|  |  |
| --- | --- |
|  | Zbornik radova Fakulteta tehničkih nauka, Novi Sad |

**UDK: 007.52**

**DOI:** [**https://doi.org/10.24867/19IH02Mirkovic**](https://doi.org/10.24867/19IH02Mirkovic)

**BEZBEDNOSNI ASPEKTI U IOT KOMUNIKACIONIM PROTOKOLIMA**

**SECURITY ASPECTS IN IOT COMMUNICATION PROTOCOLS**

Aleksandar Mirković, *Fakultet tehničkih nauka, Novi Sad*

**Oblast – MEHATRONIKA**

**Kratak sadržaj –** *Ovaj rad se sastoji od dva dela: u prvom se objašnjavaju osnove IoT-a (Internet of Things). Fokus je na komunikacionim protokolima koji se koriste u IoT-u, njihovim svojstvima i oblastima primene. Drugi deo rada objašnjava bezbednosne probleme na svim nivoima u IoT-u, i daje moguća rešenja/mere prevencije u svrhu zaštite sistema.*

**Ključne reči:** *IoT, komunikacioni protokoli, IoT bezbednost*

**Abstract** –  *This paper consists of two parts: the first part explains the basics of IoT (Internet of Things). The focus is on the communication protocols used in IoT, their properties and areas of application. The second part of the paper explains security issues at all levels in IoT, and provides possible solutions / prevention measures to protect the system.*

**Keywords:** *IoT, communication protocols, IoT security*

**1. UVOD**

Sve veći broj fizičkih objekata se povezuje na internet izuzetnom brzinom, realizujući ideju interneta stvari (IoT, *Internet of Things*). Primeri takvih objekata uključuju, na primer, termostate i HVAC (*Heating, Ventilation and Air Conditioning*) sisteme koji mogu da se umreže, nadgle­daju i upravljaju sa udaljenog mesta, što omogućava raz­voj takozvanih „pametnih kuća“. Postoje i drugi domeni i okruženja u kojima IoT može da igra izuzetnu ulogu i da unapredi kvalitet čovekovog života (slika 1).

Ove aplikacije uključuju transport, zdravstvo, industrijsku automatizaciju i reagovanje u vanrednim situacijama, npr. u prirodnim katastrofama i katastrofama izazvanim od strane čoveka gde brze i tačne odluke sprečavaju materijalnu štetu i spašavaju živote.

Internet stvari omogućava fizičkim objektima da vide, čuju, misle i izvode poslove tako što će „razgovarati” međusobno, da dele informacije i da koordinišu odluke. Internet stvari transformiše ove objekte od tradicionalnog do pametnog iskorištavanjem tehnologija kao što su sve­prisutno računarstvo, *embedded* uređaji, komunikacione tehnologije, senzorske mreže, internet protokoli i aplika­cije. Vremenom se očekuje da će IoT imati značajan udeo u kućnim i poslovnim aplikacijama, sa ciljem da dopri­nese kvalitetu života i razvoju svetske ekonomije [1].

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**NAPOMENA:**

**Ovaj rad proistekao je iz master rada čiji mentor je bila dr Ivana Šenk.**

**2. OSNOVE IoT-a**

Internet stvari se sastoji od umreženih „stvari“, pri čemu ne postoji jasna definicija šta se sve klasifikuje kao „stvar“, već se smatra da svaki uređaj koji ima mogućnost elektronske komunikacije i povezivanja na internet može biti u IoT sistemu [2]. Jedna gruba podela može biti na sledeće koncepte:



Slika 1. - *Primeri mogućih primena IoT-a*

**2.1. Velike „stvari“:**

Bez obzira na njihovu fizičku veličinu, ova kategorija se odnosi na složenije uređaje. Na primer, modemi, ruteri ili industrijske mašine, od kojih svi dele činjenicu da uglavnom nisu ograničeni svojim napajanjem, povezani su direktno na internet bez ograničenja propusnog opsega, i što je najvažnije, imaju složen model podataka, sa velikim brojem parametara kojima treba upravljati.

**2.2. Male „stvari“:**

Nova kategorija „pametnih“ stvari – jednostavnijih uređa­ja koji su direktno povezani na internet – kao što su sen­zori, pametne brave, pametna svetla, itd. Predmeti u ovoj kategoriji obično imaju relativno ograničenu memoriju i često se napajaju iz baterija, što znači da imaju i energetska ograničenja.

Pored toga, često su povezani na internet preko SIM kartice, a propusni opseg im je ili skup ili ograničen. Ove vrste uređaja generalno imaju mnogo jednostavniji model podataka, a njihova funkcionalnost se često uglavnom odnosi na komande „Set“ i „Get“. Primer „male stvari“ je pametna sijalica, koja se može uključiti ili isključiti, možda zatamniti ili promeniti boju, a kod sofisticiranijih uređaja čak i prijaviti njenu potrošnju energije – međutim, sve ove funkcije ukupno uključuju manje od 10 parame­tara koje treba kontrolisati.

* 1. **Male „stvari“ priključene na internet putem Gateway-a**

Ova kategorija će verovatno dominirati svetom interneta stvari u ne tako dalekoj budućnosti, što se može videti već danas. Ove vrste predmeta i uređaja nazivaju se IoT uređajima, ali zapravo nisu IoT u užem smislu jer nemaju deo „internet“ u sebi, odnosno nisu povezani na internet. Ovo uključuje uređaje koji komuniciraju preko protokola kao što su ZigBee, Z-Wave, LoRa, Sigfox i BLE. Iako se ovi protokoli generalno smatraju IoT protokolima, oni zapravo ne funkcionišu preko internet veze. Pretvaranje ovih uređaja u uređaje koji podržavaju Internet zahteva korišćenje mrežnog *gateway*-a u sredini.

Na slici 2 prikazana je podela navedena u ovom poglavlju:

Slika 2. – *Podela i model IoT-a*

* 1. **Komunikacioni protokoli**

Komunikacioni protokoli za IoT mogu se kategorisati u dve grupe: LPWAN protokoli, i protokoli u mrežama kratkog dometa. Ove dve grupe imaju značajno različite karakteristike i ne postoji jedan najbolji protokol za svaku primenu, već je potrebna analiza koja će identifikovati optimalni protokol za dati problem [3].

* + 1. **LPWAN (Low Power Wide Area Network)**

LPWAN su mreže velikog dometa i male snage. U ovu kategoriju spadaju: SigFox, protokoli *Cellular* (Ćelijski) protokoli prilagođeni za IoT, LoRaWAN tehnologija, itd.

- SigFox je tehnologija male potrošnje energije za bežičnu komunikaciju širokog spektra niskoenergetskih objekata kao što su senzori i M2M (*machine-to-machine*) aplikacije. Omogućava prenos malih količina podataka sa dometom i do 50 kilometara. *SigFox* koristi *Ultra Narrow Band* (UNB) tehnologiju.

- NB-IoT (*Narrow Band IoT*) i LTE-M (*Long Term Evolution for Machines*) koriste postojeću ćelijsku infrastrukturu za IoT sisteme. Oni predstavljaju *light-weight* komunikacione protokole koji nastoje da reše problem standardnih ćelijskih protokola (3G, 4G, 5G) – veliku potrošnju energije. To postižu pod cenu nižeg maksimalnog protoka podataka. Standardni ćelijski protokoli i dalje mogu služiti u IoT aplikacijama koje zahtevaju veliki protok podataka i imaju stalan izvor energije (odnosno u sistemu koji zahteva rad na većim udaljenostima, a količina raspoložive energije nije ograničena na kapacitet baterije).

- LoRaWAN je komunikacioni protokol male snage, dizajniran da bežično poveže baterijski napajane uređaje sa internetom u regionalnim, nacionalnim ili globalnim mrežama i cilja ključne zahteve interneta stvari (IoT) kao što su bi-direkciona komunikacija, *end-to-end* bezbednost, mobilnost i usluge lokalizacije [4].

**2.4.2. Mreže kratkog dometa**

U mreže kratkog dometa spadaju komunikacione tehnologije koje su namenjene za manja rastojanja među uređajima, za opseg do nekoliko desetina ili stotina metara. U ovu kategoriju spadaju, između ostalih:

- ZigBee protokol, koji je kreirala ZigBee Alliance, a zasnovan je na standardu IEEE 802.15.4. ZigBee je kreiran da bude standard koji služi kao komunikacioni protokol niske cene, ali na visokom nivou, sa ciljem stvaranja personalnih mreža malih dimenzija, digitalnih radija male snage koji prenose podatke na veće udaljenosti, za aplikacije koje zahtevaju nisku brzinu prenosa podataka, duži životni vek baterije i bezbedne mrežne uređaje.

- BLE, koji je takođe poznat kao Bluetooth smart, je značajan protokol za primenu IoT-a. Dizajniran je i poboljšan u odnosu na klasičan Bluetooth za ovu svrhu, sa malim propusnim opsegom i sa prioritetom niskog kašnjenja za IoT aplikacije.

- RFID (*Radio Frequency Identifitaction*), koji obuhvata niz standarda uključujući ISO (*International Organization for Standardization*), IEC (*International Electrotechnical Commision*), ASTM International (*American Society for Testing and Materials*), DASH7 alijansa i EPC-global (E*ngineering, Procurement and Construction contract*). RFID sistemi se sastoje od RFID čitača (RFID *reader*), i malih radio-frekventnih transpondera koji se nazivaju RFID tagovi ili oznake. RFID tag je elektronski programiran sa jedinstvenim informacijama i poseduje mogućnost čitanja sa određene fizičke daljine. Postoje dve glavne tehnologije za RFID sisteme u zavisnosti od napajanja tagova: aktivni i pasivni RFID sistemi, koji omogućavaju različiti domet, komunikacioni opseg, i održivost sistema.

- NFC (*Near Field Communication*), standard za bežičnu komunikaciju veoma kratkog dometa koji omogućava prenos podataka između uređaja dodirom ili približavanjem na daljinu od svega nekoliko centimetara. NFC koristi slične principe kao RFID, međutim ne koristi se samo za jednosmernu identifikaciju, već i za razrađeniju dvosmernu komunikaciju, tako što omogućava tri režima rada uređaja, gde se NFC uređaj može ponašati kao čitač, tag, ili *peer-to-peer* uređaj za dvosmernu komunikaciju.

- Z-Wave, MAC protokol male snage koji je razvio Zensys, se uglavnom koristi za bežičnu kućnu automa­tizaciju, za povezivanje 30-50 čvorova, kao i za IoT komunikaciju, posebno za pametne kuće i male komerci­jalne domene. Ova tehnologija je dizajnirana za male pakete podataka na relativno niskom nivou brzine do 100 kbps i 30 metara fizičke udaljenosti. Zbog toga je pogo­dan za male poruke u IoT aplikacijama, kao što su uprav­ljanje osvetljenjem, kućnim uređajima, potrošnjom ener­gije, zdravstvenim parametrima i drugo.

**3. BEZBEDNOSNE PRETNJE I REŠENJA U IOT SISTEMIMA**

Da bi IoT sistemi mogli bezbedno da se implementiraju, treba uzeti u obzir razne mehanizme, parametre, i potencijalne maliciozne napade da bi uslovi rada bili potpuno zadovoljeni. IoT paradigma obuhvata širok spektar uređaja i opreme u rasponu od malih ugrađenih čipova u uređajima do velikih *high-end* servera, pa je potrebno da se obrade bezbednosni problemi na različitim nivoima [5].

**3.1. Bezbednosne pretnje niskog nivoa**

Bezbednosne pretnje niskog nivoa opisuju probleme na fizičkom sloju, slojeve veze za prenos i nivo hardvera. U ovu kategoriju spadaju sledeće pretnje:

- Prigušivački napadi: Napadi ometanja na bežičnim uređajima u IoT-u imaju za cilj da narušavaju mrežu emitovanjem radio signala bez poštovanja protokola. Moguća rešenja podrazumevaju merenje jačine signala, računanje odnosa primljenih paketa, kodiranje paketa sa samokorektivnim kodom, promenu frekvencije i lokacije.

- Inicijalizacija: Bezbedan mehanizam inicijalizacije i konfigurisanje IoT-a na fizičkom nivou onemogućava da pri pokretanju sistema maliciozni čvorovi pristupe istom.

Moguća rešenja: Da bi se osigurao fizički interfejs komunikacije, može se uvesti softverski *framework* koji obezbeđuje bezbednu inicijalizaciju celog IoT sistema, pod cenu značajne upotrebe računarskih resursa pri startu. Drugi metod jeste postavljanje minimalne količine podataka između čvorova koji šalju i primaju podatke, kako bi se osiguralo odsustvo prisluškivača.

- *Sybil* napadi u mreži: Napadi koji su uzrokovani zlonamernim *Sybil* čvorovima koji koriste lažne identitete sa ciljem narušavanja IoT mreže. Moguće rešenje: Jedan pristup otkrivanju *Sybil* napada je merenje jačine signala kroz uvođenje detektorskih čvorova.

- Nebezbedan fizički interfejs: Pristup softveru preko fizičkih interfejsa (npr. USB priključaka) predstavlja ozbiljnu pretnju. Moguće rešenje je praćenje OWASP (*The Open Web Application Security Project*) preporuka.

- Napad deprivacije sna: Konstantni zahtevi na IoT uređa­jima smanjuju raspoloživu energiju. Moguća rešenja: Postoji više pristupa za rešavanje ovog problema, jedan predloženi sistem za detekciju deprivacije sna koristi pristup zasnovan na klasterima i sektorima.

Određuje se glavni čvor svakog sektora u koji se ugrađuju sofisticirane softverske odbrane, i preko njega se odvija komunikacija.

**3.2. Bezbednosne pretnje srednjeg nivoa**

Bezbednosne pretnje srednjeg nivoa tiču se komunikacije, rutiranja, autentifikacije i dr. U ovu kategoriju spadaju sledeće pretnje:

**-** Duplikacioni napadi: Rekonstrukcija polja fragmenta paketa na 6LoWPAN sloju može dovesti do iscrpljivanja resursa, prekoračenja bafera i ponovnog pokretanja ure­đaja. Moguća rešenja: Uvođenje vremenske oznake i *nonce* opcije za odbranu protiv napada ponavljanja, fragmentacija kroz *hash* lanac.

- Nebezbedan sused: Faza otkrivanja suseda pre prenosa podataka uključuje različite korake poput otkrivanja rutera i adrese. Korišćenje paketa za otkrivanje suseda bez odgovarajuće verifikacije može imati ozbiljne implikacije. Moguće rešenje: Autentifikacija koristeći potpis baziran na kriptografiji eliptičnih krivi (ECC).

**-** Napad rezervacije bafera:Pošto prijemni čvor zahteva rezervisanje baferskog prostora za ponovno sastavljanje dolaznih paketa, napadač može da ga iskoristi slanjem nepotpunih paketa. Moguće rešenje: Jedan metod za zaustavljanje ovog napada je korištenje pristupa podelje­nog bafera, koji povećava cenu pokretanja napada zahte­vajući da se kompletni fragmentirani paketi prenesu u kratkim i tačnim intervalima.

- Napad RPL (*Routing protocol for Low Power and Lossy Networks*) rutiranja: RPL protokol je ranjiv na različite napade kroz kompromitovane čvorove koji postoje u mreži. Moguća rešenja: Heširanje i autentifikacija bazirana na potpisu, posmatranje ponašanja node-a.

- *Sybil* čvorovi na srednjem sloju: Komunikacija *Sybil* čvorova koristeći lažne identitete može dovesti do narušavanja performansi i privatnosti korisnika u mreži. Moguća rešenja: Slučajno lutanje po grafu, analiza ponašanja korisnika, vođenje spiskova pouzdanih, odnosno nepouzdanih korisnika.

- *Sinkhole* i *Wormhole* napadi: U ovoj vrsti napada na sistem, čvor napadača odgovara na zahteve za rutiranje, čineći da paketi prolaze kroz napadački čvor. Moguća rešenja: Verifikacija ranga kroz funkciju heširanja lanca, upravljanje nivoom poverenja, analiza node / komunika­cionog ponašanja, detekcija anomalije kroz IDS.

- Autentifikacija: Uređaji i korisnici u IoT-u moraju biti autentifikovani putem sistema upravljanja ključevima, ukoliko se zlonamerni čvorovi infiltiriraju u sistem mogu dobiti pristup i kontrolu nad sistemom. Moguća rešenja: Razni kriptografski algoritmi i protokoli: AH (*Authenti­fication Header*), ESP (*Encapsulating* *Security* *Protocol*), AES (*Advanced* *Encryption* *Protocol*), TMP (*Trusted* *Platform* *Module*), SHA1 (*Secure* *Hash* *Algorithm*), hibridna autentifikacija, autentifikacija sa fuzzy ekstrak­torom, enkripcija korisnog opterećenja šifrovanog tipa sa komprimovanim AH i dr.

**-** Transportni nivo: *End-to-end* bezbednost na transport­nom nivou ima za cilj da obezbedi bezbedan mehanizam tako da se podaci iz čvora pošiljaoca pošalju na željeni čvor na potpuno pouzdan način. Moguća rešenja: DTLS-PSK (*Datagram Transport Layer Security – preshared key ciphersuites)* sa *nonce*, 6LoWPAN granični ruter sa ECC, DTL šifra bazirana na AES/SHA algoritmima, komprimovani IPSEC (*Internet Protocol Security*), kom­primovanje DTLS zaglavlja, IKE v2 (*Internet Key Exchange*) koristeći komprimovani UDP (*User Datagram Protocol*), sigurnost bazirana na AES sa identifikacijom i ovlašćenjem i mnogi drugi.

**3.3. Bezbednosne pretnje visokog nivoa**

Bezbednosne pretnje visokog nivoa se odnose na nivo aplikacija u IoT. U ovu kategoriju spadaju sledeće pretnje:

- CoAP bezbednost: *The Constrained Application protocol* (CoAP) je protokol za veb prenos, samim tim što čini vezu sa internetom ranjiv je na direktne napade sa istog. Moguća rešenja: TLS/DTLS mapiranje, *Mirror Proxy* (MP) i adresar resursa, TLS-DTLS tunel i filtriranje poruke koristeći 6LBR (6LoWPAN *Border Router*).

- Nebezbedan interfejs: Za pristup IoT uslugama, interfejsi koji se koriste preko veba, mobilnih uređaja i oblaka su ranjivi na različite napade koji mogu ozbiljno da utiču na privatnost podataka. Moguća rešenja: Onemogućavanje korišćenja slabih šifri, testiranje interfejsa na ranjivosti ili softverski alati (npr. SQLi – *Structured Query Language Injection*), korišćenje https (*Hypertext Transfer Protocol Secure*) u kombinaciji sa firewall-om.

- Različite ranjivosti u IoT-u uključuju one uzrokovane nebezbednim softverom/firmverom. Moguća rešenja: Redovna bezbednosna ažuriranja softvera/firmvera, korišćenje potpisa iz fajlova, enkripcija sa validacijom.

- *Middleware* bezbednost: IoT *middleware*, dizajniran za obezbeđivanje komunikacija među entitetima u IoT siste­mima, mora biti dovoljno bezbedan za pružanje usluga. Različite interfejse i okruženja koja koriste *middleware* potrebno je spojiti interno da bi se obezbedila bezbedna komunikacija.

Moguća rešenja: Bezbedna komunikacija koristeći autenti­fikaciju, bezbednosne odredbe, upravljanje ključevima iz­među uređaja, gateway i M2M komponente, servisni sloj M2M bezbednosti, transparentni *middleware* koristeći autentifikaciju ili enkripcione mehanizme.

**4. ZAKLJUČAK**

IoT je disruptivna tehnologija koja ima potencijal da kva­litet naših života u određenim segmentima značajno po­boljša. Moguća mesta za primenu IoT-a su brojna: pametne kuće, pametne fabrike i gradovi, u medicini, autonomnim vozilima, automatizovanim prodavnicama, poljoprivredi, u situacijama prirodne katastrofe i dr.

Gde god je potrebno nadgledanje fizičkih stvari/ljudi, ili se treba doneti neka odluka na osnovu ulaza u sistem - čovek se može zameniti senzorima i mikroprocesorom koji te ulaze može protu­mačiti i doneti pravu odluku. Jedan od bitnih koraka u raz­voju IoT sistema je biranje pravilnog komunikacionog pro­tokola. Da bi se to učinilo potrebno je vrlo jasno definisati zadatak i potrebne parametre: koliki domet je potreban, koji je protok podataka, da li su uređaji baterijski napajani ili imaju stalan pristup električnoj energiji itd. U zavisnosti od specifikacija zadatka i sistema bira se odgovarajući pro­tokol.

Procena je da se trenutno na svetu koristi preko 22 mili­jardi IoT uređaja, i da će se taj broj značajno uvećati [6]. Toliki broj uređaja sa sobom donosi potencijalne rizike u smislu bezbednosnih problema. Cilj IoT-a je da svaki uređaj na svetu može komunicirati jedan sa drugim, i ne­minovno je da će doći do situacija gde maliciozni karak­teri žele da iskoriste taj sistem na drugačije načine nego što je poželjno.

U ovom radu razmatrane su najznačajnije sigurnosne pretnje za sva 3 nivoa - niski, srednji, i visoki. Postoji nekoliko generalnih zaključaka iz datih pretnji i rešenja koja se mogu pratiti kako bi se svaki IoT sistem učinio mnogo bezbednijim:

- Nikad ne treba šifre čuvati digitalno/na internetu, i trebaju da budu bezbedne (minimum 8 znakova).

- Pre uvođenja novih uređaja u IoT sistem, potrebna je bezbedna autentifikacija.

- Heširanje i drugi kriptografski alati značajno pomažu pri očuvanju bezbednosti sistema.

- Bitno je uspostaviti pravilno okruženje/*framework* kako bi se obezbedila bezbednost u srednjem sloju i osigurala potpuno bezbednu M2M/*peer-to-peer* komunikacija.

- Ukoliko je moguće treba fizički interfejs napraviti nedostupnim prolaznicima da ne bi pristupili sistemu preko debugging ili drugih softverskih alata.

**5. LITERATURA**

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, Fourthquarter 2015, doi: 10.1109/COMST.2015.2444095.

[2] IoT whitepaper- Understanding IoT protocols clients and servers [https://friendly-tech.com/what-is-iot](https://friendly-tech.com/what-is-iot/?utm_campaign=Social&utm_source=youtube&utm_medium=social&utm_term=111617) (pristupljeno u maju 2022.)

[3] Al-Sarawi, Shadi et al. “Internet of Things (IoT) communication protocols: Review.” 2017 8th International Conference on Information Technology (ICIT) (2017): 685-690.

[4] <https://lora-alliance.org/about-lorawan/> (pristupljeno u maju 2022.)

[5] Salah, Khaled & Khan, Minhaj. (2017). IoT Security: Review, Blockchain Solutions, and Open Challenges. Future Generation Computer Systems. 82. 10.1016/j.future.2017.11.022.

[6] <https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/> (pristupljeno u maju 2022.)

**Kratka biografija:**

|  |  |
| --- | --- |
| C:\Users\Alex\AppData\Local\Microsoft\Windows\INetCache\Content.Word\212182342_10219557429550225_5828028052705260747_n.jpg | **Aleksandar Mirković** rođen je 06.02.1998. godine u Cirihu, Švajcarska. Osnovnu školu „Jelenka Voćkić“ u Brčko Distriktu završio je 2012. godine. Potom je upisao smer „mehatronika“ u Tehničkoj školi u istom gradu. Završio ju je 2016. kao đak generacije. Iste godine je upisao Fakultet tehničkih nauka u Novom Sadu, odsek mehatronika. Uža specijalnost na osnovnim studijama je robotika i automatizacija. Zvanje diplomiranog inženjera je stekao 2020. godine, sa prosečnom ocenom 9.51. Nastavio je master akademske studije na smeru „Mehatronika“ na FTN-u, sa istom specijalizacijom.kontakt:m.aleksandar98@gmail.com |