljeni odgovarajućim hardverom i softverom, bili u mogućnosti da komuniciraju međusobno, ili da komuniciraju sa drugim mašinama ili uređajima putem interneta, u cilju obavljanja određenih korisnih zadataka. Ova ideja predstavlja nastanak nove paradigme - Internet of Things [1]. Prema nekim istraživanjima, broj IoT uređaja bi mogao da dostigne brojku od 50 milijardi do 2020. godine. Usluge bazirane na IoT će biti ključna tehnologija u razvoju pametnih gradova, koji će u potpunosti promeniti način na koji obavljamo posao, brinemo o svom zdravlju, edukujemo se, zabavljamo i štitimo sebe [2].

Iako se u današnje vreme pojam *Internet of Things* sve više upotrebljava, još uvek ne postoji opšteprihvaćena definicija. Sam pojam *Internet of Things* je nastao pre skoro 20 godina i zapravo se odnosio na rad Auto-ID centra na MIT sa identifikacijama radio-frekvencija (RFID) [3]. Kevin Ešton, osnivač Auto-ID centra, smatra se tvorcem termina IoT. Predstavio je svoju ideju života u kome je Internet povezan sa realnim svetom putem sveobuhvatnih senzora i odgovora, odnosno povratnih informacija [4]. Pojam IoT se vezuje za svaki objekat ili uređaj, bilo fizički ili virtuelni, koji je povezan na Internet i ima mogućnost komunikacije sa korisnicima ili drugim uređajima [5].

Međunarodna unija za telekomunikacije ITU (*International Telecommunication Union)* definiše IoT kao "*globalnu infrastrukturu za informaciono društvo koja omogućava napredne servise kroz povezivanje (fizičko i virtuelno) stvari koje su zasnovane na postojećim i razvojnim interoperabilnim informacijama i komunikacionim tehnologijama*" [6].

Iako ne postoji jedinstvena definicija IoT, suština je da se objekti, sa kojima se susrećemo svakodnevno, mogu dopuniti svojstvima poput identifikacije, detekcije, povezivanja i procesiranja, koja će im omogućiti da komuniciraju sa drugim uređajima i servisima i ostvare značajne ciljeve. Sama ideja direktne komunikacije mašina postoji već dugi niz godina. IoT zapravo predstavlja evoluciju postojećih tehnologija, odnosno cilj je povezati tehnologiju sa uređajima koje svakodnevno koristimo [1]. Samo neki od primera su pametne kuće sa inteligentnim termostatima i bezbednosnim sistemima, ili pametne saobraćajne kamere koje nadgledaju promet i frekvenciju vozila, ili pametni sistemi za upravljanje javnom rasvetom i odnošenjem smeća u većim gradovima.

2. IOT ARHITEKTURA

Arhitektura IoT se obično može predstaviti iz tri dela tj. sloja: (1) sloj uređaja ili fizičkih stvari (objekata); (2) sloj veze

tj. komunikacioni sloj, i (3) *cloud* sloj. Sloj uređaja podrazumeva postojeći hardver kome su pridodate određene softverske funkcionalnosti i određene komponente specifične za IoT (senzori, okidači itd.). Na sloju veze se nalaze protokoli koji obezbeđuju komunikaciju između uređaja i oblaka. Na sloju oblaka nalazi se softver koji upravlja povezanim uređajima, kao i aplikativna platforma koja omogućava razvoj i izvršavanje IoT aplikacija. Takođe, ovde se prikupljaju i skladište podaci koji su generisani od različitih uređaja kako bi se kasnije obradili i analizirali [3].

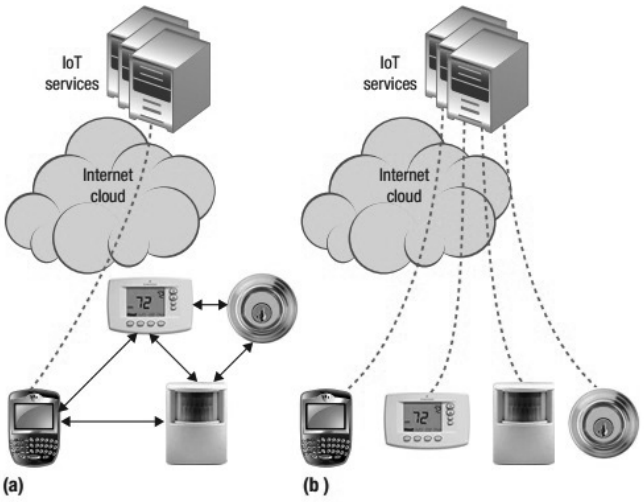
Većina perifernih komponenti IoT arhitekture su već dugo u upotrebi i široko su rasprostranjene. Neki od ključnih elemenata hardvera su RFID uređaji, NFC tehnologija, bežične senzorske mreže (WSN) i QR kodovi.

Senzori su uređaji koji prate ili mere određene parametre u okruženju, npr. senzori pokreta, senzori koji mere temperaturu, vlažnost itd. Kada se istovemeno koristi više senzora koji međusobno komuniciraju to se naziva *Wireless Sensor Network* (WSN). Senzorske mreže se mogu sastojati od velikog broja inteligentnih senzora koji prikupljaju korsine informacije i šalju ih, obično kroz neki *gateway*, ka centralnom serveru koji vrši prikupljanje, obradu i analizu prikupljenih podataka [7]. Okidači (*actuators*) pokreću određenu akciju koja će se desiti u okruženju ili na samom uređaju na kome se nalazi senzor [1]. Na primer, ako senzor ima zadatak da meri prisustvo dima u prostoriji, u slučaju pojave dima okidač će upaliti protivpožarni sistem.

2.1. *CENTRALIZOVANA ILI DISTRIBUIRANA ARHITEKTURA*

Večita dilema u svetu računarstva odnosi se na pitanje da li je bolje imati centralizovani ili distribuirani sistem. Po tom pitanju, tokom evolucije informacionih tehnologija, nekoliko puta se menjala paradigma. Prvo su postojali centralizovani *mainframe* računari, a potom se prešlo na decentralizovane personalne računare koji su pokretali tzv. *standalone* aplikacije, da bi se danas ponovo prešlo na centralizovane *cloud* servise. Nihova prednost je što se njima lakše i brže upravlja i svakako su finansijski isplativiji od izgradnje i održavanja sopstvenih centara podataka, kreiranja backup-a, fizičkog obezbeđivanja prostorija i sl. U tom smislu, veoma je pogodno koristiti *cloud* arhitekturu u IoT. To bi značilo da je svaki uređaj registrovan na *cloud* servisu i sa njim samostalno komunicira. U ovom slučaju bi postojali i određeni kompromisi kada je u pitanju kašnjenje, bezbednost, privatnost i cena. Ako se sve to zanemari, *cloud* pristup je prihvatljivo rešenje.

Svaki uređaj koji je u stanju da ostvari direktnu vezu sa internetom mora da ima Ethernet, Wi-Fi ili *cellular* modem, što znatno povećava njegovu cenu i povećava potrošnju energije. U tom slučaju mnogo je bolji Peer-to-Peer pristup, u kome postoji jedan uređaj (*bridge*), koji ima Wi-Fi pristup ka internetu, a svi ostali periferni uređaji komuniciraju sa njim. Informacije se u tom slučaju šalju ka internetu samo preko tog uređaja koji se još naziva i *gateway*. Periferna komunikacija sa centralnim uređajem bi se odvijala preko nekih od komunikacionih standarda kao što su ZigBee, 6loWPAN, BLE i drugi [8].



Slika 1. *(a) Peer-to-Peer ili (b) cloud arhitektura*

3. BEZBEDNOSNI RIZICI

Sa svim prednostima i mogućnostima koje donosi IoT dolaze i mnoge brige kada je u pitanju sigurnost. U današnje vreme milijarde uređaja imaju pristup internetu, što daje širok spektar mogućnosti napadačima da iste kompromituju i da njima manipulišu. Napad na IoT uređaj može se izvesti na svakom od gore pomenutih nivoa - hardverskom, mrežnom ili *cloud* nivou. U nekim slučajevima napadač može pristupiti hardveru uređaja i potom preuzeti ključeve ili sigurnosne parametre koji su skladišteni u samom uređaju. Sa ukradenim podacima napadač može napraviti fizičku ili virtuelnu kopiju kompromitovanog uređaja i poslati lažne podatke na server sa kojim je uređaj povezan. Isto tako, preko iste te mreže, napadač od servera može preuzeti poverljive podatke. Postoje i napadi u kojima je moguće doći do sigurnosnih parametara uređaja bez fizičkog pristupa istom. Takvi napadi su poznati pod nazivom *side channel attack.* Kada je u pitanju mrežni (komunikacioni) sloj, ni tu rizici nisu ništa manji. Sada već čuveni MIRAI malver je primer takvog napada u kome su mnogi IoT uređaji bili napadnuti spolja i posle iskorišćeni kao zombiji za napad na druge sajtove i servise. Od 2013. godine primećen je porast DDoS napada putem SSDP (*Simple Service Discovery Protocol*) protokola koji je veoma zastupljen kod IoT uređaja [9].

Prema istraživanju koje je sproveo HP ispostavilo se da je na 90% testiranih IoT uređaja skladišten barem jedan lični podatak. 80% uređaja, zajedno sa svojim pratećim mobilnim ili *cloud* aplikacijama, nije u stanju da od korisnika zahteva dovoljno kompleksnu i dugačku lozinku. 70% uređaja ne koristi kriptovanu komunikaciju ka internetu ili lokalnoj mreži. 70% IoT uređaja ostavlja mogućnost napadaču da dođe do informacija o korisničkom nalogu metodom pogađanja. 6 od 10 IoT uređaja koji imaju korisnički interfejs su imali brojne ranjivosti poput XSS (*Cross Site Scripting*) [10].

Još jedan od primera napada preko mreže desio se u Ukrajini 2015. godine. U tom sajber napadu napadači su preuzeli kontrolu nad SCADA (*Supervisory Control and Data Acquisition*) sistemom koji je zadužen za snabdevanje električnom energijom regije u kojoj je naseljeno 1,5 miliona stanovnika. Cela regija je bila u potpunom mraku nekoliko sati. Iako ovaj napad nema konkretno veze sa IoT uređajima on treba da ukaže na potencijalne opasnosti i moguće posledice, ne samo na pojedinca nego i na širu društvenu zajednicu. U nekim situacijama može doći do curenja poverljivih informacija, krađe ličnih podataka i slično, a u nekim drugim, kao što je navedeno u ovom primeru, opasnost može biti mnogo veća - nekome možda može biti ugrožen i život [11].

Autentifikacija, autorizacija, privatnost i poverljivost podataka predstavljaju najveće sigurnosne probleme u IoT. Uređaji sa odgovarajućim mehanizmom autentifikacije mogu izbeći mnoge od gore pomenutih pretnji. Mnogi istraživači su radili i još uvek rade na pronalaženju takvog sigurnog mehanizma autentifikacije, ali problem je što ne postoji univerzalno rešenje. Mehanizam koji je dobar u jednom okruženju ne mora biti dobar u nekom drugom. Dodatan problem predstavljaju brojna ograničenja uređaja ili samog okruženja. Na primer, *Bluetooth* tehnologja, koja se često koristi za komunikaciju perifernih uređaja u IoT, je kratkog dometa. Bežične senzorske mreže se često oslanjaju na signal koji nije konstantnog kvaliteta i sl. Sami uređaji imaju jako malu ili skoro nikakvu mogućnost obrađivanja podataka ili implementacije ozbiljnijih sigurnosnih protokola ili mehanizama za enkripciju. Skladišni prostor im je veoma ograničen. Svaki dodatni "napor" koji neki mali uređaj mora da uloži mu značajno povećava potrošnju energije i samim tim smanjuje autonomiju. Odličan primer su RFID uređaji i njihove baterije. Pored svega pomenutog tu su i problemi interoperabilnosti zbog prisustva brojnih standarda i samostalnih rešenja koji nisu usklađeni. Organizacija DLNA (*Digital Living Network Alliance*) je imala zadatak da poveže i omogući deljenje između uređaja različitih proizvođača, ali do sada je uspela da poveže samo manji broj njih.

Još jedan od problema sa kojima se suočava IoT jeste pouzdanost transportnog sloja, koju može omogućiti TCP. TCP zahteva uspostavljanje konekcije "trostrukim rukovanjem", što u slučaju IoT nije neophodno jer često dolazi do malih razmena podataka. Još jedan od nedostataka TCP jeste baferovanje podataka sa obe strane prenosa, a upravljanje baferima bi bez potrebe trošilo resurse [12].

Iz svega pomenutog lako se može zaključiti da je jako veliki izazov kreirati poptuno siguran IoT ekosistem. Zbog toga ni ne čudi tolika zabrinutost i strah ka širem prihatanju IoT paradigme. Upravo taj strah predstavlja i najveću prepreku ka širem prihvatanju ove tehnologije od strane korisnika, vlada i industrije. Najveća zabrinutost se odnosi na kontrolu uređaja i podataka kojima isti raspolažu. U incidentu koji je obuhvatio više od 150000 IoT uređaja, kao glavni razlog curenja podataka navodi se problem sa upravljanjem kontrolom pristupa samim uređajima. Potencijalno rešenje koje treba da ponudi potpuni nadzor nad kontrolom pristupa uređajima treba da obuhvati tri problema: autentifikaciju, autorizaciju i reviziju (*auditing*). Autentifikacija, kao prvi korak, podrazumeva proveru identiteta subjekta koji pristupa datom objektu. Zatim sledi autorizacija koja podrazumeva proveru prava koje ima subjekat nad datim objektom. Preciznije rečeno, proverava se koje radnje ili operacije subjekat ima dozvolu da izvršava. Na kraju, tu je i revizija koja podrazumeva kasniju analizu realizovanih aktivnosti na datom sistemu [13]"page":"1-6","source":"Crossref","event":"2017 IEEE Global Communications Conference (GLOBECOM 2017.

4. PREDLOZI REŠENJA

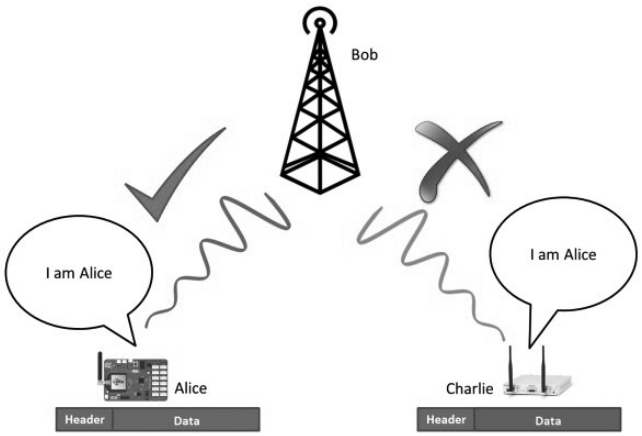
U nastavku ovog rada prikazana su neka od mogućih rešenja problema autentifikacije i autorizacije. U nekima od njih autori su predložili kompletna okruženja (*framework*), dok je u drugima predložena primena određenih protokola i mehanizama.

4.1 *PREPOZNAVANJE NESAVRŠENOSTI HARDVERA KOJI EMITUJE SIGNAL*

Kao jedna od veoma značajnih komponenti u IoT ekositemu pojavljuju se uređaji izuzetno male snage (*low-power*) koji uz pomoć različitih bežičnih tehnologija imaju mogućnost komunikacije sa drugim uređajima u oblaku. Rešenja poput LoRaWAN (*Long Range WAN*), NB-IoT (*NarrowBand IoT*) i SIGFOX omogućavaju malim uređajima, koji u sebi imaju baterije koje im garantuju desetogodišnju autonomiju, da komuniciraju sa signalnim tornjevima koji su i po nekoliko kilometara udaljeni. Takav način komunikacije, upotrebom male snage, ima svoje nedostatke - sigurnosne ranjivosti. Ranjivost dolazi do izražaja u trenucima kada mali uređaji pokušavaju da se autentifikuju ka svojoj baznoj stanici u okruženju u kome su prisutni uređaji, moguće i napadači, koji imaju mnogo veću snagu. Takvi uređaji imaju mnogo veću moć obrade podataka, a imaju i mogućnost reprodukcije delova signala koji šalju slabi uređaji. Na neki način može se reći da imaju mogućnost da ih oponašaju. U nastavku je prikazano moguće rešenje problema identifikacije uređaja u prostoru u kome se signali različite snage mešaju tj. nadmeću.

Autori [14] su došli na ideju da pokušaju na neki način jedinstveno da identifikuju svaki uređaj. Ideja se zaniva na kreiranju tzv. otiska (*fingerprint*) uređaja. I ranije je bilo nekih predloga [15], [16] Florida, USA","page":"441","source":"Crossref","event":"the 19th annual international conference","event-place":"Miami, Florida, USA","abstract":"Despite the important role that WiFi networks play in home and enterprise networks they are relatively weak from a security standpoint. With easily available directional antennas, attackers can be physically located off-site, yet compromise WiFi security protocols such as WEP, WPA, and even to some extent WPA2 through a range of exploits specific to those protocols, or simply by running dictionary and human-factors attacks on users' poorly-chosen passwords. This presents a security risk to the entire home or enterprise network. To mitigate this ongoing problem, we propose SecureArray, a system designed to operate alongside existing wireless security protocols, adding defense in depth against active attacks. SecureArray's novel signal processing techniques le-

verage multi-antenna access point (AP da se uređaji prepoznaju na osnovu njihove lokacije, međutim to nije dalo dobre rezultate u situacijama kada se napadači nalaze neposredno pored uređaja koje je trebalo identifikovati.



Slika 2. *Prepoznavanje legitimnih uređaja naspram malicioznih koji ih oponašaju*

Autori su predstavili sistem koji bezbedno identifikuje uređaje male snage i pored prisustva hardveski jačih i superiornijih uređaja. Ideja je da se uz pomoć arhitekture zasnovane na mašinskom učenju uoče hardverske nesavršenosti uređaja male snage i da se u tim uzorcima prepoznaju jedinstvenosti.

Većina tehnika mašinskog učenja zahteva da se veoma precizno definišu karakteristike na osnovu kojih će moći da se klasifikuje pripadnost signala određenim korisnicima ili uređajima. Pošto je poprilično teško definisati ove karakteristike ručno, u ovom slučaju korišćene su neuronske mreže koje uče hijerarhijske nelinearne karakteristike i koje su u stanju da otkriju skrivene strukture u podacima koji se šalju. Korišćena je posebna klasa neuronskih mreža pod nazivom LSTM (*Long Short Term Memory*) koje se obično koriste u automatskom prepoznavanju govora i predviđanju finansijskih podataka.

Veliki izazov bio je pronaci optimalan odnos između složenosti sistema i kvaliteta klasifikacije signala. Zbog toga je bilo veoma važno precizno definisati dužinu tj. veličinu uzorka. Duži uzorci nose više informacija, ali su i zahtevniji u obradi, kako procesorski tako i vremenski. Testiranje je podrazumevalo da su signali koje šalju legitimni uređaji unapred snimljeni kao uzorci u fazi treniranja sistema. Takođe, pretpostavka je da se kao uljezi mogu pojaviti uređaji male snage (mW) i uređaji veće snage (do 1 W).

Testno okruženje je podrazumevalo upotrebu jednog legitimnog uređaja i 29 uljeza. Na strani predajnika korišćeni su Semtech SX1274, dok su za prijem korišćeni SX1257 čipovi. Bitno je napomenuti da su svi uređaji slali identičnu poruku, što testiranje čini realnim. U tom slučaju veliki je izazov bio na strani prijemnika prepoznati signal koji dolazi od legitimnog uređaja. Kao rezultat testiranja potvrđena je početna hipoteza da je moguće upotrebom neuronskih mreža prepoznati različite signale na osnovu hardverskih nesavršenosti predajnika koji ih šalju. Detaljniji prikaz preciznosti prepoznavanja je prikazan na slici ispod.

.	*Accuracy (%)*		
Placement	*1-layer* LSTM	*2-later* LSTM	*3-layer* LSTM
LOS (< 1 m)	97.45	**99.58**	96.60
LOS (>15 m)	89	**90.74**	88.42
NLOS	84.48	85.28	**88.10**

Slika 3. *Klasifikacija preciznosti sistema u zavisnosti od scenarija*

4.2 *ANALIZA PONAŠANJA SENZORA*

Trenutna sigurnosna rešenja su daleko od zadovoljavajućih i teško da mogu da spreče eksponencijalni rast i sve veću složenost sajber napada. Postoje dve osnovne tehnike sa kojima se može detektovati sajber napad. U jednu grupu spadaju IDS (*Intrusion Detection System*) sistemi koji se oslanjaju na prepoznavanje potpisa napada (*signature*), dok se u drugu grupu svrstavaju sistemi zasnovani na analizi anomalija u ponašanju uređaja. Sistemi koji rade na principu prepoznavanje potpisa napada se uglavnom oslanjaju na već postojeću bazu sa poznatim vrstama napada. Njihov nedostatak se ogleda u tome što nisu u stanju da prepoznaju nove vrste napada, čak ni neke postojeće ako im je samo malo promenjen potpis. Sa druge strane, sistemi koji se oslanjaju na prepoznavanje ponašanja uređaja u stanju su da prepoznaju nove napade. Ovakvi sistemi se oslanjaju na kreiranje šablona ponašanja uređaja kroz fazu treninga, da bi kasnije mogli svako odstupanje od tog ponašanja da smatraju za anomaliju.

U nastavku je prikazana metodologija [2] koja štiti krajnje uređaje (senzore) tako što ih konstatno nadzire i beleži anomalije u njihovom ponašanju. Osnovni koraci ovog pristupa su: (1) konstantni nadzor uređaja, (2) podaci o ponašanju senzora (*Sensor Behavior Data Structures*), (3) analiza neuobičajenog ponašanja (*Anomaly Behavior Analysis),* (4) klasifikacija senzora, i (5) akcije opravka.

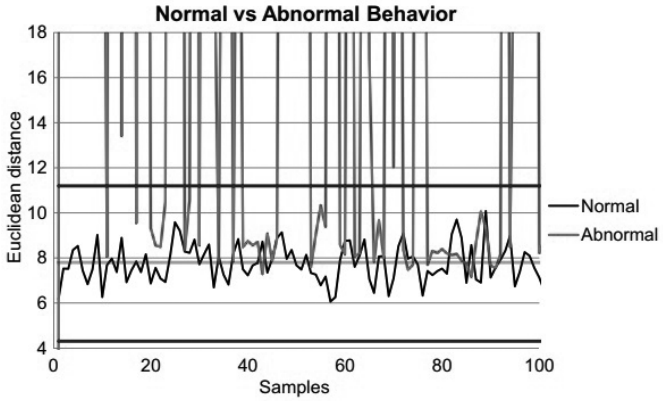
Prva faza je snimanje saobraćaja koji šalju senzori u njihovom normalnom režimu rada. U ovu svrhu korišćen je alat Wireshark. Podaci koji su uzimani su izvorišna i destinaciona IP adresa, kao i sadržaj paketa. Proces snimanja se odvijao između kontrolera i sigurnog *gateway*-a tako da je moguće zabeležiti eventualnu anomaliju i pre nego što paketi stignu do *gateway*-a. Na osnovu prikupljenih podataka identifikuje se senzor i kreira se njegov radni profil (s-DNA). Za ovo je zadužen modul SBDS. Profili se kreiraju upotrebom DWT (*Discrete Wavelet Transform*) metode i beleže se u formi matrice. Ovi profili se čuvaju u ABA modulu koji obavlja nekoliko zadataka: (1) izračunava DWT koeficijente iz dobijenih signala, (2) na osnovu primljenih podataka utvrđuje tip senzora i (3) kreira radni profil senzora kako bi mogao isti da uporedi sa već postojećim s-DNA.

Prilikom kreiranja baze uzoraka normalnog ponašanja vrši se tzv. treniranje senzora. Sledeći korak je snimanje ponašanja senzora kada je pod napadom. U konkretnom eksperimentu primenjeni su sledeci napadi: *replay*, *delay*, DoS, *flooding*, *sensor impersonation*, *pulse DoS* i *noise injection*.

Nakon toga, prati se ponasanje senzora u radu, i ti uzorci se porede sa već kreiranim šablonima od ranije. Ukoliko se uoči

određeno odstupanje (devijacija) pretpostavka je da je došlo do određenog incidenta (napada i sl.). Sledeći korak je pokušaj da se utvrdi o kojoj vrsti napada je reč (klasifikacija), ako je to uopšte i moguće jer postoji mogućnost da je u pitanju neki novi (za sada nepoznati napad). U zavsinosti od klasifikacije napada preduzimaju se određene akcije (odbacivanje podataka koje senzor šalje, zahtev za ponovnom autentifikacijom senzora, promena mrežne konfiguracije).

Prilikom testa, kao glavni kontroler je korišćen Arduino UNO, a za *gateway* je izabran Raspberry PI 3. Prilikom testiranja kreirana je baza od 500 uzoraka.



Slika 4. *Prikaz normalnog ponašanja naspram ponašanja kada je uređaj pod DoS napadom*

Attack	Detection Rate	Classification Rate
Replay Attack	98%	98%
Delay Attack	98%	88%
DoS Attack	99.9%	98%
Flooding Attack	98%	98%
Sensor Impersonation	97.4%	85%
Pulse DoS	96%	93%
Noise Injection	100%	95%

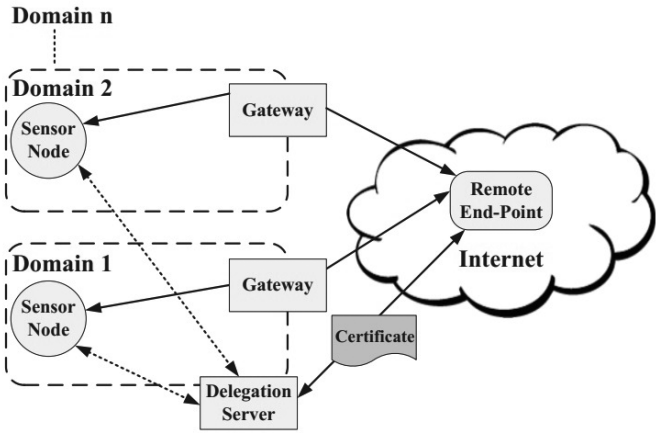
Slika 5. *Uporedni prikaz uspešnosti detekcije i klasifikacije napada*

Iz priloženih rezultata može se videti da ova metodologija u proseku pokazuje uspešnost klasifikacije od 98% kod poznatih napada, i 97,4% kod nepoznatih napada. Važno je napomenuti da je ovakakav pristup moguće primeniti samo u okruženju sa konačnim brojem uređaja.

4.3 *IOT U SISTEMIMA ZDRAVSTVENE ZAŠTITE*

Rastući troškovi zdravstvene zaštite i učestalost hroničnih bolesti širom sveta zahtevaju određenu transformaciju sistema zdravstvene zaštite. Ta transformacija predstavlja prelazak sa sistema koji su bili orijentisani na ustanove tj. bolnice, na sisteme kojima je u fokusu korisnik tj. pacijent [17]. Predviđa se da će se način pružanja zdravstvene zaštite u narednim decenijama drastično promeniti. Akcenat će sa centara u kojima se pruža zdravstvena nega biti polako pomeren ka modelu bolnica-kuća u narednih deset godina, da bi već od 2030. sva pažnja bila usmerena ka kućnom lečenju pacijenata [18]. Ovakav zaokret podrazumeva i veću upotrebu IoT arhitekture. Veća upotreba IoT uređaja u zdravstvenim sistemima podrazumeva baratanje sa osetljivim podacima pacijenata koji mogu biti prikupljeni iz različitih izvora. Obično su to bezazleni mali senzori koji prate određene parametre stanja pacijenta i te podatke beleže ili šalju negde na obradu. U nekim slučajevima to mogu biti veoma poverljivi podaci. Logično je da postoji određena zabrinutost po pitanju privatnosti od strane korisnika ovakvih sistema. Upravo to je jedna od većih prepreka ka masovnijem korišćenju aplikacija kućne nege zasnovanih na IoT arhitekturi.

U ovakvom okruženju, u kome uređaji pre svega bežično komuniciraju, potrebno je primeniti neke nove mehanizme zaštite koji će biti prilagođeni uređajima koji se koriste. Jasno je da konvencijalne metode zaštite ne mogu biti od koristi u ovakvom okruženju pre svega zbog ograničenih resursa IoT senzora. Bilo je ranije napora da se kreiraju pametni *gateway*-i za aplikacije e-zaštite bazirane na IoT uređajima. Takvi uređaji (*gateway*-i) su uglavnom obavljali neke jednostavne operacije kao što je npr. usklađivanje komunikacije (prevođenje protokola) između interneta i unutrašnje mreže u kojoj rade senzori. U nastavku je opisana arhitektura [19] za sigurnu i efikasnu autentifikaciju i autorizaciju u IoT okruženju zdravstvene zaštite zasnovana na distribuiranim pametnim *gateway*-ima. Arhitektura ima naziv SEA (*Secure Efficient Authentication/ Authorization*). Ova arhitektura koristi prednosti koje imaju *gateway*-i po pitanju resursa. Omogućava da se deo opterećenja prebaci na *gateway* i da se tako senzori rasterete i da im se omogući da komuniciraju unutar nezavisnog domena. Pružaju i mogućnost kreiranja konekcija ka senzorima i na taj način se izbegava nepotrebna autentifikacija ili autorizacija senzora ka udaljenim centrima zdravstvene zaštite. Pored toga, svaka zlonamerna aktivnost može biti blokirana na *gateway*-u pre nego uđe u ograničeni domen.

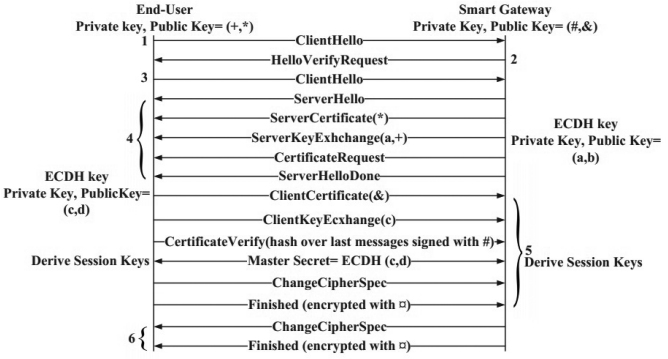


Slika 6. *Arhitektura e-health nadzora bazirana na IoT*

Na slici 6 prikazan je konvencionalni sistem pametnog e-health okruženja za praćenje zdravstvenog stanja. U ovakvom sistemu, određeni zdravstveni parametri se snimaju na senzore koji su prikačeni na telo pacijenta. Ovim podacima se obično mogu dodati i informacije o datumu, vremenu, lokaciji i temperaturi, koji zajedno mogu olakšati uočavanje određenih problema i bolje sagledavanje konkretne situacije. Predlože-

na SEA arhitektura sastoji se od sledećih komponenti: i) MSN (*Medical Sensor Network*) koja podrazumeva identifikaciju, praćenje i prijem signala sa tela pacijenta ili iz prostorije. Ovi signali se zatim prosleđuju ka *gateway*-u bežičnim ili žičnim putem (Serial, Wi-Fi, Bluetooth). ii) *Smart e-Health Gateway,* predstavlja tačku spajanja između MSN i interneta i podržava različite komunikacione protokole. Prihvata podatke iz različitih podmreža, vrši konverziju protokola po potrebi i pruža usluge višeg nivoa kao što su agregacija podataka i filtriranje. iii) *Back-End System,* sastoji se od lokalnog sviča (*switch*), *cloud* platforme, skladišta podataka i lokalne baze podataka bolnice koja se povremeno sinhronizuje sa skladištem u oblaku.

SEA arhitektura koristi pametne distribuirane *e-health gateway*-e kako bi se sigurno i efikasno izvršila autentifikacija i autorizacija udaljenih korisnika, umesto da se ti procesi obavljaju na samim senzorima. Kao što je ranije pomenuto, glavna uloga *gateway*-a je da podrži različite bežične protokole i internu komunikaciju između uređaja. U kontekstu IoT zdravstvene zaštite *gateway* dobija i neke dodatne funkcionalnosti. Može da se ponaša kao lokalni repozitorijum, može da privremeno skladišti podatke od senzora i pacijenata ili da vrši analizu i agregaciju prikupljenih podataka. Najveća odgovornost *gateway*-a je da obezbedi sigurnu komunikaciju senzora sa udaljenim korisnicima. Ideja SEA arhitekture polazi od pretpostavke da *gateway* i krajnji korisnik imaju dovoljno resursa kako bi mogli da podrže upotrebu kompleksnijih sigurnosnih mehanizama poput npr. efikasne validacije sertifikata. Kako bi se obezbedila sigurna veza između krajnjeg korisnika i medicinskog uređaja sa ograničenim resursima uvedena je podrška za sigurnosni DTLS (*Datagram Transport Layer Security*) [20] tampering, or message forgery. The DTLS protocol is based on the Transport Layer Security (TLS protokol. Pre nego što krajnji korisnik stupi u vezu sa senzorom on mora da se autentifikuje i autorizuje preko *gateway*-a. Na taj način *gateway* može na siguran način da dozvoljava samo proverenim korisnicima da komuniciraju sa senzorima. Nakon obostrane uspešne autentifikacije krajnjeg korisnika i *gateway*-a, autorizovanom korisniku se dozvoljava da svoje upite prosleđuje ka senzoru. Da bi komunikacija u potpunosti bila sigurna neophodno je da se i senzor i *gateway* obostrano autentifikuju unutar mrežnog domena pametne bolnice. To se postiže upotrebom DTLS *handshake*-a baziranog na javnom ključu između oba entiteta.



Slika 7. *DTLS handshake između krajnjeg korisnika i gateway-a*

Osnovne prednosti predstavljene SEA arhitekture se ogledaju pre svega u činjenici da je ogroman deo posla (autentifikacija i autorizacija korisnika) prebačen na distribuirani pametni *gateway*, što je u poređenju sa konvencionalnom arhitekturom dovelo do značajnog smanjenja kašnjenja i nepotrebnog saobraćaja (*overhead*). Pored toga, povećana je privatnost pacijenata, sigurnost sertifikata, a i sama arhitektura je postala skalabilnija i pouzdanija. Ovakvo rešenje je mnogo otpornije na DDoS napade od konvencionalnog iz razloga što je sistem podeljen na poddomene. Nakon testiranja došlo se do zaključka da je za 26% smanjen *overhead* u odnosu na klasičnu arhitekturu koja se koristila do sada, a kašnjenje između krajnjeg korisnika i *gateway*-a je smanjeno za 16%. Na osnovu svega navedenog može se reći da se predložena arhitekura nameće kao veoma prihvatljivo rešenje kada su u pitanju sistemi zdravstvene nege bazirani na IoT.

5. ZAKLJUČAK

U ovom radu predstavljeni su neki od ključnih problema u IoT okruženju. To su pre svega problemi autentifikacije i autorizacije. Takođe, opisani su i neki od najčešćih napada kojima se napadači služe kako bi kompromitovali IoT uređaje. Predstavljena su i neka od sigurnosnih rešenja kako bi se sigurnije utvdio identitet perifernih uređaja u IoT okruženju. Postoje i određeni izazovi i problemi koje je potrebno rešiti, pre svega po pitanju sigurnosti i privatnosti podataka koji se prikupljaju. Takođe, veliki problem je i nepostojanje jasno definisanih komunikacionih standarda koje proizvođači perifernih uređaja moraju da zadovolje. Očigledno, ne postoji rešenje koje odgovara svim potrebama, i možda u budućnosti treba uzeti u obzir i hibridna rešenja [21]. Pored toga, postoje i određena ograničenja kada su u pitanju periferni uređaji, u smislu ograničenih izvora napajanja, ograničenog dometa, mogućnosti skladištenja i obrade podataka i slično. IoT je velik i složen ekosistem koji spaja mnoštvo različitih tehnologija, i sasvim sigurno bi, kada bi se rešili postojeći problemi i ograničenja, pronašao primenu u mnogim sferama života. Na osnovu svega navedenog zaključuje se da IoT ima veliki potencijal da promeni, i u mnogome olakša, naše iskustvo u korišćenju uređaja sa kojima smo svakodnevno okruženi.

REFERENCE

[1] A. Whitmore, A. Agarwal, and L. Da Xu, "The Internet of Things—A survey of topics and trends," Inf. Syst. Front., vol. 17, no. 2, pp. 261–274, Apr. 2015.

[2] J. Pacheco and S. Hariri, "Anomaly behavior analysis for IoT sensors," Trans. Emerg. Telecommun. Technol., vol. 29, no. 4, p. e3188, Apr. 2018.

[3] F. Wortmann and K. Flüchter, "Internet of Things: Technology and Value Added," Bus. Inf. Syst. Eng., vol. 57, no. 3, pp. 221–224, Jun. 2015.

[4] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," Comput. Commun., vol. 54, pp. 1–31, Dec. 2014.

[5] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," in 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, Matsue, Japan, 2014, pp. 230–234.

[6] "ITU Overview of the IoT.pdf.", http://handle.itu.int/11.1002/1000/11559-en?locatt=format:pdf&auth, [Accessed June 28, 2019].
[7] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," Future Gener. Comput. Syst., vol. 29, no. 7, pp. 1645–1660, Sep. 2013.
[8] R. Want, B. N. Schilit, and S. Jenson, "Enabling the Internet of Things," CO M P U T E R, p. 8.
[9] T. Shah and S. Venkatesan, "Authentication of IoT Device and IoT Server Using Secure Vaults," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, 2018, pp. 819–824.
[10] A. F. A. Rahman, M. Daud, and M. Z. Mohamad, "Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework," in Proceedings of the International Conference on Internet of things and Cloud Computing - ICC '16, Cambridge, United Kingdom, 2016, pp. 1–5.
[11] H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," IT Prof., vol. 19, no. 5, pp. 27–33, 2017.
[12] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[13] O. J. A. Pinno, A. R. A. Gregio, and L. C. E. De Bona, "ControlChain: Blockchain as a Central Enabler for Access Control Authorizations in the IoT," in GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1–6.
[14] R. Das, A. Gadre, S. Zhang, S. Kumar, and J. M. F. Moura, "A Deep Learning Approach to IoT Authentication," in 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, 2018, pp. 1–6.
[15] J. Xiong and K. Jamieson, "SecureArray: improving wifi security with fine-grained physical-layer information," in Proceedings of the 19th annual international conference on Mobile computing & networking - MobiCom '13, Miami, Florida, USA, 2013, p. 441.
[16] S. Gil, S. Kumar, M. Mazumder, D. Katabi, and D. Rus, "Guaranteeing Spoof-Resilient Multi-Robot Networks," p. 13.
[17] A.-M. Rahmani et al., "Smart e-Health Gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems," in 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 2015, pp. 826–834.
[18] C. E. Koop et al., "Future delivery of health care: Cybercare," IEEE Eng. Med. Biol. Mag., vol. 27, no. 6, pp. 29–38, Nov. 2008.
[19] S. R. Moosavi et al., "SEA: A Secure and Efficient Authentication and Authorization Architecture for IoT-Based Healthcare Using Smart Gateways," Procedia Comput. Sci., vol. 52, pp. 452–459, 2015.
[20] E. Rescorla and N. Modadugu, "Datagram Transport Layer Security Version 1.2," RFC Editor, RFC6347, Jan. 2012.
[21] C. Sengul, "Privacy, consent and authorization in IoT," in 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), Paris, 2017, pp. 319–321.

Bojan Marčeta, Asistent na Fakultetu organizacionih nauka Univerziteta u Beogradu
Kontakt: bojan.marceta@fon.bg.ac.rs
Oblasti interesovanja: Računarske mreže, IoT, Linux administracija, Bezbednost računarskih sistema

UPUTSTVO ZA PRIPREMU RADA

1. Tekst pripremiti kao Word dokument, A4, u kodnom rasporedu 1250 latinica ili 1251 ćirilica, na srpskom jeziku, bez slika. Preporučen obim – oko 10 strana, single prored, font 11.
2. Naslov, abstakt (100-250 reči) i ključne reči (3-10) dati na srpskom i engleskom jeziku.
3. Jedino formatiranje teksta je normal, bold, italic i bolditalic, VELIKA i mala slova (tekst se naknadno prelama).
4. Mesta gde treba ubaciti slike, naglasiti u tekstu (Slika1...)
5. Slike pripremiti odvojeno, VAN teksta, imenovati ih kao u tekstu, radi identifikacije, u sledećim formatima: rasterske slike: jpg, tif, psd, u rezoluciji 300 dpi 1:1 (fotografije, ekranski prikazi i sl.), vektorske slike – cdr, ai, fh,eps (šeme i grafikoni).
6. Autor(i) treba da obavezno priloži svoju fotografiju (jpg oko 50 Kb), navede instituciju u kojoj radi, kontakt i 2-4 oblasti kojima se bavi.
7. Maksimalni broj autora po jednom radu je 5.

Redakcija časopisa Info M