Istraživanje sigurnosnih rizika u okruženju Interneta stvari

Rohlik, Andrej

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:994699

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Andrej Rohlik

ISTRAŽIVANJE SIGURNOSNIH RIZIKA U OKRUŽENJU INTERNETA STVARI

DIPLOMSKI RAD

Zagreb, 2022.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

ISTRAŽIVANJE SIGURNOSNIH RIZIKA U OKRUŽENJU INTERNETA STVARI

EXPLORING SECURITY RISKS IN AN INTERNET OF THINGS ENVIRONMENT

Mentor: dr. sc. Ivan Cvitić

Student: Andrej Rohlik

JMBAG: 0135251341

Zagreb, rujan 2022.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 4. svibnja 2022.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Sigurnost i zaštita informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 6898

Pristupnik: **Andrej Rohlik (0135251341)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Istraživanje sigurnosnih rizika u okruženju Interneta stvari**

Opis zadatka:

Diplomskim radom potrebno je istražiti sigurnosne rizike u okruženju Interneta stvari. Nužno je utvrditi relevantnost istraživanja kroz analizu aktualne znanstvene i stručne literature te je potrebno pružiti pregled trenutno aktualnih sigurnosnih rizika i izazova u IoT okruženju kao i postojećih metoda zaštite. Uz navedeno, kao ključan dio istraživanja potrebno je simulirati okruženje pametnog doma i sigurnosne prijetnje korištenjem dostupnih simulacijskih programskih alata. Rezultate dobivene simulacijom potrebno je analizirati i interpretirati te, posljedično predložiti unaprjeđenja sigurnosti promatranog IoT okruženja.

Mentor:

dr. sc. Ivan Cvitić

Predsjednik povjerenstva za diplomski ispit:

SAŽETAK

Internet stvari predstavlja opći koncept sposobnosti mrežnih uređaja da osjete i prikupljaju podatke iz svijeta oko nas, a zatim podijeli te podatke preko interneta, gdje se može obrađivati i koristiti za različite svrhe. Rad se bavi istraživanjem sigurnosnih rizika u okruženju Interneta stvari. Opisane su najčešće vrste sigurnosnih rizika i izazova sa kojima se korisnici prilikom implementacije ili korištenja mogu susresti i njihove karakteristike. Zbog velikog broja povezanih uređaja i mreža u okruženju Interneta stvari postoji područje IoT sigurnosti koje se bavi zaštitom takvih okruženja i zbog toga su u radu opisane i neke od suvremenih metoda zaštite IoT okruženja. U radu je također provedena simulacija pametnog doma i sigurnosnih prijetnji pomoću alata NetSim kako bi se razumio način funkcioniranja pametnog doma, te su analizirani rezultati simulacije i predložena neka od unaprjeđenja takvog okruženja.

KLJUČNE RIJEČI: Internet stvari; sigurnosni rizici; zaštita; simulacija; pametni dom

SUMMARY

The Internet of Things represents the general concept of the ability of networked devices to sense and collect data from the world around us, and then share that data over the Internet, where it can be processed and used for various purposes. The paper deals with the research of security risks in the environment of the Internet of Things. The most common types of security risks and challenges that users may encounter during implementation or use and their characteristics are described. Due to the large number of connected devices and networks in the Internet of Things environment, there is an area of IoT security that deals with the protection of such environments, and for this reason, some of the modern methods of protecting the IoT environment are described in the paper. The paper also carried out a simulation of the Smart Home and security threats using the NetSim tool in order to understand how the Smart Home works, the results of the simulation were analyzed and some of the improvements of such an environment were proposed.

KEY WORDS: Internet of Things; security risks; protection; simulation; Smart Home

SADRŽAJ

1. Uvod 1
2. Pregled dosadašnjih istraživanja 2
2.1. Zastupljenost IoT-a u Hrvatskoj 3
2.2. Analiza dosadašnjih istraživanja 5
3. Sigurnosni rizici i izazovi u IoT okruženju 8
3.1. Sigurnost i autentikacija 8
3.2. Heterogenost i politike 9
3.3. Standardizacija i implementacija 10
3.4. Pitanja privatnosti 13
3.5. Najčešće sigurnosne prijetnje i napadi IoT okruženja 14
4. Suvremene metode zaštite IoT okruženju 16
4.1. Metode zaštite pametnih domova i zgrada 16
4.2. Metode zaštite pametnih gradova 19
4.3. Tehnike sigurnosti i privatnosti u IoT okruženju 20
5. Simulacija okruženja pametnog doma i sigurnosnih prijetnji 22
5.1. Priprema i instalacija simulacijskog alata NetSim 23
5.2. Pokretanje NetSim-a i provođenje simulacije 24
5.2.1. Simulacija SYN Flood napada 31
5.2.2. Simulacija *Sink Hole* napada 33
5.2.3. Simulacija DIS Flood napada 34
6. Analiza rezultata istraživanja i prijedlozi unaprjeđenja 36
6.1. Analiza rezultata istraživanja 36
6.2. Prijedlozi unaprjeđenja 41
7. Zaključak 44
Literatura 46
Popis kratica 50
Popis slika 53
Popis tablica 54

1. Uvod

Tijekom posljednjih nekoliko godina, IoT (engl. *Internet of Things*) je postao jedna od najvažnijih tehnologija 21. stoljeća. Sada se svakodnevni predmeti (kao što su kuhinjski aparati, automobili, termostati, monitori za bebe, itd.) mogu povezati s internetom putem ugrađenih uređaja, te je tako moguća besprijekorna komunikacija između ljudi, procesa i stvari. Pomoću jeftinog računalstva, oblaka, velikih podataka, analitike i mobilnih tehnologija, fizičke stvari mogu dijeliti i prikupljati podatke uz minimalnu ljudsku intervenciju. U ovom hiperpovezanom svijetu digitalni sustavi mogu snimati, pratiti i prilagođavati svaku interakciju između povezanih stvari. Fizički svijet susreće se s digitalnim svijetom i oni surađuju.

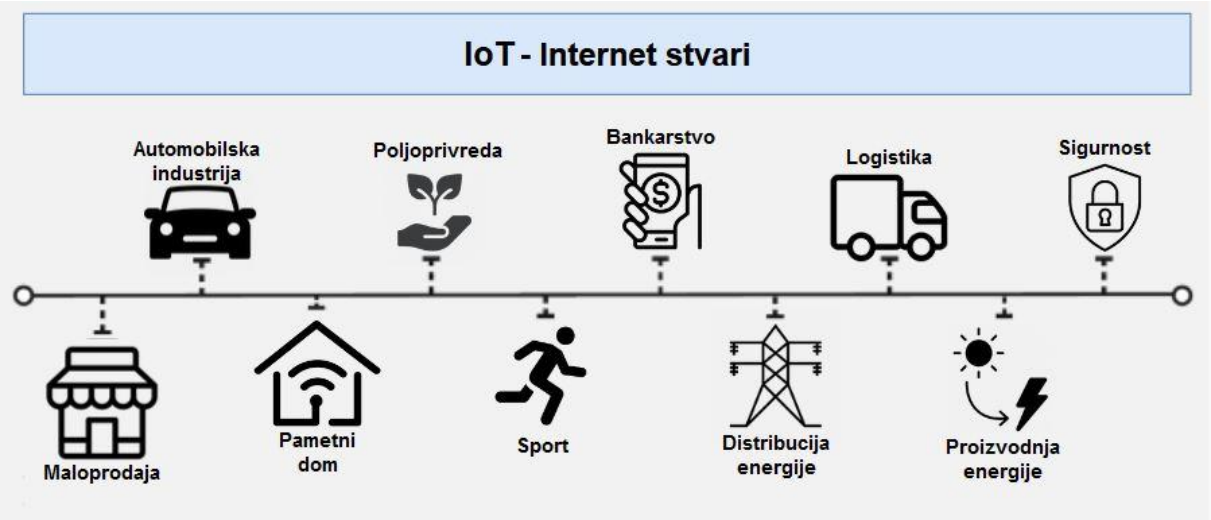
Naslov diplomskog rada je *Istraživanje sigurnosnih rizika u okruženju Interneta stvari*, a cilj je prikazati sigurnosne prijetnje i izazove, analizirati potencijalne utjecaje na korisnika, prikazati kako bi se mogao smanjiti rizik od takvih prijetnje, te validacija IoT sustava. Rad je podijeljen u 7 cjelina:

1. Uvod
2. Pregled dosadašnjih istraživanja
3. Sigurnosni rizici i izazovi u IoT okruženju
4. Suvremene metode zaštite IoT okruženja
5. Simulacija okruženja pametnog doma i sigurnosnih prijetnji
6. Analiza rezultata istraživanja i prijedlozi unaprjeđenja
7. Zaključak

U poglavlju *Pregled dosadašnjih istraživanja* se pruža osvrt na neka dosadašnja istraživanja raznih autora kao i analiza istih. U trećem se poglavlju analiziraju sigurnosni izazovi i rizici sa kojima se privatni korisnici ili tvrtke mogu susresti prilikom implementacije pametnih uređaja i mreže u svoja okruženja. Četvrto poglavlje pruža uvid u neke metode i tehnike pomoću kojih korisnici mogu zaštititi svoje podatke i zlonamjernom akteru onemogućiti lagan ulazak u mrežu. U petom poglavlju se vrši simulacija okruženja pametnog doma pomoću NetSim mrežnog simulatora, a u šestom se poglavlju analiziraju rezultati provedeni simulacijom kao i neki prijedlozi unaprjeđenja okruženju pametnog doma kako bi se dom što bolje zaštitio od napada.

2. Pregled dosadašnjih istraživanja

U svijetu u kojem su "stvari" i uređaji međusobno povezani na svim razinama, od nosivih uređaja do automatizacije domova i zgrada, pametnih gradova i infrastrukture, pa čak i do pametnih industrija, sigurnost Interneta stvari (IoT) igra središnju ulogu gdje nema mjesta za pogreške ili manjak u opskrbi. Osiguranje, uključujući autentikaciju takvih uređaja, postaje svačiji prioritet, od proizvođača do dobavljača, programera softvera i aplikacija, te do krajnjeg potrošača, korisnika koji upotrebljava IoT proizvode. Zajedno se moraju prilagoditi zahtjevima tržišta, inovirati i poboljšati procese, steći nove vještine i naučiti nove metode, te podići svijest. Na slici 1. je prikazano u kojim sve područjima industrije se može primijeniti IoT.



Slika 1. IoT primjena u industrijama

Tijekom godina IoT je promijenio način na koji tvrtke komuniciraju s ljudima i donio razne prednosti kako ljudima tako i industrijama. Omogućuje industrijama razumijevanje potreba potrošača u stvarnom vremenu, poboljšavanje kvalitete strojeva i sustava, pojednostavljivanje operacija i otkrivanje inovativnih načina rada kao dio napora digitalne transformacije. Izvješće *Fortune Business Insightsa* kaže da se očekuje da će globalno tržište Interneta stvari od 190 milijardi dolara dosegnuti 1,11 bilijuna dolara (1111,3 milijarde dolara) godišnjeg rasta do 2026. godine. Očekuje se da će sektor bankarskih i financijskih usluga biti segment s najvećim tržišnim udjelom, [1].

2.1. Zastupljenost IoT-a u Hrvatskoj

Iako se o IoT-u priča već desetljećima, tek je u posljednje vrijeme ova tehnologija uzela maha. Za IoT rješenja donedavno nije ni bilo velike potrebe, pogotovo dok se nije razvila potporna tehnologija koja bi omogućila da ta sva IoT rješenja funkcioniraju kako treba. Jedan od praktičnijih načina rješavanja starih problema kroz IoT je *retrofitting*. Riječ je o opremanju postojećih uređaja novim tehnologijama i senzorima koji čine cijeli sustav učinkovitijim. Internet stvari utjelovljuje veliki ekonomski i društveni inovacijski val koji je omogućio internet u kojem komponente, proizvodi, usluge i platforme povezuju, virtualiziraju i integriraju sve u komunikacijsku mrežu za digitalnu obradu. U Republici Hrvatskoj je u posljednjih nekoliko godina rad započelo mnogo tvrtki koje se bave uvođenjem IoT tehnologija u sve sfere života od pametnog upravljanja proizvodnjom, pametne poljoprivrede pa do pametne mobilnosti/automatizirane vožnje.

U području pametne proizvodnje za veću učinkovitost, veću fleksibilnost, agilnost i niže operativne troškove brinu se tvrtke kao što su npr. Ascalia, ByteLab i Mobilisis. Ascalia je tvrtka sa sjedištem u Velikoj Britaniji i Hrvatskoj koja pruža softverska i hardverska rješenja za digitalizaciju proizvodnih pogona bez visokih troškova ili zastoja. To je moderna „sve u jednom“ platforma za IIoT (engl. *Industrial IoT*) sustave, koja poboljšava produktivnost i smanjuje otpad u tvornicama koristeći napredne sustave pokretane umjetnom inteligencijom. Sa sjedištem u Zagrebu, Byte Lab je uspješno dovršio više od 200 projekata diljem svijeta, a njihova specijalnost je dizajn elektroničkih proizvoda, razvoj ugrađenog softvera, što znači da dizajniraju, testiraju i proizvode vodeći računa o specifičnim potrebama svakog klijenta. Mobilisis je na tržištu već gotovo 15 godina uz kontinuirani rast i zapošljavanje. Mobilisis proizvodi modernu i inovativnu IT infrastrukturu za upravljanje industrijskim procesima, kao i mobilno prikupljanje i prijenos podataka. Mobilisis razvija inovativnu elektroničku opremu prvenstveno namijenjenu Industriji 4.0 i IoT tržištima, [2].

Kod pametne poljoprivrede prednjači tvrtka Agrivi koju je osnovao 2013. godine Matija Žulj čija je vizija bila promijeniti način proizvodnje hrane. Danas je softver za upravljanje farmom Agrivi globalno prepoznat kao jedno od najboljih rješenja za upravljanje farmom na tržištu, uz snažnu podršku tisuća farmera u više od 150 zemalja diljem svijeta koji su u mogućnosti poboljšati svoju proizvodnju uz pomoć Agrivija. U

području pametne mobilnosti/automatizirane vožnje spominju se tvrtke kao što su Rimac Automobili, Mikroprojekt i Visage Technologies. Rimac je tehnološka snaga koja stvara električne hiperautomobile i pruža cjelovita tehnološka rješenja svjetskim proizvođačima automobila. U njihovom istraživanju i razvoju autonomne vožnje, tvrtka radi na primjeni umjetne inteligencije na trkaća vozila i vozila visokih performansi, razvijajući sljedeću generaciju softvera i algoritamskih rješenja kako bi naučili vozila izvršavati manevre vožnje kao vozači trkaćih vozila, ako ne i bolje od njih. Još jedna hrvatska tvrtka je i Mikroprojekt koja se bavi ugrađenim sustavima koji se fokusiraju na napredna rješenja u ugrađenim video i grafičkim sustavima temeljenim na FPGA (engl. *Field Programmable Gate Array*), a također isporučuju inovativni softver i hardver koji omogućuje fleksibilnu funkcionalnost i visoke performanse u takvim sustavima, [2].

U Zagrebu je postavljena i puštena u rad prva bazna stanica za tehnologiju IoT u Hrvatskoj 2017. godine. Stanicu je proizvela tvrtka Sigfox, čija se tehnologija temelji na visokoj isplativosti i maloj potrošnji energije budući da stanice ne služe za telefoniranje i surfanje internetom, već samo jednostavnom i izravnom vezom za povezivanje stvari. Uvođenje prve bazne stanice označilo je i početak razvoja nacionalne IoT mreže u Hrvatskoj koju je implementirala tvrtka IoT NET Adria. U prvih šest mjeseci od potpisivanja suradnje sa SigFox-om, IoT Net Adria je uspjela pokriti gotovo polovicu stanovništva u Hrvatskoj te četvrtinu hrvatskog teritorija. Prvi komercijalni partner IoT Net Adrije je Marinacloud koja se brine za brodove u svojoj marini pa su tako prepoznali potencijal IoT tehnologije i u brodove ugradili senzor koji signalizira ako se baterija bliži svojem kraju kako bi djelatnici marine mogli preuzeti brigu o punjenu baterije te vlasnike zaštiti od nabavke skupe nove baterije, a također javlja prisutnost vode u trupu, kao i dima, [3].

Od trenutka kada se počelo govoriti o IoT-ju, logistika i praćenje imovine se nametnulo kao jedan od prvih logičnih slučajeva korištenja tehnologije, a također su se razvili i projekti gdje je primjerice pametni vodomjer smanjio gubitke vode, IoT tehnologija je omogućila pravovremeno i preciznije lociranje pošiljki, transformirala i unaprijedila procese u poljoprivredi i prehrambenoj industriji u načinu prikupljanja i obrade podataka. Sigfox kao tehnologija za Internet stvari odlično se uklapa u tu priču, te zbog svog specifičnog načina rada i produženog životnog vijeka uređaja i baterije omogućava korisniku dugoročno iskorištavanje uređaja, brzi povrat investicije i daljnji profit nakon samog povrata investicije, [3].

2.2. Analiza dosadašnjih istraživanja

Zbog specifičnosti komunikacijske tehnologije, odnosno svepristutnosti njene primjene u potrošačkom gospodarstvu, IoT se pojavljuje kao novi pokretač u svim industrijama, bile one proizvodne ili uslužne, uključujući, energetske, zdravstvene, transportne i građevinske tehnologije. U svima njima Internet stvari stvara mjerljivu novu vrijednost, a nova vrijednost lako je mjerljiva u industriji, ali i u javnim djelatnostima, odnosno onome što se naziva javni sektor. Zbog toga postoji poprilično veliki broj istraživanja i publikacija objavljenih na tu temu.

U istraživanju Hall F., Maglaras L., Aivaliotis T., Xagoraris L., Kantzavelou I.: *Smart Homes: Security Challenges and Privacy Concerns*, 2020., obrađena je tema pametnog doma, gdje su se autori fokusirali na neke sigurnosne izazove i brigu o privatnosti, a također su se u istraživanju fokusirali na sljedeće izjave:

- eksponencijalni rast u IoT industriji zaslužan je za porast popularnosti pametnih domova,
- brzi rast industrije pametnih domova izaziva ozbiljnu zabrinutost u pogledu sigurnosti i privatnosti svojih korisnika,
- dobre sigurnosne prakse moraju se koristiti u sve tri faze životnog ciklusa pametnog uređaja: razvoj, integracija i korištenje IoT uređaja u pametnom domu, [4].

Također se u istraživanju autori fokusiraju na svrhu i povezivost unutar pametnog doma gdje se govori da je pametni dom u biti skup povezanih IoT uređaja koji imaju za cilj poboljšati životno iskustvo korisnika. Takvi uređaji i servisni uređaji se mogu kategorizirati u šest glavnih područja:

- okoliš – vodomjeri, upravljanje energijom, rasvjeta i sl.,
- sigurnost – alarmi, kamere, itd.,
- kućna zabava – televizori, zvučnici, itd.,
- kućanski uređaji – hladnjaci, mikrovalne pećnice, aparat za kavu i sl.,
- informacije i komunikacije – telefoni, Internet, itd.,
- zdravlje – pomoć u kući, [4].

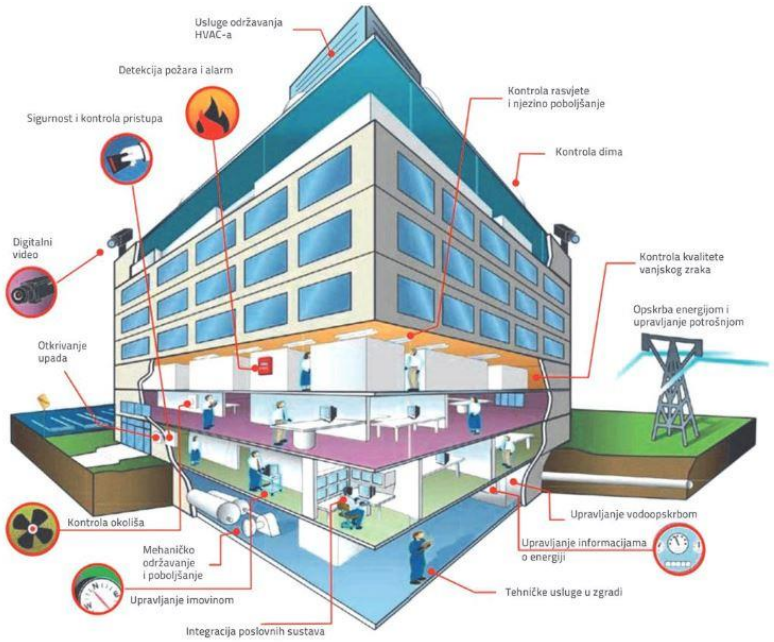
U znanstvenoj studiji Khalifa E.: *Smart Cities: Opportunities, Challenges and Security Threats*, 2019., autor govori da pametni gradovi predstavljaju način života koji se u potpunosti temelji na korištenju tehnoloških dostignuća kao što su sustavi umjetne inteligencije, Internet stvari i veliki skupovi podataka, s ciljem maksimiziranja korištenja dostupnih resursa, smanjenja potrošnje energije i otpada, stvaranja okruženja koje poboljšava stvaranje i inovacije te poboljšava kvalitetu života ljudi smanjenjem troškova života i čineći život lakšim i sigurnijim. Ova studija je normativna studija gdje se raspravlja o prednostima i prijetnjama pametnih gradova. Prvo se usredotočuje na široko usvajanje pametnih gradova među nacijama, a drugo raspravlja o razlozima koji potiču zemlje kako bi usvojili takav model gradova i ostvarili dobit koju žele ostvariti takvim modelom, treće raspravlja o raznim sigurnosnim prijetnjama koje se mogu pojaviti iz pametnih gradova, te na kraju autor zaključuje studiju s nekim preporukama za ublažavanje prijetnji pametnih gradova, [5]. Slika 2. prikazuje na kojim se sve sustavima u gradu može primijeniti IoT tehnologija.

Slika 2. Primjeri pametnih uslužnih sustava grada

Izvor: [6]

Članak Krishnan S., Anjana M. S., Rao S.: *Security Considerations for IoT in Smart Buildings*, 2017., pruža pristup uključivanju sigurnosti prilikom implementacije Interneta stvari za pametne zgrade. U području bežičnih mreža u posljednjih nekoliko desetljeća došlo je do dramatičnog porasta tehnoloških izuma, kao i sigurnosnih prijetnji povezanih s njima. Sigurnosne prijetnje su neizbježne zbog otvorenosti bežične komunikacije. U skupu TCP/IP (engl. *Transmission Control Protocol/Internet Protocol*) protokola, prijetnje se mogu vidjeti na svakom sloju, što uključuje

prisluškivanje na fizičkom sloju, uskraćivanje usluge – DoS (engl. *Denial of Service*), ispuštanje paketa, preusmjeravanje paketa na mrežnom sloju i slično. S obzirom na to, potrebno je analizirati utjecaje sigurnosnih prijetnji na pametne zgrade. U ovom radu bave se također sigurnosnim prijetnjama koje će se vjerojatno pojaviti u IoT mreži pametnih zgrada, daju prioritete prijetnjama na temelju rizika, a zatim se fokusiraju na rješenja za suzbijanje glavnih prijetnji, [7]. Na slici 3. se može vidjeti u koje sve uslužne sustave zgrade možemo implementirati IoT tehnologiju kako bi ona što više postala automatizirana.



Slika 3. Pametni uslužni sustavi zgrade

Izvor: [6]

U znanstvenom članku Manivannan T., Radhakrishnan P.: *A Comprehensive Analysis of Simulation Tools for Internet of Things,* 2020., autori govore da uz paradigmu IoT-a koja obećava velike promjene u raznim područjima kao što su zdravstveni sektor, transport, pametna poljoprivreda i pametni gradovi kako bi se život učinio boljim mjestom za ljude važno je da su novi sustavi izgrađeni pomoću takve paradigme ispravno dizajnirani i daju pouzdana rješenja. Korištenje alata za simulaciju ima glavnu ulogu kada se IoT aplikacije dizajniraju i razvijaju. Međutim, današnjim glavnim istraživačima i programerima IoT-a je teško odabrati pravi alat za simulaciju. Članak pruža opsežan pregled simulacijskih alata za pomoć istraživačima i programerima u odabiru pravog alata za njihove eksperimente pri radu s IoT okruženjem, [8].

3. Sigurnosni rizici i izazovi u IoT okruženju

Razvojem IoT-a iz mreža ograničenog pristupa u distribuiranu javnu mrežu povećala se potreba za sigurnosnim alarmima za zaštitu međusobno povezanih IoT uređaja od upada kao što su modifikacije podataka, ubrizgavanje zlonamjernog koda, njuškanje i uskraćivanje usluge i mnogih drugih prijetnji. *SonicWall* je izvijestio da su se IoT napadi zlonamjernog softvera povećali za 215,7%. Prva dva tromjesečja 2021. godine premašila su za 55% prva dva tromjesečja 2020. godine. Iako postoje postojeće tehnologije i protokoli koji se bave pitanjima prijetnji sigurnosti, ograničenja na IoT uređajima i mreži onemogućuju jednostavnu prilagodbu i implementaciju IoT rješenja u novonastalim skupovima sigurnosnih scenarija, [9].

Trenutno usvojeni sigurnosni protokol i kriptografske postavke zahtijevaju puno resursa i IoT uređaji kao što su pametni telefoni, tableti, računala, usmjerivači, aktivni senzori ili pasivne RFID (engl. *Radio Frequency Identification*) oznake, imaju vrlo ograničene resurse i mogućnosti za podršku implementaciji i prilagodbi tradicionalne sigurnosti protokolarnih rješenja. Stoga implementacija i prilagodba tradicionalnih sigurnosnih protokola i dalje ostaje izazov zbog čega je teško osigurati povjerljivost prijenosa podataka. Budući da se IoT uređaji ne nadziru jer rade na način samoodržavanja s ograničenim održavanjem (npr. nadzor), to dodatno dovodi do zabrinutosti u smislu integriteta podataka (povjerenja). Kao rezultat toga, podaci dobiveni s IoT uređaja vjerojatno će biti niske kvalitete ili oštećeni. Postoje različiti sigurnosni izazovi i ograničenja vezana uz IoT, a koja utječu na usvajanje velikih razmjera. U sljedećim potpoglavljima su ti izazovi i ograničenja detaljno razmotreni, [10].

3.1. Sigurnost i autentikacija

Privatnost korisnika i zaštita podataka važno je pitanje u IoT sigurnosti uzimajući u obzir sveprisutne karakteristike IoT okruženja. Sposobnost IoT senzora i uređaja da osjete, prikupljaju i prenose podatke putem interneta predstavlja prijetnju privatnosti pojedinaca. Poznato je da IoT čvorovi prikupljaju privatne podatke ljudi, a da oni to uopće ne primjećuju. Iako je već predloženo mnoštvo istraživanja u vezi s privatnošću, mnoge teme još trebaju dodatno istražiti. Prema nekim izvješćima, *Nest* termostat, koji je jedan od najsigurnijih IoT uređaja, može se *hakirati* i kontrolirati dok se uređaj

pokreće. *Hakeri* mogu na njega učitati svoj prilagođeni softver koji bi spriječio slanje podataka termostata natrag na *Nestove* poslužitelje. Kompromitirani *Nest* termostat će tada djelovati kao polazna točka za preuzimanje kontrole nad drugim uređajima u domu, što napadačima omogućuje pristup osjetljivim informacijama o ljudima kao što su njihova prisutnost u kući ili njihov raspored spavanja. Aplikacije za pametne uređaje također mogu biti ranjive kao i sam uređaj. Studija sigurnosnog istraživačkog tima u *Checkmarxu* pokazala je kako napadači zaobilaze korisnička dopuštenja i preuzimaju kontrolu nad *Googleovim* i *Samsungovim* aplikacijama za kamere. Napadači mogu daljinski snimati fotografije, snimati video, špijunirati razgovore, identificirati lokaciju ljudi i još mnogo toga, [11].

Identifikacija i provjera autentičnosti objekata mogla bi biti izazovna zbog prirode IoT okruženja. Bitno je razmotriti upravljanje autentikacijom identiteta u IoT-u, budući da se više korisnika i uređaja treba međusobno provjeravati putem pouzdanih usluga. Osim toga, učinkovita implementacija ključeva i upravljanje ključevima izazov je za IoT uređaje jer može uzrokovati prevelike troškove na IoT čvorovima. Štoviše, u nedostatku zajamčenog tijela za izdavanje certifikata (engl. *Certificate Authority - CA*), potrebni su drugi mehanizmi za provjeru valjanosti kriptografskih ključeva i osiguranje integriteta prijenosa ključeva, [12].

3.2. Heterogenost i politike

IoT uređaji povezani s različitim tipovima entiteta s različitom složenošću sposobnosti i dobavljačima dolaze s različitim konfiguracijama, datumima, verzijama izdanja i korištenjem tehničkih sučelja koja su dizajnirana za potpuno različite funkcije. Stoga je potreban zahtjev za razvojem protokola za rad sa svim različitim uređajima. Još jedan izazov koji se mora razmotriti u IoT-u je dinamičko okruženje, u jednom trenutku uređaj može biti povezan s potpuno drugačijim skupom uređaja nego u nekom drugom trenutku, stoga je za osiguranje sigurnosti potreban optimalan kriptografski sustav s adekvatnim upravljanjem ključevima i protokolima, [12].

Trenutne politike koje se provode u računalnoj i mrežnoj sigurnosti možda neće biti primjenjive na IoT zbog njegove heterogene i dinamičke prirode. Stoga moraju postojati politike i standardi razvijeni kako bi se osiguralo da će se podacima upravljati, štititi i prenositi na učinkovit način. To uključuje mehanizam za provođenje takvih politika koji je potreban kako bi se osiguralo da svaki subjekt primjenjuje standarde.

Slično, za svaku uključenu IoT uslugu mora biti jasno identificiran Ugovor o razini usluge *(*engl. *Service Level Agreement – SLA*) kako bi se uvelo povjerenje ljudskih korisnika u IoT okruženje što će dodatno rezultirati njegovim rastom i skalabilnosti, [13].

Većina tehničkih sigurnosnih problema odnosi se na standarde proizvodnje, upravljanje ažuriranjem, fizičko očvršćavanje, znanje i svijest korisnika. Slabe i pogodne zadane lozinke, problemi s hardverom, nesiguran prijenos i pohrana podataka od strane tvrtki mogli bi izložiti uređaje raznim napadima i time ugroziti korisnika i uređaj. Mnogi IoT uređaji imaju operativna ograničenja kao što su niska procesorska snaga i mala memorija koja je dovoljna za obavljanje dodijeljenih zadataka i ne mogu podnijeti ispravna ažuriranja softvera. Zbog nesvjesnosti i neznanja korisnika, tvornički zadane lozinke se obično zaboravljaju promijeniti. Neki uređaji imaju lošu lozinku koju je lako „provaliti“ u zlonamjerne svrhe. Mnoge poznate tvrtke zato nude dvofaktorsku autentikaciju kako bi eliminirali rizik od sigurnosnih prijetnji, ali još uvijek milijuni IoT uređaja ne podržavaju ovu značajku. Promjena tvornički zadanih lozinki, instaliranje potrebnih ažuriranja, onemogućavanje daljinskog pristupa IoT uređajima kada nisu potrebni, onemogućavanje značajki koje se ne koriste također mogu smanjiti rizik od kompromitacije. Wi-Fi mreže također su jedna od prvih točaka sigurnosnih napada koji cijelu mrežu čine ranjivom. Postavljanje jakih lozinki i metoda šifriranja za Wi-Fi mreže, može ublažiti rizik od sigurnosnih napada, [10].

3.3. Standardizacija i implementacija

Izazovi s kojima se susreće IoT standardizacija mogu se podijeliti u četiri kategorije: platforma, povezivanje, poslovni model i *killer* aplikacije[1].

- Platforma – ovaj dio uključuje oblik i dizajn proizvoda, analitičke alate koji se koriste za rješavanje ogromne količine podataka koji se prenose sa svih proizvoda na siguran način i skalabilnost što znači široko prihvaćanje protokola kao što je IPv6 u svim vertikalnim i horizontalnim tržištima.
- Povezivanje - ova faza uključuje sve dijelove potrošačeve dnevne i noćne rutine, od korištenja nosivih uređaja, pametnih automobila, pametnih domova i u velikoj shemi, pametnih gradova. S poslovne perspektive imamo povezivanje

[1] *„killer“ aplikacija - softverski program s korisničkim sučeljem koji se smatra dovoljno inovativnim tako da utječe na računalne trendove i prodaju*

koristeći Industrijski Internet stvari gdje M2M[2] (engl. *Machine-to-machine)* komunikacije dominiraju poljem.

- Poslovni model - ovaj model mora zadovoljiti sve zahtjeve za sve vrste e-trgovine, vertikalna tržišta, horizontalna tržišta i potrošačka tržišta, ali ova kategorija je uvijek žrtva regulatornog i pravnog nadzora.
- *Killer* aplikacije - u ovoj kategoriji postoje tri funkcije potrebne za *killer* aplikacije: kontroliranje stvari, prikupljanje podataka i analiziranje podataka. IoT-u su potrebne *killer* aplikacije za pokretanje poslovnog modela pomoću objedinjene platforme, [14].

Ne postoji univerzalni standard za cijelu industriju, što znači da sve tvrtke moraju razviti vlastite protokole i smjernice. Nedostatak standardizacije otežava osiguranje IoT uređaja, a također otežava omogućavanje komunikacije između stroja (M2M) bez povećanja rizika.

Povećanje sigurnosti doma jedna je prednost pametnog kućnog uređaja. Instaliranjem pametnih kamera korisnici mogu pratiti svoj dom u bilo koje vrijeme bilo gdje i primati sigurnosna upozorenja na svoj mobilni telefon. Pametne brave za vrata također smanjuju rizik od zaključavanja iz kuće. Korisnici mogu osigurati i zaključati vrata s bilo kojeg mjesta ako imaju pristup internetu. *Smart Home* uređaji se dijele na pametne uređaje, sigurnost, kontrolu i povezivanje, kućnu zabavu, upravljanje energijom te udobnost i rasvjetu. Mnoge tvrtke i dobavljači ulažu u uređaje za pametne kuće, a očekuje se da će tržište pametnih kuća dosegnuti 141 milijardu dolara do 2023. Pametni uređaji se obično povezuju ili jedni s drugima ili sa središnjim kontrolnim čvorištem putem kućne Wi-Fi mreže, [15].

Iako je pametni dom donio mnoge prednosti u živote ljudi, nedostaju im tehnički standardi i heterogene platforme. Nekoliko tvrtki prihvatilo je industrijske standarde koji su doveli do više nekompatibilnih platformi i tehnologija. Pametni uređaji i senzori prikupljaju mnogo informacija o ljudima kako bi naučili i predvidjeli njihovo ponašanje. Da bi automatizirali zadatak, moraju znati što, gdje i kada ljudi rade zadatak. Pametni uređaji znaju u kojoj prostoriji i kada treba uključiti ili isključiti svjetla. Stoga povezivanje ovih uređaja s bežičnim mrežama i internetom čini korisnike ranjivima na zlonamjerne

[2] *M2M – machine-to-machine - izravna je komunikacija između uređaja koji koriste bilo koji komunikacijski kanal, uključujući ožičeni i bežični*

napade što dodatno rezultira prijetnjama sigurnosti i privatnosti kao što su krađa identiteta i curenje podataka, [16].

Proliferacija IoT uređaja i porast broja kaznenih djela kibernetičke sigurnosti doveli su do poboljšanja forenzičkih istražnih tehnika u IoT-u. Pametne kuće mogu se smatrati jednostavnim oblikom IoT okruženja koje može biti dobra polazna točka za istraživanje izazova provođenja forenzičkih istraživanja u IoT okruženju. Neki od glavnih izazova koje forenzički istražitelji moraju prevladati u bilo kojoj forenzičkoj istrazi postoje u fazi prikupljanja podataka i fazi analize podataka gdje odgovarajući i prikladni forenzički alati igraju važnu ulogu u podršci forenzičkim istražiteljima u istragama. Još jedan izazov je što svaka država ima propisano kojim točno forenzičkim alatom se može provoditi istraga i to dovodi istražitelje u tešku situaciju jer ako koriste neki drugi forenzički alat (koji je bolji u ekstrakciji i analizi podataka/dokaza) na sudu se nebi priznali forenzički dokazi koji su prikupljeni tim alatom, iako bi se time omogućila bolja forenzička istraga, [17].

Instalirane aplikacije na korisnikovom mobilnom telefonu/računalu koje se koriste za upravljanje IoT uređajima u pametnom domu generiraju podatke specifične za korisnika gdje su neki od podataka pohranjeni na lokalnoj pohrani uređaja mobilnog telefona, a ostatak podataka mogao bi se pohraniti na poslužitelje u oblaku. Podaci pohranjeni u oblaku neće biti dostupni tijelima za provođenje zakona ako dođe do neke kriminalne radnje osim ako davatelji usluga u oblaku ne budu pod nekim zakonskim obvezama da to učine. To pokazuje da je suradnja između vlade, akademske zajednice i industrije od vitalnog značaja za reguliranje i standardizaciju IoT industrije iz sigurnosne perspektive pomoću koje bi se naknadno provodile forenzičke istrage, [18].

Razumljivo je da pružatelji usluga u oblaku nerado posvećuju svoje resurse za provođenje takvih forenzičkih istraga, osim ako se ne daju neki poticaji. Stoga se predlaže IoT forenzika kao usluga koju nude pružatelji usluga u oblaku kako bi podržali agencije za provođenje zakona u njihovim forenzičkim istragama kada je to potrebno. Međutim, postoje neki tehnički i pravni izazovi za pružanje takvih usluga koji zahtijevaju više istraživanja i ulaganja. Primjerice, neki od pravnih izazova koji se odnose na privatnost i zaštitu podataka mogli bi se riješiti istraživanjem opcija i ažuriranjem pravnih ugovora o uslugama korisnika, [19].

3.4. Pitanja privatnosti

Rast popularnosti Interneta stvari doveo je do mnogih sigurnosnih problema u vezi s problemima skalabilnosti i interoperabilnosti među IoT uređajima. Prijetnje eksponencijalno rastu u smislu učestalosti napada i složenosti. Međutim, međusobno povezani uređaji ne izlažu samo sigurnosna pitanja, već postoji i ozbiljna zabrinutost u vezi s privatnošću. Priroda pametnih domova otvara korisnika mnogim različitim problemima vezanim uz privatnost od neprihvatljivog ili neprimjerenog pristupa nečijim osobnim podacima od strane napadača, do psiholoških dimenzija privatnosti (samoća, rezerviranost, izolacija, anonimnost, intimnost) ili čak fizičke povrede privatnosti gdje samom domu pristupi neovlaštena osoba, [20].

Velik dio u razvoju značajke pametnih domova koja omogućuje udaljeni pristup i nadzor bilo je uvođenje pohrane u oblaku od strane trećih strana. To omogućuje da podaci iz pametnog doma budu dostupni s bilo kojeg mjesta. Treća strana mogla bi pohraniti zabrinjavajuću količinu osobnih podataka i privatnih informacija. To je bio slučaj s kineskom tvrtkom Orvibo koja pruža pametna rješenja za domove korisnika. Tvrtka je bila podvrgnuta povredi podataka uslijed koje je otkriveno 2 milijarde zapisa u vezi s pametnim kućnim uređajima. Informacije poput lozinki, kodova za resetiranje računa, precizne geolokacije i informacije o rasporedu bile su uključene u provalu. Takve informacije bi napadačima pružile informacije o korisničkim rutinama i lokacijama, potencijalno identificirajući kada su kuće prazne, što bi omogućilo mogućnosti provale u korisnikov dom. Informacije bi također mogle neke od uređaja učiniti beskorisnima, poput pametnih brava ili sigurnosnih kamera, budući da bi im napadači mogli pristupiti i time nanijeti štetu korisniku, [21].

Kada kupuju i postavljaju nove pametne kućne uređaje, korisnici se također mogu složiti da će dopustiti da se njihovi podaci koriste na način koji nije samo za sam uređaj, kao što je slučaj s *Amazonovim* Alexa uređajem. Uređaj omogućuje korisnicima postavljanje pitanja i glasovnu interakciju s uređajem. Radnici analiziraju uzorke glasa poslane na uređaj kako bi poboljšali *Amazonov* softver za prepoznavanje glasa. To predstavlja nekoliko problema s podacima koje bi uređaj mogao nenamjerno uhvatiti. Privatni razgovori koje korisnici vode u svom domu tada više nisu tako privatni. Takvo korištenje podataka također može dovesti do povjerljivosti i moralnih problema. Tako

je dvoje radnika izjavilo da su čuli nešto za što vjeruju da je bio fizički napad kada su analizirali glasovne uzorke, [22].

Rast pametnih domova te raznolikost i količina IoT uređaja povezanih unutar domova povećali su područje napada za zlonamjerne aktere. Kao što je identificirano u Trendovima kibernetičke sigurnosti, pametni domovi bit će popularne mete zlonamjernih aktera zbog broja potencijalnih ulaznih točaka. Ako napadač može dobiti pristup jednom pametnom uređaju unutar doma, potencijalno bi mogao imati pristup cijeloj mreži, što bi rezultiralo izlaganjem osobnih podataka i privatnih informacija (prisluškivanje). Godine 2017., službeno tijelo za provjeru proizvoda u Njemačkoj uputio je roditelje da unište ili maknu iz kućanstva lutku koja ima sposobnost pričanja po imenu Cayla. Otkriveno je da je ugrađeni Bluetooth uređaj nesiguran i da bi se mogao iskoristiti dopuštajući napadaču slušanje i razgovaranje s djetetom koje se igra s takvom lutkom, [23].

3.5. Najčešće sigurnosne prijetnje i napadi IoT okruženja

Sigurnosni uređaji povezani s Internetom pružaju brz i jednostavan način za stvaranje kućnog sigurnosnog sustava. No, stvaraju i mogućnosti za sigurnosnu slabost. Dvije glavne mane u pametnim domovima su ranjive lokalne mreže i slabi IoT uređaji koje ih čine osjetljivim na napade. Bežična mreža može biti ranjiva na napad zbog zadanih ili slabih SSID-ova (engl. *Service Set Identifier*) ili lozinki i ranjivih protokola šifriranja. Zadane vjerodajnice omogućuju uljezu da bez napora pristupi usmjerivaču. Snažne Wi-Fi lozinke prisiljavaju *hakere* da traže neka druga čvorišta za infiltriranje u mrežu.

Njuškanje (engl. *Sniffing*) najčešći je način na koji napadači upadaju u mrežu. U njuškanju, napadači otimaju bilo koji paket podataka koji se prenose između uređaja i usmjerivača, prenose ga na svoj uređaj i koriste „grubu silu“ kako bi ga dešifrirali. Obično je za takav napad potrebno samo nekoliko minuta. Većina Wi-Fi usmjerivača koristi WEP (engl. *Wired Equivalent Privacy*), WPA (engl. *Wi-Fi Protected Access*) ili WPA2 sigurnosni protokol. Slabost WEP-a je mala veličina vektora inicijalizacije (24-bitni), što uzrokuje ponovno korištenje, a to ga ponavljanje čini ranjivim. Pametni kućni uređaji osjetljivi su na napade jer su oni uređaji napravljeni za posebne namjene. Dobavljači IoT uređaja ne pružaju potrebna sigurnosna rješenja posebne namjene. Nadalje, pametne kućne uređaje često pokreću mali operativni sustavi kao što su

INTEGRITY, Contiki, FreeRTOS i VxWorks, itd., čija sigurnosna rješenja nisu tako robusna kao ona u sustavima Windows ili Linux, [24].

Napadi na pametne kućne uređaje izvode se u različitim metodama, ovisno o uređaju i komunikacijskom protokolu. Uobičajene metode napada uključuju:

- Povreda podataka i krađa identiteta - nesigurni IoT uređaji generiraju podatke i pružaju *cyber* napadačima dovoljno prostora za ciljanje osobnih podataka. To bi potencijalno moglo završiti krađom identiteta i lažnim transakcijama.
- Čovjek u sredini (engl. *Man in The Middle – MITM*) - napad gdje napadač presreće komunikaciju između dva sustava. To je opasan napad jer se napadač predstavlja kao izvorni pošiljatelj, a budući da napadač ima originalnu komunikaciju on može prevariti primatelja tako da on i dalje misli da dobiva legitimnu poruku.
- Preuzimanje kontrole nad uređajem - takve je napade prilično teško otkriti jer napadač ne mijenja osnovnu funkcionalnost uređaja. U ovom napadu potreban je samo jedan uređaj da bi se potencijalno zarazilo sve pametne uređaje u kući. Primjerice, napadač koji u početku kompromitira termostat teoretski može dobiti pristup cijeloj mreži i na daljinu otključati vrata ili promijeniti PIN kod sigurnosnog sustava (alarma) kako bi ograničio ulazak.
- Napad distribuiranog uskraćivanja usluge (engl. *Distributed Denial of Service* – DDoS) - zlonamjerni je pokušaj poremećaja normalnog prometa ciljanog poslužitelja, usluge ili mreže preplavljivanjem cilja ili okolne infrastrukture „poplavom“ internetskog prometa. U slučaju DDoS napada, dolazni promet koji poplavljuje cilj potječe iz više izvora, što otežava zaustavljanje napada jednostavnim blokiranjem jednog izvora.
- Stalno uskraćivanje usluge (engl. *Permanent Denial of Service* – PDoS) je napad koji toliko oštećuje uređaj da zahtijeva zamjenu ili ponovno instaliranje hardvera, [7].

4. Suvremene metode zaštite IoT okruženju

Novi uređaji se velikom brzinom uključuju u Internet stvari. Iako se očekuje da će IoT ponuditi mnoge prednosti, dodavanje nesigurnih uređaja u mrežu poduzeća može imati ozbiljne posljedice. Dobra vijest je da sigurnosne politike i procedure mogu zaštititi infrastrukturu IoT okruženja, očvrsnuti IoT konfiguracije i učiniti okruženje pametnijim i branjivijim. Istraživanja pokazuju da većina sustava nije ugrožena sofisticiranim ili specifičnim ranjivostima uređaja, već zbog nedostatka osnovnih sigurnosnih kontrola. Iako rizični uređaji imaju neke zajedničke stvari kao što je korištenje TCP/IP protokola i softvera temeljenom na Internetu, također pokrivaju širok spektar cijena, primjene i namjene. Ta kategorija uključuje tipičnu IT opremu kao što su pametni telefoni, tableti, senzorska oprema i kontrolni sustavi, kao i video kamere, mrežni pisači, industrijske kontrole i medicinska oprema, [25].

4.1. Metode zaštite pametnih domova i zgrada

Sigurnost je imperativ. Za tvrtke i dobavljače hardvera, kao i za korisnike pametnih domova uvođenje nove tehnologije i povećanje globalnih implementacija donosi bezbroj novih sigurnosnih problema koje treba uzeti u obzir prilikom implementacije M2M uređaja. Do 2025. godine 25% podataka koje ljudi generiraju bit će u stvarnom vremenu, to znači da se mora osigurati sigurnost od samog početka i filtrirati je kroz sve poslovne funkcije. Internet stvari donosi sigurnosne izazove, no mogu se riješiti korištenjem znanja i praktičnih rješenja. U sljedećim navodima opisano je nekoliko najboljih savjeta koji će pomoći u informiranju cjelokupne IoT strategije kibersigurnosti i koji će omogućiti implementaciju sigurnosnih mjera, [26].

Budući da su IoT uređaji često udaljeni, fizička sigurnost ključna je za sprječavanje neovlaštenog pristupa uređaju. Ovdje je vrijedno koristiti otporne komponente i specijalizirani hardver koji otežava pristup korisničkim podacima. Na primjer, u mobilnim IoT uređajima puno kritičnih informacija pohranjuje se na SIM (engl. *Subscriber Identity Module*) karticu. Većina oblika SIM kartice može se ukloniti, što ove podatke čini ranjivijima. Međutim, eSIM je zalemljen izravno na tiskanu ploču. Teže im je fizički pristupiti, a također su otporniji na promjene temperature i oštećenja od udara, što se ponekad koristi u pokušajima sabotaže ili hakiranja uređaja. Štoviše, potreban je robustan sigurnosni protokol daljinskog pristupa koji omogućuje funkcionalnost SIM-

a koja se može zaključati za određene uređaje i mogućnost daljinskog onemogućavanja veza ako dođe do fizičke povrede sigurnosti. IMEI (engl. *International Mobile Equipment Identity*) jedinstveni je identifikacijski broj koji se nalazi na većini mobilnih uređaja. Zaključavanje IMEI-ja omogućit će konfiguraciju funkcionalnosti SIM-a na određeni IMEI u stvarnom vremenu kako bi se spriječilo uklanjanje SIM-a i korištenje na bilo kojem drugom uređaju, [27].

Slanje i primanje poruka putem udaljenih uređaja samo po sebi predstavlja sigurnosni rizik. Povezivanjem uređaja i omogućavanjem ove komunikacije putem mreža s javnim pristupom, kao što je Wi-Fi, te se poruke otvaraju za presretanje. Šifriranje poruka korak je u pravom smjeru, ali korištenje javnih mreža za slanje osjetljivih podataka zahtijeva više mjera opreza. Preporučuje se izgradnja privatnih mreža povrh postojećih sigurnosnih mehanizama kako bi se osiguralo da podaci nikada ne prijeđu i mrežu s javnim pristupom. Tipično, mali M2M uređaji imaju ograničenu procesorsku snagu, a to ih sprječava u uspostavljanju vatrozida. Mrežni vatrozid, međutim, štiti podatke u trenutku kada uđu u mrežu. Ovo uklanja intenzivan proces filtriranja paketa s uređaja, osiguravajući da se zlonamjerni promet nikada ne prenosi na uređaj niti uopće može ući u mrežu. Mrežni vatrozidi omogućuju tvrtkama praćenje i blokiranje prometa izvan VPN-a (engl. *Virtual Private Network*) ili jednostavno blokiraju određene komunikacije. Također može otkriti upade ili pokušaje hakiranja koji nisu u skladu s unaprijed konfiguriranim pravilima, [28].

Tek nekoliko uređaja koristi šifrirane komunikacije kao dio svoje početne konfiguracije. Umjesto toga, većina koristi obične web protokole koji komuniciraju preko interneta u obliku običnog teksta, što ih čini lakim metama za hakere koji promatraju mrežni promet kako bi identificirali slabosti. U najmanju ruku, sav web promet trebao bi koristiti HTTPS protokol (engl. *HyperText Transfer Protocol Secure*), TLS protokol (engl. *Transport Layer Security*), SFTP protokol (engl. *Secure File Transfer Protocol*), sigurnosna proširenja DNS-a (engl. *Domain Name System*) i druge sigurne protokole za komunikaciju preko interneta. Osim toga, uređaji koji se povezuju s mobilnim aplikacijama ili drugim udaljenim pristupnicima trebali bi koristiti šifrirane protokole kao i šifrirati podatke pohranjene na flash pogonima. Jedan od razloga za šifriranje podataka jest osigurati da zlonamjerni softver nije zarazio uređaj, [29].

Važno je razumjeti razliku između restriktivnih mrežnih komunikacija i permisivnih mrežnih komunikacija. Na primjer, postoji razlika između osobnog

računala koje cijeli svoj tvrdi disk dijeli sa svima i web poslužitelja koji samo nekolicini ovlaštenih korisnika ograničava pregled njegovog sadržaja. Za razliku od većine ograničenih web poslužitelja, pretpostavka je da su IoT uređaji, kao što su temperaturni senzori, permisivni. Prema zadanim postavkama mogu i trebaju komunicirati s bilo kim i bilo kojim uređajem. Ova popustljiva komunikacija dio je njihovog dizajna. Dobavljači žele sudjelovati na mrežama i dijele svoje podatke s raznim alatima i softverskim programima. Nažalost, permisivnost je ono što ove uređaje čini inherentno nesigurnima i ranjivima na sve vrste iskorištavanja. Umjesto toga treba implementirati restriktivne mrežne komunikacije, kao što su pravila ugrađenog vatrozida ili pažljivija provjera autentičnosti korisnika ili aplikacije. Uređaji ne bi trebali biti dostupni standardnim TCP/IP priključcima kao što su Telnet ili FTP (engl. *File Transfer Protocol*), a korisnici ne bi trebali pretpostaviti da rade iza vatrozida poduzeća koji će spriječiti komunikaciju preko mreže ili van na Internet. Jedan od načina za pružanje bolje sigurnosti je izolacija senzora i drugih permisivnih uređaja na zasebnom virtualnom LAN-u. Ova postavka sprječava hakera da promatra cjelokupni mrežni promet ako je jedan senzor ugrožen ili da ga koristi za pokretanje napada na cijelo poduzeće, [25].

Odgovornost za sigurnost IoT uređaja prvenstveno leži na programerima IoT uređaja. Oni bi trebali poduzeti potrebne mjere kako bi uređaji bili sigurni. Neke potencijalne mjere mogle bi biti:

- Integracija programabilnog hardverskog korijena povjerenja (engl. *Hardware Root of Trust* – HRoT) unutar IoT uređaja. HRoT je temelj sigurnog rada elektroničkih uređaja, posebice sustava na čipu (engl. *System on Chip – SoC*). Sadrži ključeve koji se koriste za kriptografske funkcije i omogućuje siguran proces pokretanja sustava. Programabilni HRoT može se kontinuirano ažurirati kako bi se borio sa sve većim rasponom prijetnji. Pokreće potpuno nove kriptografske algoritme i osigurava aplikacije da se suoče s evoluirajućim napadima.
- *Edge Computing* - distribuirana računalna paradigma koja računanje i pohranu podataka približava izvorima podataka. Očekuje se da će ovo poboljšati vrijeme odziva i uštedjeti propusnost. Podaci ne putuju kroz slabe mreže do udaljenih poslužitelja, pa je rizik od provale smanjen.

- Dizajniranje OTA (engl. *Over The Air*) mogućnosti ažuriranja - proizvodnja uređaja s učinkovitim OTA mogućnostima nadogradnje. Mnogi potrošači imaju svoje uređaje na udaljenim lokacijama i stoga ih neredovito ažuriraju. Programeri moraju uključiti robusnu OTA strategiju ažuriranja koja se može izvršavati učinkovito i redovito, [24].

4.2. Metode zaštite pametnih gradova

Povezani pametni gradski uređaji trebaju biti zaštićeni sveobuhvatnim IoT sigurnosnim rješenjima (uređaj u oblak). Praktična i jednostavna, a opet sigurna rješenja koja OEM (engl. *Original Equipment Manufacturer*) proizvođači i usluge mogu lako i široko usvojiti učinkovitija su od „super rješenja“. Takva rješenja trebaju uključivati sljedeće mogućnosti:

- **Integritet *firmwarea* i sigurno pokretanje** - sigurno pokretanje koristi tehnike potpisivanja kriptografskog koda, osiguravajući da uređaj izvršava samo kod koji je generirao OEM uređaja ili druga povjerljiva strana. Korištenje tehnologije sigurnog pokretanja sprječava *hakere* da zamijene *firmware* zlonamjernim verzijama, čime se sprječavaju napadi. Nažalost, nisu svi IoT skupovi čipova opremljeni mogućnostima sigurnog pokretanja. U takvom scenariju važno je osigurati da IoT uređaj može komunicirati samo s ovlaštenim servisima kako bi se izbjegao rizik zamjene *firmwarea* zlonamjernim skupovima uputa.
- **Uzajamna provjera autentičnosti** - svaki put kada se pametni gradski uređaj spoji na mrežu, treba ga autentificirati prije primanja ili prijenosa podataka. Time se osigurava da podaci potječu s legitimnog uređaja, a ne iz lažnog izvora. Sigurna i uzajamna autentikacija gdje dva entiteta (uređaj i usluga) moraju dokazati svoj identitet jedna drugoj pomaže u zaštiti od zlonamjernih napada.
- **Sigurnosno praćenje i analiza** - hvata podatke o ukupnom stanju sustava, uključujući uređaje krajnjih točaka i promet putem povezivanja. Ti se podaci zatim analiziraju kako bi se otkrile moguće povrede sigurnosti ili potencijalne prijetnje sustavu. Nakon otkrivanja treba izvršiti širok raspon radnji formuliranih u kontekstu cjelokupne sigurnosne politike sustava, kao što je karantena uređaja na temelju nepravilnog ponašanja.
- **Upravljanje životnim ciklusom sigurnosti** - značajka upravljanja životnim ciklusom omogućuje pružateljima usluga i proizvođačima originalne opreme

kontroliranje sigurnosnih aspekata IoT uređaja dok rade. Brza OTA zamjena ključeva uređaja tijekom oporavka od *cyber* katastrofe osigurava minimalan prekid usluge. Osim toga, sigurno povlačenje uređaja iz upotrebe osigurava da se rashodovani uređaji neće prenamijeniti i iskorištavati za povezivanje s uslugom bez ovlaštenja, [30].

Rambus je američka tvrtka koja stvara proizvode i usluge koji osiguravaju podatke i pružaju bolju, bržu komunikaciju između IoT uređaja omogućujući aplikacije i usluge koje poboljšavaju živote ljudi. Neka od sigurnosnih rješenja za pametne gradove su [30]:

- *Root of Trust* rješenja pružaju temelj na razini hardvera za sigurnosne funkcije kao što su sigurno pokretanje, sigurno izvršavanje aplikacija, otkrivanje neovlaštenih promjena i zaštita te sigurno skladištenje i rukovanje ključevima.
- *Protocol Engines* osigurava mrežnu komunikaciju između IIoT uređaja i oblaka bez mijenjanja prometa. Omogućuju sigurnu komunikaciju s kraja na kraj, a istovremeno održavaju vitalne performanse mreže.
- Pružanje i upravljanje ključevima osiguravaju rješenja opskrbnog lanca za proizvođače čipova i IoT uređaja, te omogućuju sigurno umetanje ključeva i usluge upravljanja ključevima uređaja temeljene na oblaku.

4.3. Tehnike sigurnosti i privatnosti u IoT okruženju

U slijedećim navodima biti će opisane neke od tehnika sigurnosti i privatnosti u IoT okruženju. Autori u [31] predlažu CATSWoTS (engl. *Context-Aware Trustworthy Social Web of Things System*) koji rješava problem interoperabilnosti uključivanjem web tehnologija. Aspekt društvenog weba u dizajniranom sustavu pomaže u dobivanju preporuka iz društvenih odnosa. U radu prvo navodi važnost ovisnosti o kontekstu povjerenja i kriterija kvalitete usluge (engl. *Quality of Service – QoS*) za prepoznavanje i preporuku pouzdanih aplikacija WoT (engl. *Web of Things*). Stoga se u projektiranom sustavu razmatraju parametri svijesti o kontekstu i ograničenja QoS-a. CATSWoTS procjenjuje pružatelje usluga na temelju navedenih parametara i ograničenja, a zatim identificira prikladnog pružatelja usluga korištenjem kolaborativnog filtriranja koji se temelji na pravilima. Eksperimenti su provedeni korištenjem stvarnog QoS skupa podataka za procjenu performansi dizajniranog CATSWoTS-a. Ukratko, dizajnirani

CATSWoTS pokazao je dobre rezultate dinamičkim identificiranjem i preporukom pouzdanih usluga, prema zahtjevima tražitelja usluge.

U dokumentu [32] predlaže se posrednik koji čuva privatnost odnosno enkripciju temeljenu na atributima (engl. *Attribute Based Encryption – ABE*) gdje se IoT pristupnik čini posrednikom. Općenito, posrednik je moćniji od drugih uređaja. Stoga je ABE shema odvojena u dva dijela: zadatak ugradnje pravila i zadatak šifriranja. Zadatak ugradnje pravila, premješta se na posrednika, dok se zadatak šifriranja zadržava u senzoru kako bi se posrednik spriječio u prisluškivanju i stoga se shema brine o sigurnosti i praktičnosti u isto vrijeme. Osim toga, ovaj dokument ukazuje na važno pitanje privatnosti podataka u oblaku. Budući da se podaci tamo obrađuju, oblak može biti prisiljen otvoriti podatke trećim stranama. Tradicionalne sheme šifriranja ne mogu zaštititi privatnost korisnika u ovom modelu napada. Ovaj dokument čini predloženu shemu shemom šifriranja bez obveze. Stoga se oblak može nositi s vanjskom prisilom pružanjem lažnih podataka.

Autori u [33] imali su za cilj osigurati sigurno IoT okruženje predlažući učinkovitu tehniku upravljanja ključevima koja koristi kombinaciju simetričnih i asimetričnih kriptosustava. Njihov prijedlog razmatra skup pametnih objekata koji je sposoban za registraciju, generiranje i distribuciju ključeva u prijenosu IoT podataka. Oni koriste MQTT (engl. *Message Queuing Telemetry Transport*) protokol za olakšavanje komunikacije između izvorišnog i odredišnog čvora. Prikladnost predloženog pristupa mjerena je eksperimentalno, a rezultati su bili usporedivi s postojećim radom s obzirom na vrijeme konverzije ključa, vrijeme izvršenja algoritma, broj ponovnih veza i iskorištenje propusnosti.

5. Simulacija okruženja pametnog doma i sigurnosnih prijetnji

NetSim je mrežni simulator i emulator na razini paketa. Mrežnim inženjerima pruža tehnološko razvojno okruženje za modeliranje protokola, istraživanje i razvoj mreže i vojne komunikacije. Ponašanje i performanse novih protokola i uređaja mogu se istražiti u virtualnoj mreži unutar NetSim-a uz znatno nižu cijenu i u kraćem vremenu nego s hardverskim prototipovima. U tablici 1. je moguće vidjeti neke prednosti NetSim mrežnog simulatora u odnosu na neke druge *open-source* simulatore, [34].

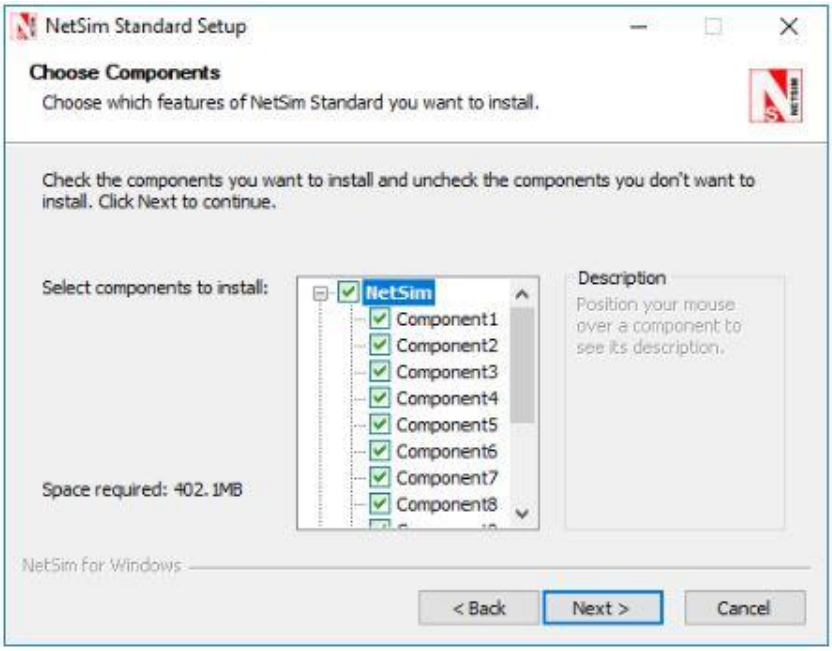
Tablica 1. Prednosti NetSim mrežnog simulatora u odnosu na druge simulatore

NetSim mrežni simulator	Besplatni ili drugi simulatori otvorenog koda
• Jednostavan GUI za projektiranje mreže. • Nadzorna ploča s rezultatima s grafikonima i tablicama • Paketna animacija za vizualno razumijevanje rada protokola.	• Simulatori otvorenog koda koriste sučelje naredbenog retka i skriptne jezike. • Vrlo teško za nekvalificirane korisnike za korištenje i razumijevanje.
• NetSim verzije podržavaju širok raspon tehnologija uključujući najnovije 802.11, 802.15.4, LTE, IOT, MANETs, 802.22, poboljšani TCP itd.	• Nema eksperimenata u najnovijim tehnologijama
• Dobro dizajnirani i ažurni priručnici za eksperimente i korisnike	• Nejasna dokumentacija, tj. napisana za programere, a ne za studente, nedostaju joj snimke zaslona, primjeri itd.
• Jednostavna instalacija i licenciranje	• Složen postupak instalacije sklon pogreškama
• Namjenska podrška - online podrška uživo tijekom instalacije. Služba za podršku nakon instalacije. Treninzi putem team viewera. Mjesečni webinari.	• Podrška otvorenog koda - ovisi o neformalnoj mreži ljudi koji će odgovoriti na upite na forumu.

Izvor: [35]

5.1. Priprema i instalacija simulacijskog alata NetSim

Za potrebe izvršavanja simulacije okruženja pametnog doma koristit će se standardna verzija NetSim alata, odnosno NetSim Standard. Jedan od prozora koji će se pojaviti prilikom instalacije alata je licencni ugovor. Najvažniji dio instalacije je odabir komponenti. Takav popis komponenti je dostupan samo pri instalaciji standardne ili Pro verzije, dok su ostale verzije NetSim-a dostupne kao jedan paket. Prilikom odabira komponenti kod instalacije NetSim alata što je prikazano slikom 4., tvrtka *Tetcos* preporuča odabir svih komponenti za potpunu instalaciju softvera kako bi provedene simulacije bile što vjerodostojnije.

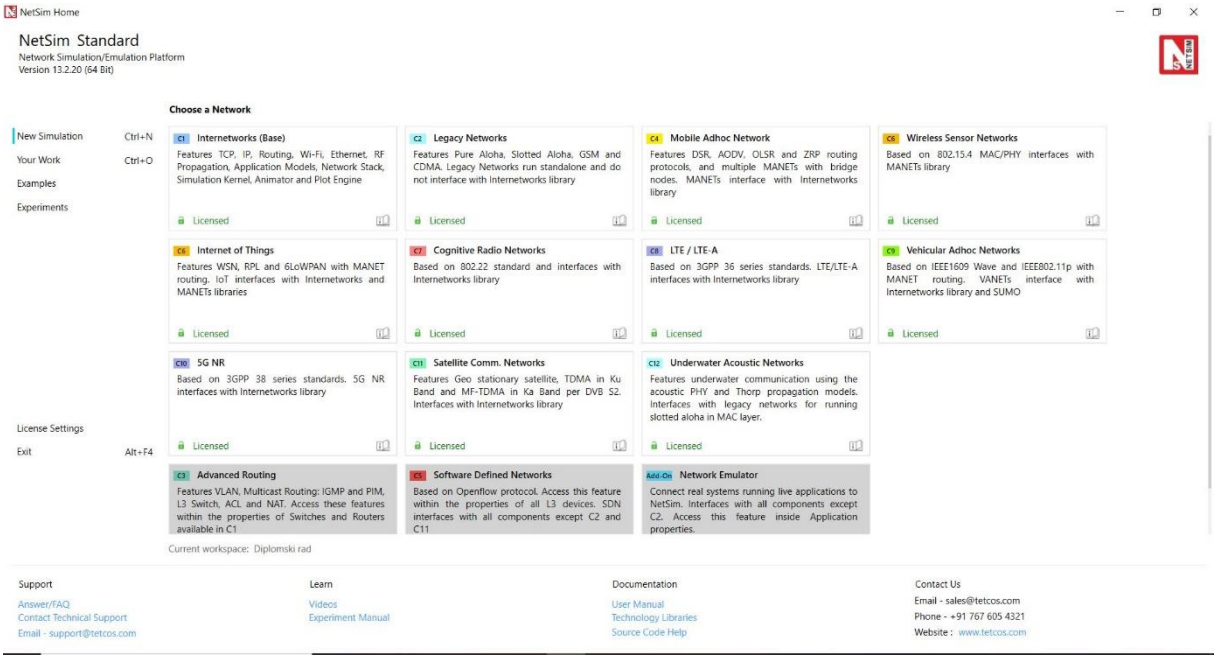


Slika 4. Odabir komponenti koje se žele instalirati

Nakon svih provedenih koraka slijedi instalacijski proces. U procesu instalacije NetSim alata kako bi se instalacija u potpunosti završila slijedi instalacija drugih potrebnih alata koji su u nekim koracima važni kako bi se što vjernije interpretirali rezultati simulacija. Za NetSim standardnu i Pro verziju, instalacija alata *Wireshark* će početi ukoliko se na računalu ne nalazi najnovija verzija ili će ako je na računalu instalirana starija verzija toga alata ažurirati alat. Ako se na računalu nalazi najnovija verzija takvog alata prilikom instalacije će se preskočiti taj korak. Ovo ujedno vrijedi i za sve ostale softvere koji će se instalirati kao što su Python, USBPcap i Npcap.

5.2. Pokretanje NetSim-a i provođenje simulacije

Kada se NetSim alat otvara po prvi puta na NetSim ikonu na radnoj površini ili u bilo kojoj mapi gdje se instalirao alat treba odabrati opciju “Pokreni kao administrator”. Nakon toga se otvara prozor sa informacijama o licencnom poslužitelju gdje se u polju za unos licence umeće datoteka *.lic* koja sadrži licencu, a koju je Tetcos tvrtka proslijedila korisniku alata. Kada se alat otvori prikazuje se početni zaslon koji je prikazan na slici 5.



Slika 5. Početni zaslon NetSim alata

Na početnom zaslonu se mogu vidjeti sljedeća stavke:

- Nova simulacija: ovaj izbornik služi za odabir simulacija različitih vrsta mreža u NetSim-u. Mogu simulirati neke od sljedećih vrsta mreža: mobilne mreže, kognitivne radio mreže, bežične senzorske mreže, Internet stvari, LTE/LTE-A mreže (LTE/LTE-A, LTE D2D, LTE Vanet), 5G mreža, itd.
- Otvori simulaciju: ovaj izbornik služi za učitavanje spremljenih konfiguracijskih datoteka iz radnog prostora. Mogu se pogledati, modificirati ili ponovno pokrenuti postojeće simulacija. Uz to, korisnici također mogu izvesti spremljene datoteke iz trenutnog radnog prostora na željenu lokaciju na svom osobnom računalu.
- Primjeri: ovaj izbornik omogućava odabir simulacija različitih vrsta kategoriziranih tehnološki. Korisnici mogu odabrati bilo koju mrežu koju žele, a

koja je predefinirana. Klikom na bilo koju otvorit će se već postojeća simulacija koju korisnici mogu pokrenuti i analizirati.

- Eksperimenti: ovaj izbornik omogućava učenje mrežnih koncepata kroz simulaciju eksperimenata. Dokumentacija dolazi sa ciljem, teorijom, rezultatima i diskusijom.

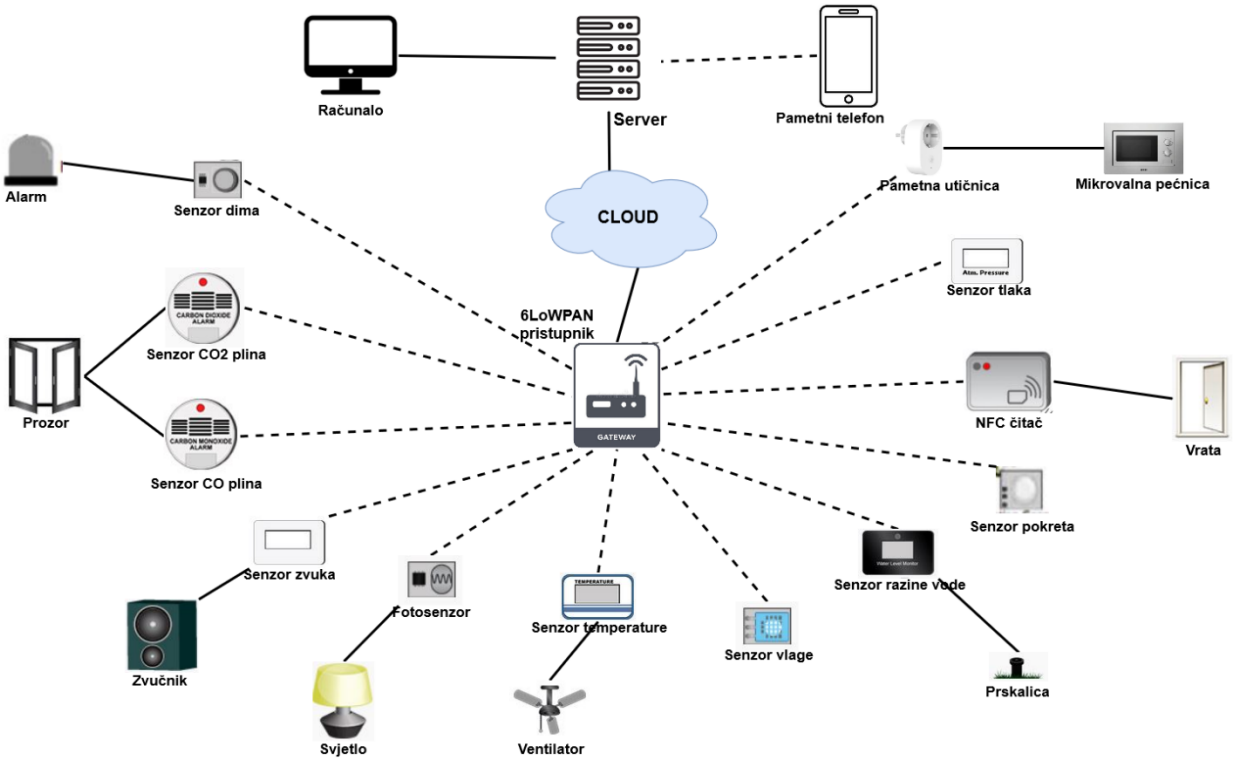
Mrežna topologija koja će se koristiti u simulaciji prikazana je na slici 6. Dizajn pametnog doma na slici sastoji se od različitih senzora koja služe korisniku za poboljšanje i automatizaciju svakodnevnih aktivnosti. Svaki senzor ima svoju namjenu i korisnik može upravljati s njime u svakom trenutku. Topologija se sastoji od 12 senzora, 6LoWPAN (engl. *Low Power Wireless Personal Area Network*) pristupnika, rutera i krajnjeg uređaja (stolno računalo ili pametni telefon) pomoću kojeg korisnik može upravljati sustavom. Senzor dima je uređaj koji se ugrađuje većinom na vidljiva mjesta, a služi za otkrivanje prevelike količine dima u kućanstvu te ukoliko je veća količina dima u prostoriji u kojoj se senzor nalazi uključuje alarm koji korisnika upozorava na prijetnju od požara. U dizajnu prikazanom na slici nalaze se također i senzori koji očitavaju količinu štetnih plinova u prostoriji kao što je npr. garaža u koju korisnik može parkirati neka od svojih motornih vozila bio to automobil ili neki motocikl. Ukoliko neki od senzora bio to senzor za CO plin ili senzor za CO2 plin očita veću količinu štetnog plina od uobičajene količine kako bi spriječili nakupljanje tih štetnih plinova u prostoriji ti senzori otvaraju prozor u prostoriji kako bi se smanjila količina plina provjetravanjem.

Sljedeći od senzora koji se nalazi u dizajnu je senzor zvuka koji se koristi za otkrivanje intenziteta zvuka. Ovaj senzor se koristi kod sustava za zabavu kako bi očitavao preveliku ili premalu vrijednost zvuka i time regulirao jačinu zvuka, te potrebno li je zvuk pojačati ili stišati. Fotosenzor je senzor svjetlosti koji upravlja sa svjetlom. Većinom se koriste kao i u ovom slučaju za automatsku rasvjetu gdje u sumrak uključuje, a u zoru isključuje svjetlo/rasvjetu. Također ako se u prostoriji spuštaju ili dižu rolete/zastori očitava količinu svjetlosti i u skladu s time uključuje ili isključuje svjetlo. Senzor temperature korisniku javlja kolika je temperature zraka u prostoriji. Ukoliko je veća temperatura koja korisniku ne pogoduje onda uključuje ventilator, a onda kad se temperatura smanji isključuje rad ventilatora.

Senzor vlage je također važan jer omogućuje jednostavno praćenje vlažnosti zraka radi zaštite električnih instalacija, upravljačkih ormarića, itd. Jedan od senzora je također i onaj za mjerenje razine vode u bunaru. Takav senzor se može postaviti u vanjski bunar gdje regulira i korisniku omogućuju uvid u razinu vode s kojom raspolaže. Također omogućuju upravljanje vanjskom prskalicom gdje prskalicu uključuje ako je količina vode u bunaru iznad prosjeka, te tu istu prskalicu nakon nekog vremenskog roka isključuje kako bi se voda sačuvala za kasniju upotrebu, odnosno kako bi se sačuvala voda posebno u mjesecima suše gdje je regulacija vode prijeko potrebna. Senzor pokreta je važan kod sigurnosti doma gdje pomoću njega korisnik dobiva informacije o pokretima ispred ili oko svojeg doma. Tada korisnik može prepoznati radi li se o neovlaštenoj osobi odnosno uljezu ili o nekome drugome.

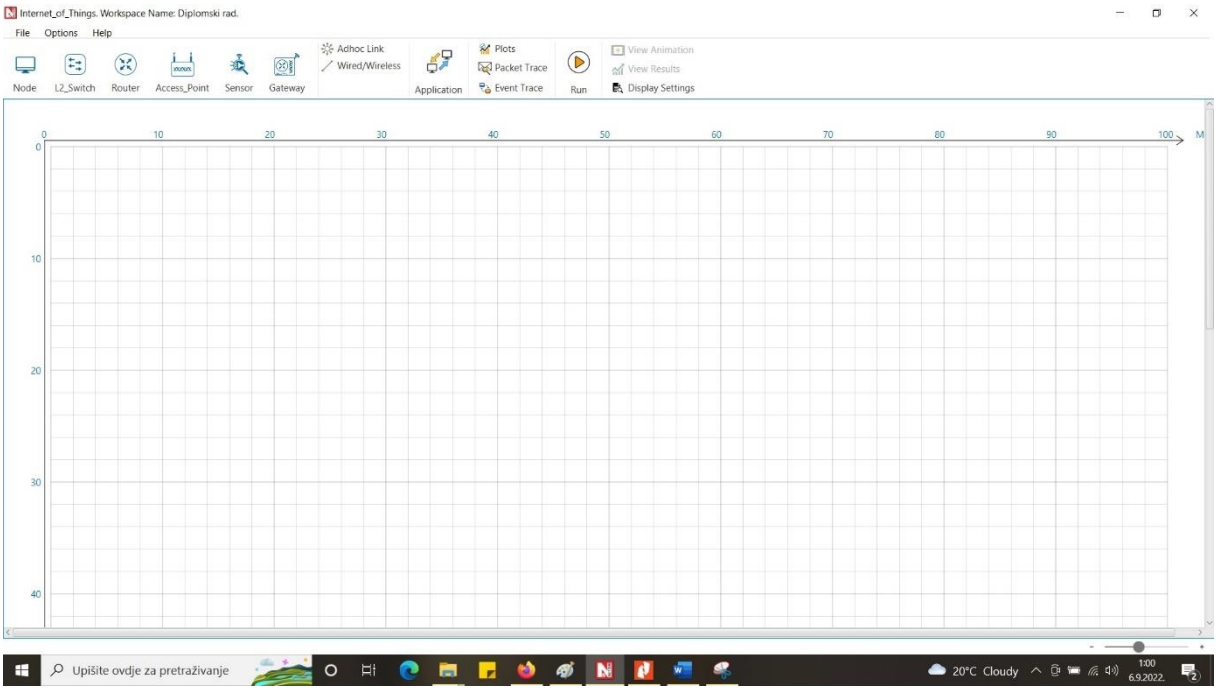
Kako bi se spriječio neovlašteni ulazak u korisnikov dom za ulazak u svoj dom korisnik može koristiti NFC (engl. *Near Field Communication*) tehnologiju. Pomoću NFC čitača koji se nalazi kod ulaznih vrata i NFC *tag*a koji se može nalaziti na poleđini pametnog telefona korisnika, korisnik ulazi u svoj dom, odnosno prislanjanjem pametnog telefona na čitač, čitač očitava da se radi o legitimnom korisniku te otključava vrata kako bi on mogao ući. Senzor tlaka očitava i javlja korisniku vrijednosti atmosferskog tlaka. Pametna utičnica pomaže korisniku kod uštede energije. Pomoću nje korisnik preuzima svu kontrolu nad uređajima koji su uključeni u nju. Pa tako korisnik može na daljinu vidjeti ako je prilikom odlaska iz doma zaboravio isključiti neke uređaje, primjerice mikrovalnu pećnicu, te pomoću pametnog telefona taj uređaj isključiti.

Sustav 6LoWPAN koristi se za različite primjene uključujući bežične senzorske mreže. Ovaj oblik bežične senzorske mreže šalje podatke kao pakete i koristi IPv6 - pružajući osnovu za naziv - IPv6 preko bežičnih osobnih mreža male snage. 6LoWPAN pruža način prijenosa paketnih podataka u obliku IPv6 preko IEEE 802.15.4 i drugih mreža. Omogućuje *end-to-end* IPv6 i kao takav može pružiti izravnu povezanost s velikom raznolikošću mreža, uključujući izravnu povezanost s Internetom. Na ovaj način, 6LoWPAN usvaja drugačiji pristup drugim rješenjima mreže bežičnih senzora male snage. Također jedni od važnih uređaja u pametnom domu su krajnji uređaji (stolno računalo ili pametni telefon). Pomoću njih korisnik može pristupiti cijelom sustavu pametnog doma te njime upravljati u unutrašnjosti doma ili na daljinu u svakome trenutku.



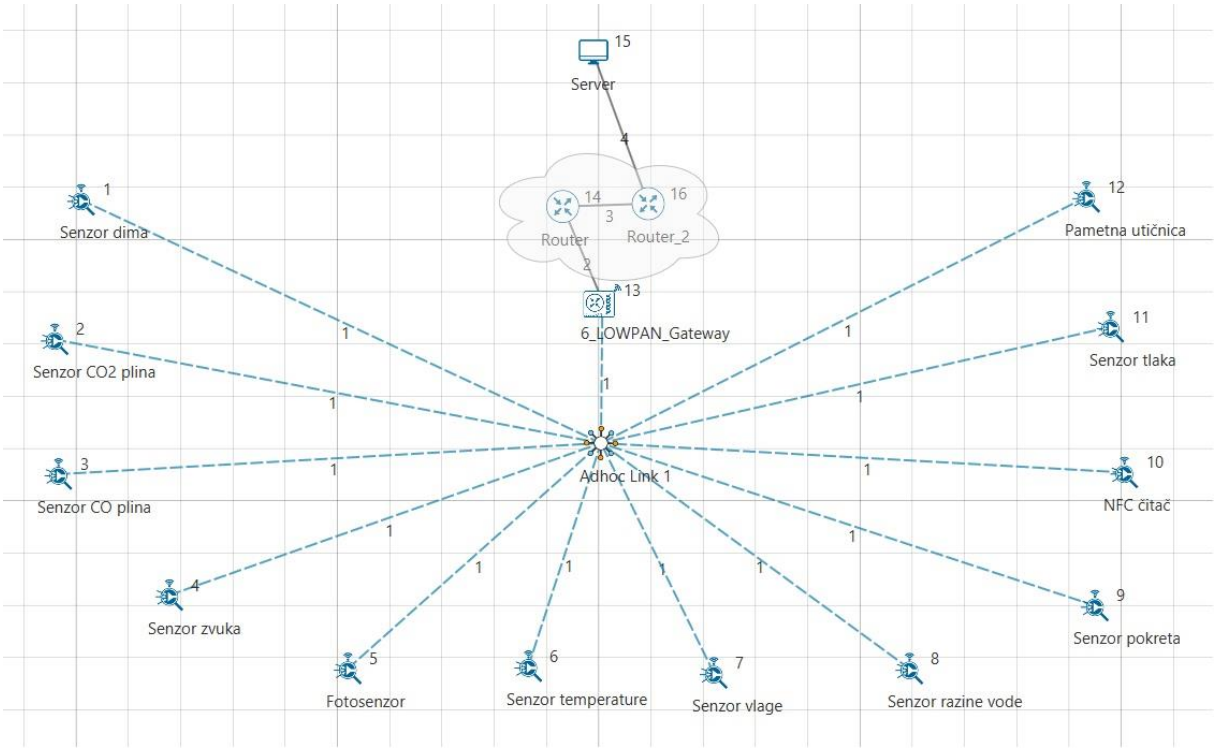
Slika 6. Mrežna topologija okruženja pametnog doma

Na početnom zaslonu koji je prikazan na slici 5. odabire se željena vrsta mreže za simulaciju (u ovom slučaju IoT). Nakon tih odrađenih radnji otvara se prozor gdje se nalazi koordinatna mreža i komponente koje se mogu postaviti u tu mrežu kao što je prikazano na slici 7.



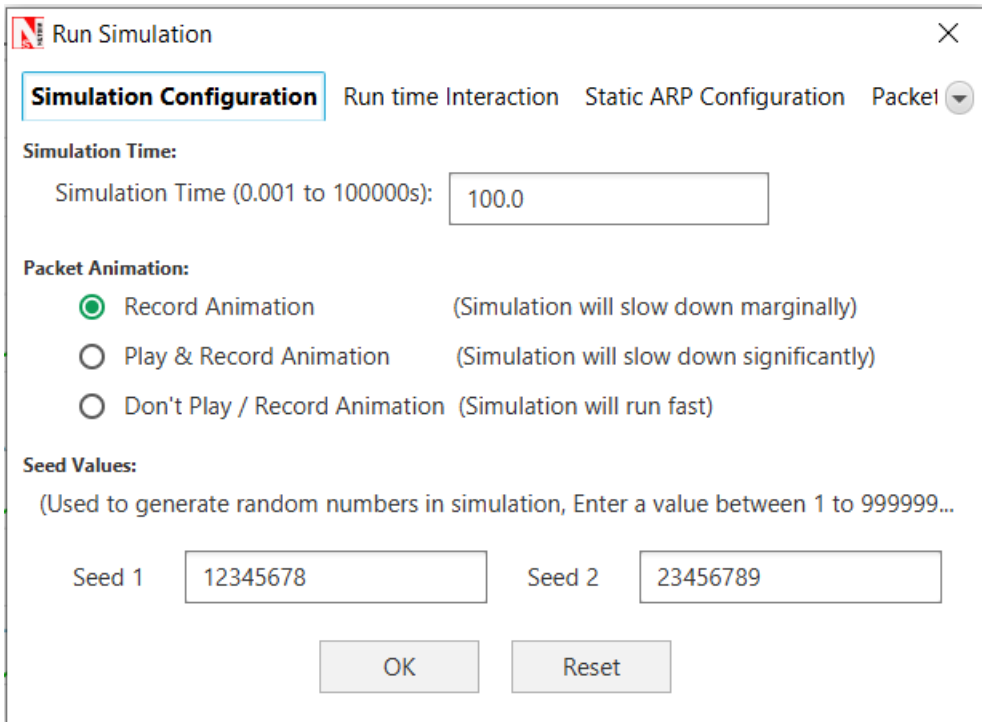
Slika 7. Prikaz zaslona za postavljanje komponenti i simulaciju

Na slici 8. se može vidjeti mrežna topologija pametnog doma koja je izrađena u NetSim alatu i nad kojom će se u istom alatu izvoditi i simulacija. NetSim korisniku pruža mogućnost reprodukcije i snimanja animacija. Paketna animacija omogućuje korisnicima promatranje toka prometa kroz mrežu za dubinsku vizualizaciju i analizu. NetSim također omogućuje korisnicima praćenje datoteka koje pružaju detaljne informacije o paketima korisne za provjeru valjanosti performansi, statističku analizu i otklanjanje pogrešaka prilagođenog koda. Praćenje paketa bilježi skup odabranih parametara za svaki paket dok prolazi kroz mrežu, kao što je vrijeme dolaska, vrijeme čekanja, vrijeme odlaska, nosivost, opterećenje, pogreške, kolizije i slično. Alat NetSim omogućuje korisniku i praćenje događaja koje bilježi svaki pojedinačni događaj zajedno s povezanim informacijama (kao što su vremenska oznaka, ID događaja, vrsta događaja) u tekstualnu datoteku ili .csv datoteku koja se može pohraniti na korisnički definiranu lokaciju. U NetSim-u, IoT je modeliran kao WSN (engl. *Wireless Sensor Network*) koji se povezuje na internet preko 6LoWPAN pristupnika. WSN za IoT koristi sljedeće protokole: AODV (engl. *Ad hoc On-Demand Distance Vector*) s IPv6 adresiranjem na mrežnom sloju i 802.15.4 na MAC & PHY slojevima. WSN šalje podatke na LoWPAN pristupnik koji koristi Zigbee (802.15.4) sučelje i WAN (engl. *Wide Area Network*) sučelje. Zigbee sučelje povezuje se bežično na WSN, a WAN sučelje povezuje se na Internet.



Slika 8. Topologija okruženja pametnog doma u alatu NetSim

Nakon postavljanja mrežnog scenarija pokreće se simulacija. Nakon pokretanja simulacije potrebno je u zasebnom prozoru definirati hiperparamtere simulacije,poput vremena trajanja simulacije. Vrijeme simulacije stvorenog mrežnog scenarija sa slike 8. postavljeno je na 100 sekundi, što se može vidjeti na slici 9. Nakon završetka simulacije pojavljuju se rezultati iste koji će biti pojašnjeni u sljedećem poglavlju.



Slika 9. Skočni prozor za postavljanje vremena trajanja simulacije

Napad uskraćivanjem usluge (DoS) je pokušaj da se sustav učini nedostupnim željenom korisniku, kao što je sprječavanje pristupa web stranici. Uspješan DoS napad troši svu dostupnu mrežu ili resurse sustava, što obično dovodi do usporavanja ili pada poslužitelja. Kad je više zaraženih izvora u DoS napadu, postaje poznat kao DDoS napad. Standardne vrste DDoS napada su:

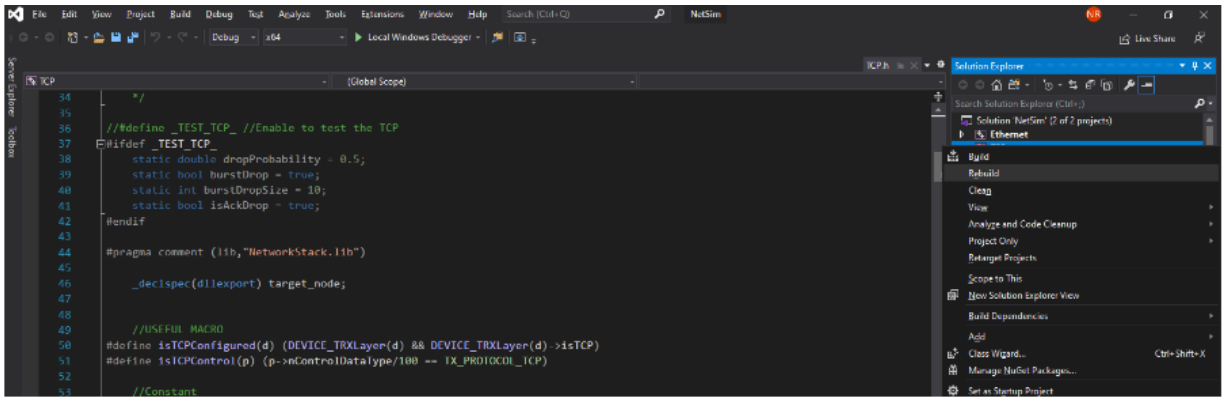
- SYN Flood,
- UDP Flood,
- SMBLoris,
- ICMP Flood i
- HTTP GET Flood.

TCP SYN poplave su DoS napadi koji pokušavaju poplaviti DNS poslužitelj novim zahtjevima za TCP vezu. Obično klijent inicira TCP vezu putem *Three Way Handshake* poruka:

- Klijent zahtijeva vezu slanjem SYN poruke poslužitelju.
- Poslužitelj potvrđuje zahtjev slanjem SYN-ACK natrag klijentu.
- Klijent odgovara odgovorom ACK, uspostavljajući vezu.

Ova trostruka razmjena je temelj za svaku vezu uspostavljenu korištenjem TCP protokola. SYN Flood jedan je od najčešćih oblika DDoS napada. Događa se kada napadač pošalje niz zahtjeva za TCP sinkronizaciju (SYN) meti u pokušaju da potroši dovoljno resursa da poslužitelj učini nedostupnim za legitimne korisnike. Ovo funkcionira jer SYN zahtjev otvara mrežnu komunikaciju između budućeg klijenta i ciljnog poslužitelja. Kada poslužitelj primi SYN zahtjev, odgovara potvrđujući zahtjev i drži komunikaciju otvorenom dok čeka da klijent potvrdi otvorenu vezu. Međutim, u uspješnom SYN Floodu, potvrda klijenta nikad ne stigne, trošeći tako resurse poslužitelja dok veza ne istekne. Velik broj dolaznih SYN zahtjeva ciljnom poslužitelju iscrpljuje sve dostupne resurse poslužitelja i rezultira uspješnim DoS napadom.

Kako bi se simulirao SYN Flood napad u NetSim alatu potrebno je poduzeti neke korake prije same simulacije. Prvo je potrebno otvoriti izvorni kod u alatu Visual Studio tako da se na početnom zaslonu odabire opcija *Your work*. Drugi korak je da se u Visual Studiu unutar TCP projekta u pregledniku rješenja dodaje datoteka SYN_FLOOD.c u sklopu tog projekta. Nakon uspješne izmjene, modificirana datoteka *libTCP.dll* i *libEthernet.dll* automatski se ažurira u direktoriju koji sadrži NetSim binarne datoteke.



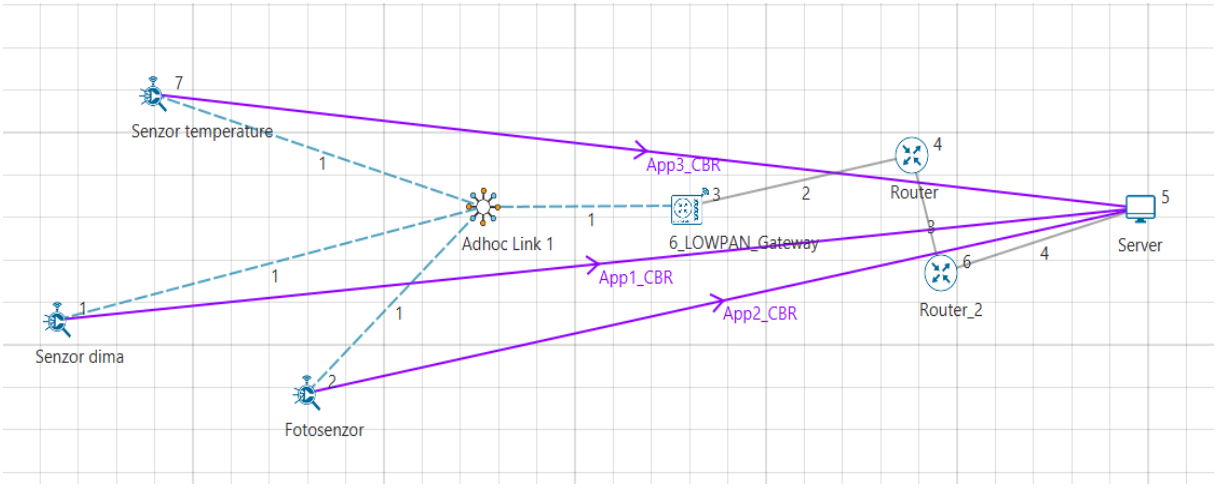
Slika 10. Prikaz NetSim izvornog koda u alatu Visual Studio

5.2.1. Simulacija SYN Flood napada

U simulaciji SYN Flood napada izdvojit ćemo jedan dio stvorene mreže, a koji će nam biti dovoljan kako bi mogli vidjeti koji učinak ima na mrežu, a sastoji se od tri senzora, LoWPAN pristupnika, rutera i poslužitelja. U simulaciji se koriste tri scenarija koja se kasnije uspoređuju i analiziraju. Prvi scenarij je simulacija mreže bez zaraženog senzora u mreži koji se može vidjeti na slici 11. Također je potrebno prije same simulacije u Visual Studiu u datoteci TCP.h i u datoteci SYN_FLOOD.c postaviti nekoliko parametara potrebnih za provođenje simulacije, a ti parametri su vidljivi u tablici 2. za sva tri provedena scenarija. Nakon uspješnog postavljanja i izmjene potrebnih parametara, modificirana datoteka *libTCP.dll* i *libEthernet.dll* automatski se ažurira u direktoriju koji sadrži NetSim binarne datoteke. Vrijeme simulacije za sva tri scenarija postavljeno je na 100 sekundi.

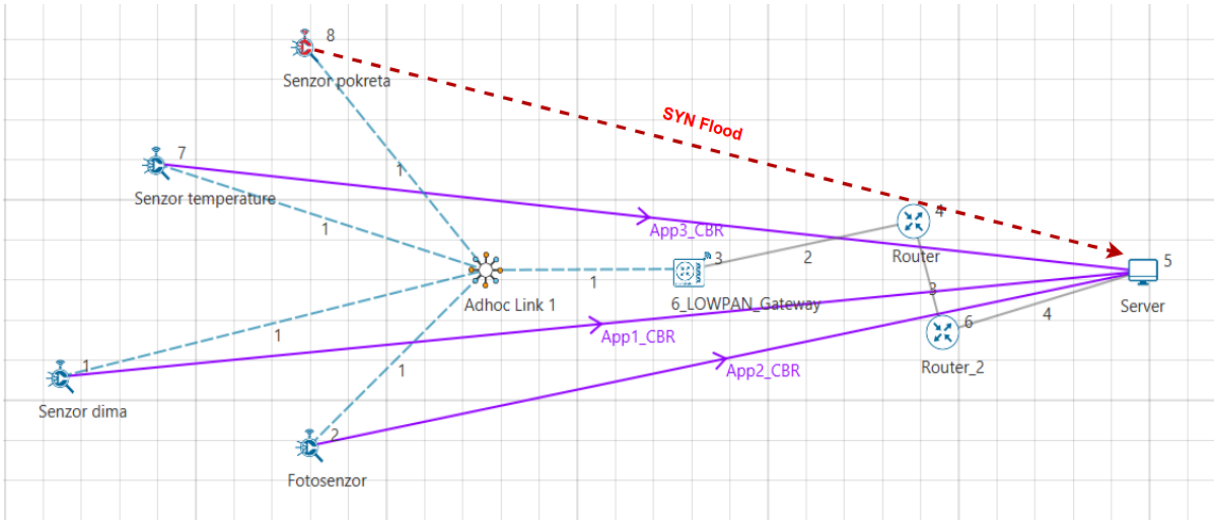
Tablica 2. Vrijednosti potrebnih parametara za provođenje simulacije SYN Flood napada

	Datoteka TCP.h		
Parametar	Scenarij 1	Scenarij 2	Scenarij 3
NUMBEROFMALICIOUSNODE	0	1	2
	Datoteka SYN_FLOOD.c		
Parametar	Scenarij 1	Scenarij 2	Scenarij 3
malicious node	0	Senzor 8 (senzor pokreta)	Senzor 8 (senzor pokreta) i senzor 9 (senzor zvuka)



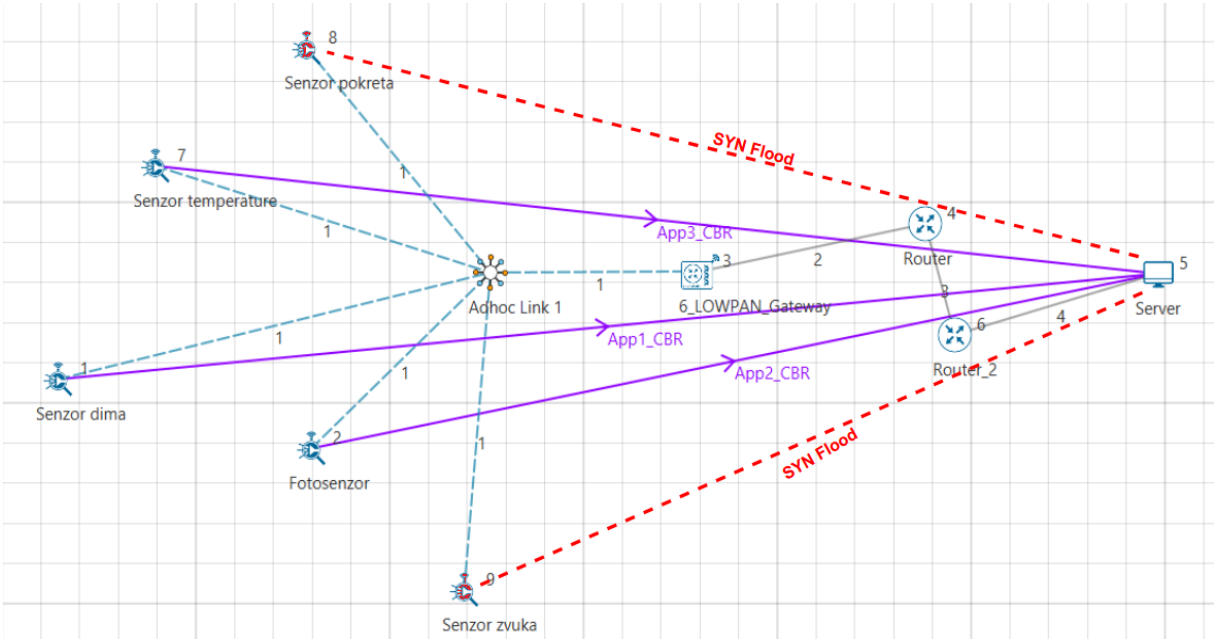
Slika 11. Prvi scenarij koji prikazuje mrežu bez zaraženog senzora

Drugi scenarij je umetanje jednog zaraženog senzora u mrežu koji je prikazan na slici 12.



Slika 12. Drugi scenarij koji prikazuje mrežu sa jednim zaraženim senzorom

U trećem scenariju se nalaze dva zaražena senzora u mreži koji je prikazan na slici 13. Nakon provedenih scenarija putem simulacije u NetSim alatu u sljedećem poglavlju je provedena analiza u kojoj je moguće vidjeti na koji način umetanje jednog ili dva zaražena senzora u mrežu utječe na propusnost u odnosu na propusnost u mreži u kojoj se ne nalazi niti jedan zaraženi senzor.



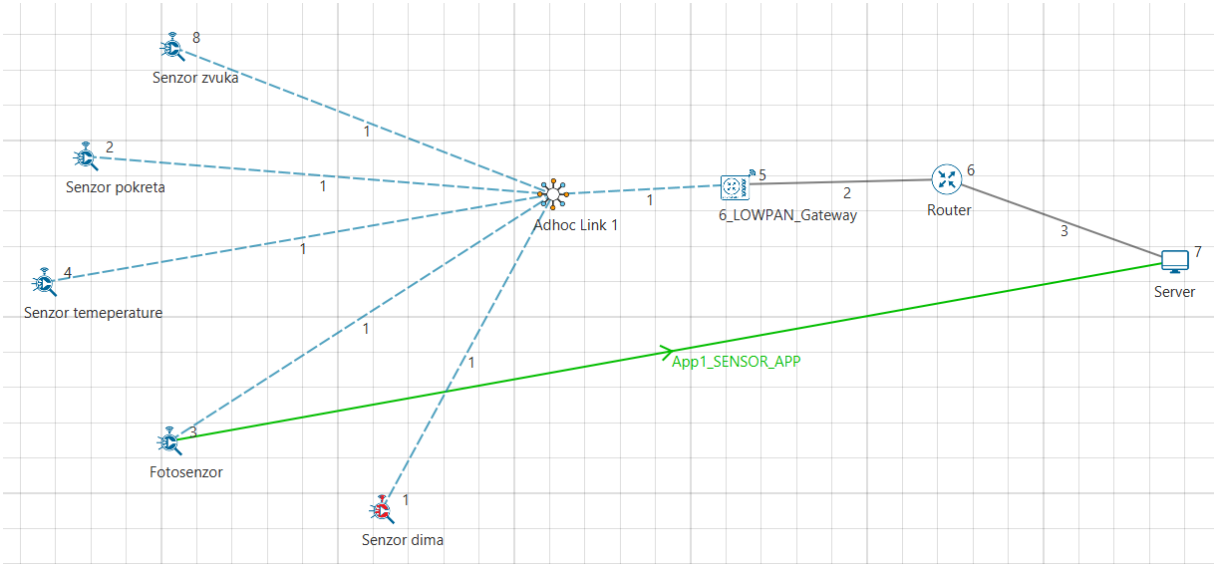
Slika 13. Treći scenarij koji prikazuje mrežu sa dva zaražena senzora

5.2.2. Simulacija *Sink Hole* napada

U *Sink Hole* napadu, kompromitirani čvor ili zlonamjerni čvor reklamira lažne informacije o rangu kako bi formirao lažne rute. Nakon što primi paket poruke, odbacuje informacije o paketu. *Sink Hole* napadi utječu na performanse IoT mrežnih protokola kao što je RPL (engl. *Routing Protocol for Low-Power and Lossy Networks*) protokol. Može se postaviti bilo koji uređaj kao zlonamjeran i moguće je imati više od jednog zlonamjernog čvora u scenariju. ID-ovi uređaja zlonamjernih čvorova mogu se postaviti unutar funkcije fn_NetSim_RPL_MaliciousNode(). Da bi se mogla izvršiti simulacija *Sink Hole* napada potrebno je u Visual Studiu u izvorni kod NetSim alata dodati datoteku *Malicious.c* u RPL projekt. Ta datoteka sadrži sljedeće funkcije:

- fn_NetSim_RPL_MaliciousNode(); - ova funkcija se koristi za utvrđivanje da li je trenutni uređaj zlonamjeran ili nije kako bi se moglo uspostaviti zlonamjerno ponašanje.
- fn_NetSim_RPL_MaliciousRank(); - ova se funkcija koristi za davanje lažnog ranga zlonamjernom čvoru.
- rpl_drop_msg(); - ova se funkcija koristi za ispuštanje paketa od strane zlonamjernog čvora ako uđe u mrežni sloj.

Scenarij mreže koji će se koristiti u simulaciji prikazan je na slici 14., a mreža se sastoji od pet senzora, jednog 6LoWPAN pristupnika, rutera i poslužitelja.



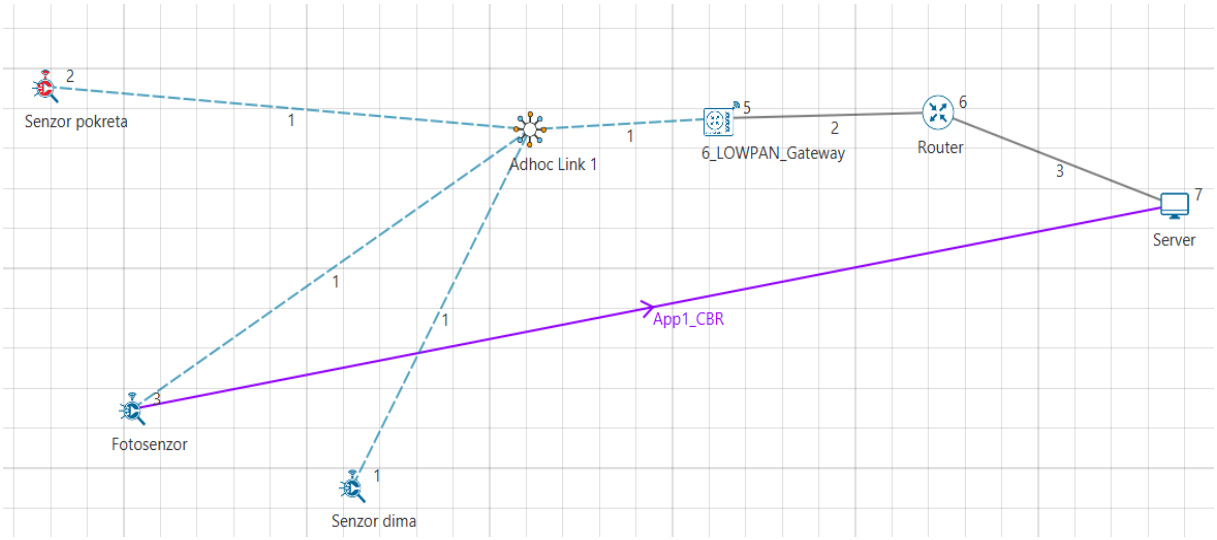
Slika 14. Prikaz scenarija koji se koristi u simulaciji Sink Hole napada

5.2.3. Simulacija DIS Flood napada

RPL je protokol za usmjeravanje za IPv6-bazirane LoWPAN mreže. U RPL protokolu, DIS (engl. *DODAG Information Solicitation*) poruke šalje čvor za pridruživanje mreži. Zlonamjerni čvor može iskoristiti ovaj mehanizam za slanje nelegitimnih DIS poruka susjednim čvorovima za izvođenje DIS Flood napada. Čvor šalje DIS poruku svojim susjednim čvorovima kako bi zatražio informacije o usmjeravanju kako bi se mogao pridružiti postojećem DODAG-u (engl. *Destination Oriented Directed Acyclic Graph*). Dakle, novi čvor kontinuirano odašilje DIS poruke s fiksnim intervalom dok ne primi DIO (engl. *DODAG Information Object*) poruku od bilo kojeg susjednog čvora. Jednom kada čvor primi DIO poruku, prestaje slati DIS poruke i pridružuje se mreži slanjem DAO (engl. *DODAG Advertisement Object*) zatraženom čvoru. Zlonamjerni čvor može iskoristiti ovu značajku za degradaciju performansi mreže odabirom različitih DIS intervala prijenosa za povremeno slanje DIS poruka svojim susjednim čvorovima (DIS Flood napad). To dovodi do povećanja potrošnje kontrolnog paketa mreže i potrošnje energije.

Da bi se mogla izvršiti simulacija DIS Flood napada potrebno je u Visual Studiu u izvorni kod NetSim alata dodati datoteku *Malicious.c* u RPL projekt, kao što je to bilo i u slučaju *Sink Hole* napada. Datoteka *Malicious.c* također sadrži iste dvije funkcije koje sadrži i *Malicious.c* datoteka u *Sink Hole* napadu: fn_NetSim_RPL_MaliciousNode() i rpl_drop_msg(). Za potrebe simulacije potrebno je

također i stvoriti scenarij u kojem se kao prijenosni protokol označava UDP (engl. *User Datagram Protocol*). Scenarij koji će se koristiti u simulaciji prikazan je na slici 15. Vrijeme trajanja simulacije podešava se na 100 sekundi.



Slika 15. Prikaz scenarija koji se koristi u simulaciji DIS Flood napada

6. Analiza rezultata istraživanja i prijedlozi unaprjeđenja

Kao što je već u prethodnim poglavljima spomenuto NetSim alat omogućava simulaciju stvorene mreže i prikaz rezultata te simulacije. IoT mreža koja se simulirala pomoću NetSim alata prikazana je na slici 8., a nakon provedene simulacije moguće je vidjeti performanse mreže kao što je propusnost, kašnjenje, *jitter*, itd. Također su nakon simulacije rezultati vidljivi u tablicama, odnosno metrikama, te se može vidjeti IP metrika, metrika korisničke aplikacije u kojoj su prikazane performanse kao što je propusnost, kašnjenje, i sl., metrika veza između komponenata, itd.

6.1. Analiza rezultata istraživanja

U *Link* metrici, prikazanoj slikom 16., vidljive su vrijednosti metrike koje se odnose na svaku vezu u mreži. Pomoću nje je moguće vidjeti ukupan broj paketa prenesenih u svakoj vezi u simuliranoj mreži, ukupan broj pogrešaka u prijenosu paketa, ukupan broj paketa koji su se sudarili u vezi (uključujući podatkovne i kontrolne pakete).

Link_Metrics_Table

Link_Metrics

Link ID	*Link Throughput Plot*	Packets Trans...		Packets Errored		Packets Collided	
		Data	Control	Data	Control	Data	Control
All	NA	1719	9720	0	0	54	4343
1	Link_throughput	522	9650	0	0	54	4343
2	Link_throughput	399	35	0	0	0	0
3	Link_throughput	399	35	0	0	0	0
4	Link_throughput	399	0	0	0	0	0

Slika 16. Prikaz vrijednosti Link metrike

U metrici aplikacije, koja je prikazana slikom 17., se prikazuje ID aplikacije, njezino ime, ID izvora koji pokreće te određene aplikacije, ID odredišta, ukupan broj paketa generiranih od izvora, ukupan broj generiranih i poslanih paketa od strane izvora, ukupan broj paketa primljenih na odredištu, ukupan korisni teret prenesen u bajtovima, ukupni korisni teret primljen na odredištu u bajtovima, propusnost, *jitter* i

kašnjenje, odnosno prosječno vrijeme koje je potrebno da svi paketi dođu do odredišta od trenutka kada je paket poslan iz izvorišta.

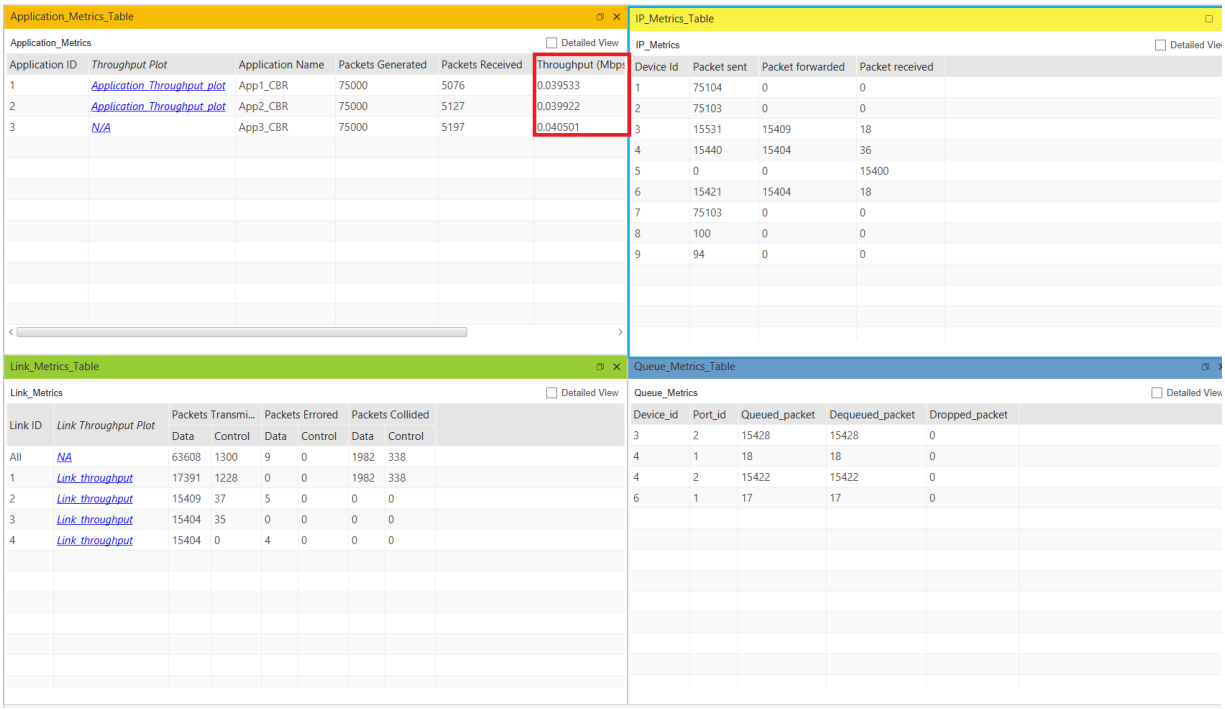
Application_Metrics_Table

Application_Metrics

Application ID	*Throughput Plot*	Application Name	Packets Generated	Packets Received	Throughput (Mbps)	Delay (microsec)	Jitter (microsec)
1	*Application Throughput plot*	App1_SENSOR_APP	100	68	0.000272	21322.858824	12227.238806
2	*Application Throughput plot*	App2_SENSOR_APP	100	66	0.000264	40651.996970	26626.000000
3	*Application Throughput plot*	App3_SENSOR_APP	100	80	0.000320	24126.300000	13515.177215
4	*Application Throughput plot*	App4_SENSOR_APP	100	56	0.000224	23364.800000	11543.654545
5	*Application Throughput plot*	App5_SENSOR_APP	100	65	0.000260	37868.292308	13017.625000
6	*Application Throughput plot*	App6_SENSOR_APP	100	64	0.000256	22688.768750	10032.174603

Slika 17. Prikaz vrijednosti metrice aplikacija

U promatranom slučaju kod simulacije SYN Flood napada promatra se propusnost koja je označena na slici 18., a koja se nalazi u metrici aplikacije.



Slika 18. Prikaz rezultata simulacije u mreži bez zaraženog senzora

Zbog toga što se u prethodnom poglavlju provela simulacija tri scenarija u koja su se dodavali zaraženi senzori provodi se analiza i učinak tih scenarija na propusnost. U tablici 3. se nalaze vrijednosti propusnosti koju vide korisničke aplikacije. Prvi red predstavlja propusnost kada nema napada. U drugom redu se može vidjeti propusnost u mreži u kojoj se nalazi jedan zaraženi senzor, a zadnji redak predstavlja propusnost kada se u mreži nalaze dva zaražena senzora. Slučaj 1 pokazuje rezultate kada nema napada. Tri korisničke aplikacije postižu propusnost od oko 0,04 Mbps. U tablici se može vidjeti da propusnost za ove tri aplikacije pada kako se povećava broj zaraženih

senzora. To je zato što se resursi poslužitelja troše u rukovanju SYN-FLOOD paketima i poslužitelj ne može održati prijenos paketa za redovne aplikacije. U ovom primjeru, s koordiniranim napadom propusnost je manja za čak 30%.

Tablica 3. Propusnost koju vide korisničke aplikacije

	Propusnost_APP1 (Mbps)	Propusnost_APP2 (Mbps)	Propusnost_APP3 (Mbps)
Slučaj 1 – Zlonamjerni senzor = 0	0.039533	0.039922	0.040501
Slučaj 2 – Zlonamjerni senzor = 1	0.033603	0.033934	0.034426
Slučaj 3 – Zlonamjerni senzor = 2	0.027743	0.027945	0.028351

U provedenoj simulaciji u kojoj se simulirao *Sink Hole* napad putem NetSim alata moguće je vidjeti da paket šalje čvor 3 (fotosenzor), a prima ga čvor 1 (senzor dima), to je zbog toga što zlonamjerni čvor 1 privlači mrežni promet oglašavanjem lažnih informacija o rangu tako da preuzima rang 6LoWPAN pristupnika. Budući da je čvor 1 (senzor dima) zlonamjerni čvor, on ispušta paket i zbog toga je propusnost u ovom scenariju jednaka nuli kao što je prikazano na slici 19. Nakon provedene simulacije potrebno je provjeriti također i protok paketa putem opcije “Praćenje paketa” gdje se promatra stupac *Transmitter_Id* i *Receiver_Id*. Budući da je čvor 1 (senzor dima) zlonamjerni čvor, on ispušta paket bez daljnjeg prosljeđivanja što je također vidljivo na slici 20.

Application_Metrics_Table

Application_Metrics

Application ID	Application Name	Packets Generated	Packets Received	Throughput (Mbps)	Delay (microsec)	Jitter (microsec)
1	App1_SENSOR_APP	100	0	0.000000	0.000000	0.000000

Slika 19. Propusnost kod simulacije Sink Hole napada

1	PACKET_ID	SEGMENT_ID	PACKET_TYPE	CONTROL_PACKET_TYPE/APP_NAME	SOURCE_ID	DESTINATION_ID	TRANSMITTER_ID	RECEIVER_ID
129	2	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
153	3	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
165	4	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
185	5	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
196	6	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
204	7	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
220	8	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
239	9	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
247	10	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
263	11	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
276	12	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
284	13	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
296	14	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
304	15	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
323	16	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
338	17	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
346	18	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
354	19	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
362	20	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7
373	21	0	Sensing	App1_SENSOR_APP	SENSOR-8	NODE-3	SENSOR-8	SENSOR-7

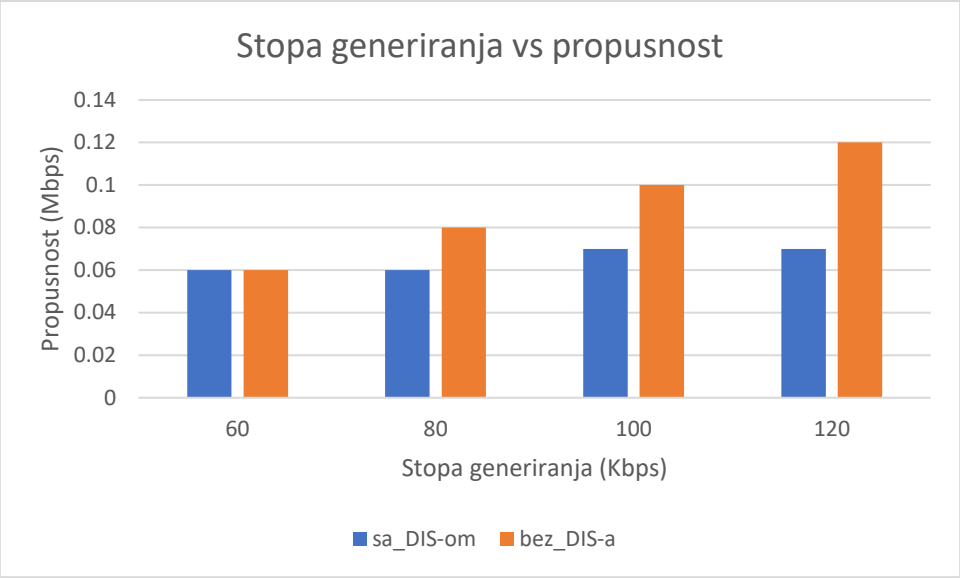
Slika 20. Opcija praćenja paketa u alatu NetSim

Treća simulacija koja je provedena je simulacija DIS Flood napada. U scenariju 1 se uspoređuje propusnost aplikacije u odnosu na stopu generiranja aplikacije. Postavlja se DIS interval na 10 milisekundi i mijenja se stopa generiranja aplikacija kako bi se vidio utjecaj preplavljivanja DIS-a na izvedbu mreže. U tablici 4. se može vidjeti usporedba propusnosti i kašnjenja sa i bez DIS Flood-a.

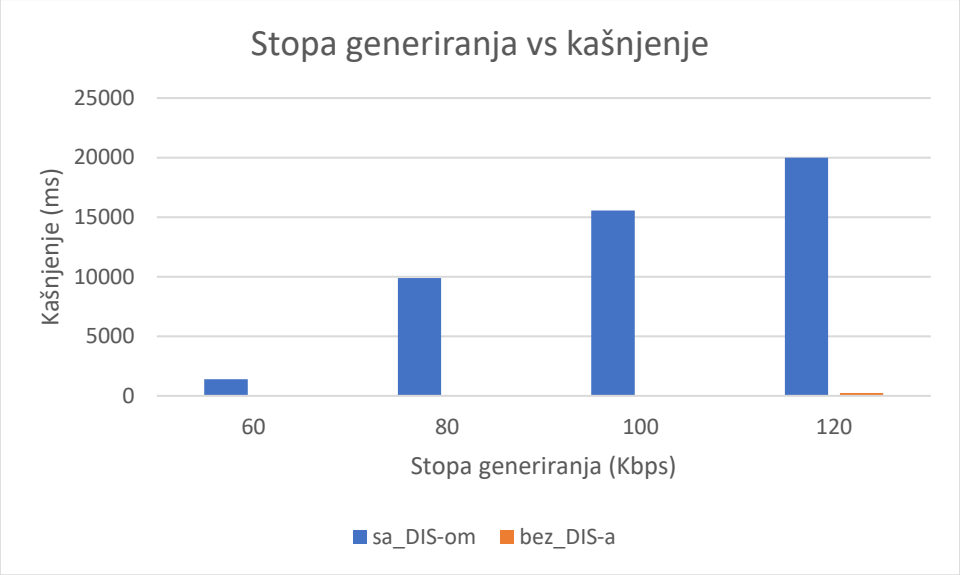
Tablica 4. Usporedba propusnosti i kašnjenja sa i bez DIS Flood-a

	Propusnost (Mbps)		Kašnjenje (ms)	
Stopa generiranja (Kbps)	sa_DIS-om	bez_DIS-a	sa_DIS-om	bez_DIS-a
60	0.06	0.06	1394.49	51.80
80	0.06	0.08	9896.58	51.75
100	0.07	0.10	15553.54	51.76
120	0.07	0.12	19988.49	239.62

Može se primijetiti da se propusnost aplikacije smanjuje u slučaju preplavljivanja DIS-a u usporedbi s uobičajenim simulacijama za različite stope generiranja prometa aplikacije. Kašnjenje je relativno visoko u slučaju plavljenja DIS-a i povećava se s povećanjem stope proizvodnje. To je zato što su čvorovi često zauzeti primanjem i odgovaranjem na DIS poruke od zlonamjernog čvora. Čvorovi koji primaju DIS poruke prisiljeni su poništiti svoje mjerače vremena i preplaviti mrežu DIO porukama. Ovo se dalje može razumjeti uz pomoć sljedećih dijagrama koji su prikazani na slici 21. i na slici 22.



Slika 21. Usporedba stope generiranja u odnosu na propusnost



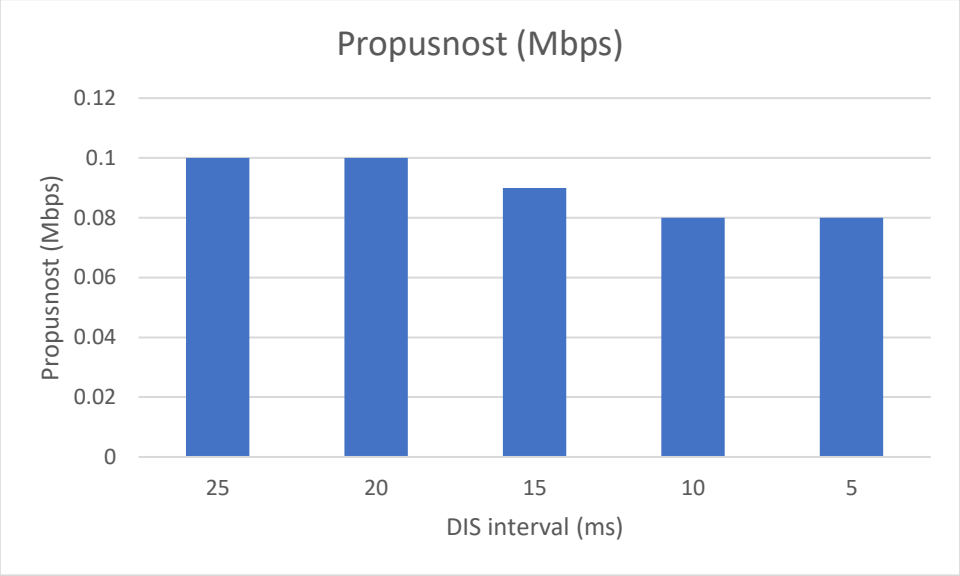
Slika 22. Usporedba stope generiranja u odnosu na kašnjenje

U scenariju 2 se uspoređuje propusnost aplikacije u odnosu na vrijeme DIS intervala. Brzina generiranja aplikacije se postavlja na 250 Kbps i mijenja se DIS interval kako bi se vidio utjecaj preplavljivanja DIS-a na performanse mreže. U tablici 5. se može vidjeti različiti DIS interval u odnosu na propusnost.

Tablica 5. Različiti DIS interval (ms) u odnosu na propusnost (Mbps)

DIS Interval (ms)	Propusnost (Mbps)
25	0.10
20	0.10
15	0.09
10	0.08
5	0.08

Može se uočiti da se propusnost aplikacije smanjuje kako se smanjuje vrijeme DIS intervala. Nakon smanjenja DIS intervala, maliciozni će čvorovi češće slati više DIS poruka. Legitimni senzori troše više vremena na obradu i odgovaranje na DIS poruke nego na slanje paketa podataka. Preplavljivanje DIS-a ozbiljno degradira performanse mreža male snage i gubitaka zbog povećanja opterećenja kontrolnih paketa. Ovo se dalje može razumjeti uz pomoć sljedećeg dijagrama koji je prikazan na slici 23.



Slika 23. Usporedba DIS intervala u odnosu na propusnost

6.2. Prijedlozi unaprjeđenja

Prvi korak u osiguranju umreženog sustava je otkrivanje napada, čak i ako ga nije u mogućnosti spriječiti, tako da se otkrivanje upada može smatrati prvom linijom obrane u svakom sigurnosnom sustavu. IDS sustavi (engl. *Intrusion Detection Systems*) su sigurnosni alati čiji je cilj obrana sustava, izvođenje protumjera ili

generiranje upozorenja za entitet koji je sposoban izvršiti odgovarajuće radnje, kada dođe do napada. Ovisno o vrsti provedene analize, IDS se može klasificirati u detekciju anomalija ili detekciju potpisa. U otkrivanju anomalija, IDS definira zadano ponašanje i signalizira sva abnormalna ponašanja. U detekciji potpisa, IDS uspoređuje nadzirane radnje s potpisima prethodno definiranim u sustavu. Detekcija temeljena na potpisima obično je učinkovita samo u poznatim napadima, nasuprot tome, detekcija temeljena na anomalijama ima potencijal otkriti nametljive događaje koji prije nisu viđeni, [35].

Nakon identifikacije upada, IDS se može ponašati pasivno, gdje se o otkrivenom događaju obavještava odgovorni korisnik, putem konzola s porukama, e-pošte, izvješća, itd. Osim toga, IDS može aktivno djelovati poduzimanjem proaktivnih i korektivnih radnji na identificiran kritični događaj, ispravljanje ranjivosti sustava, rekonfiguracija vatrozida, itd. IPS (engl. *Intrusion Prevention Systems*) ima iste mogućnosti kao IDS, gdje je sposoban detektirati napade u stvarnom vremenu. Za prepoznavanje SYN Flood napada, pomoću razvijenog softvera za analizu paketa registrira se izvorna IP adresa u privremenoj tablici i vrši se praćenje broja SYN paketa primljenih preko IP-a. IP je u toj tablici dok se na pakete ne odgovori s ACK. Softver je konfiguriran kao maksimalno ograničenje paketa po vremenskom intervalu koji se smatra napadom. Stoga će napadač biti blokiran ako dosegne nametnutu granicu poslanih SYN paketa. IP adrese napadača blokirane su u vatrozidu sustava i pohranjene u tablici koja sadrži blokirane IP adrese, koja se naziva crna lista. Privremena tablica se briše svaki put kada završi korisnički definirani vremenski interval, jer je time moguće blokirati IP-ove koji pokušavaju poslati veliki broj SYN paketa u malom vremenskom intervalu, signalizirajući napad, [35].

Statistički pristup je također pouzdana metoda otkrivanja *Sink Hole* napada tako da se proučavaju i bilježe podatci povezani s određenim aktivnostima čvorova u mreži, što može biti nadgledanje uobičajenog paketa koji se prenosi između čvorova ili nadziranje iscrpljenosti resursa čvorova poput upotrebe procesora. Kompromitirani čvor otkriva se usporedbom stvarnog ponašanja s vrijednošću koja se koristi kao referenca, ako bilo koji čvor premaši tu vrijednost smatra se uljezom. SOS (engl. *Secure Overlay Service*) još je jedna preventivna tehnika protiv napada u IoT mreži. Korištenjem ove usluge preklapanja, tajni čvor komunicira s drugim nasumičnim čvorom na način da se identitet tajnog čvora ne može provjeriti, ali ga prethodno ovlašteni izvori mogu znati i pristupiti mu. Ovaj proces uključuje dvije neovisne provjere

autentičnosti. Prvo, uspješna autentikacija omogućuje prijenos prometa na neki poslužitelj koji se naziva tajnim, a drugo, poslužitelj ponovno autentificira i prosljeđuje samo valjani promet rubnim usmjerivačima mreže, [36].

Nekoliko najboljih jednostavnih praksi također uvijek može pomoći u zaštiti pametnog doma, odnosno cijele mreže i njezinih komponenata u mreži. Prilikom postavljanja novog IoT uređaja, dobra je ideja onemogućiti pristup i značajke povezivanja koje nisu potrebne. Postoji niz značajki povezivanja koje mogu biti korisne u nekim okolnostima, ali mogu biti rizik u drugima. Osim toga, uređaji se obično isporučuju s minimalnim sigurnosnim značajkama i slabim zadanim lozinkama i zbog toga je preporučljivo odmah promijeniti lozinku. Korištenje višefaktorske autentikacije također je jednostavno za korištenje, ali iznimno sigurno. Prilikom prijave može se od korisnika tražiti potvrda identiteta pomoću sigurnog jednokratnog koda koji se šalje na potvrđeni telefonski broj ili adresu e-pošte. Ovi su kodovi nasumični, praktički ih je nemoguće pogoditi i istječu nakon određenog vremena. Jedna od praksi je također i korištenje jake Wi-Fi enkripcije te je također važno softver održavati ažuriranim jer napadači mogu iskoristiti zastarjele operativne sustave, koji imaju slabe ili zastarjele sigurnosne značajke.

7. Zaključak

Iako su kućna automatizacija i tehnologija interneta stvari prisutni već neko vrijeme, mnoga rješenja su u testnom režimu i uvijek postoji ogroman prostor za poboljšanje. Jedan od izazova automatizacije pametnog doma o kojem se najviše raspravlja je problem unakrsne kompatibilnosti – sposobnost međusobnog komuniciranja i rada pametnih uređaja te sigurno dijeljenje podataka. To je glavna prepreka uspješnoj kućnoj automatizaciji. Ako se ne dobije takva komunikacija pametnih uređaja, npr. zbog razlike u protokolima povezivanja ili zaključavanja platforme, neće se moći konfigurirati željeni skup ovisnosti i radnji. Pametni uređaji se ugrađuju u domove velikom brzinom. Imajući sve ove međusobno povezane i internet povezane uređaje, unose se ranjivosti u mrežu. Korisnici takvih uređaja moraju biti spremni na to s kojim se uređajima mogu susresti, ranjivosti koje postoje ili prijete IoT uređajima, te održivim metodama istraživanja ovih IoT uređaja i potencijalnim podacima koji se mogu prikupiti upotrebom tih pametnih uređaja.

U radu je prikazana simulacija okruženja pametnog doma i nekih od mogućih prijetnji pomoću NetSim alata. Alat je odabran zbog toga što je jednostavan za korištenje i što ga zbog toga može koristiti svatko. Alat omogućuje prikaz performansa mreže (propusnost, kašnjenje, *jitter*, i slično), kroz tablice gdje se lako mogu rezultati kasnije usporediti i analizirati. Peto poglavlje se prvim dijelom odnosi na provođenje simulacije okruženja pametnog doma, te se objašnjava koji su postupci potrebni kako bi alat mogao simulaciju provesti do kraja. Drugi dio simulacije se odnosi na simulaciju mogućih napada u mreži, te koje je sve korake potrebno poduzeti kako bi simulacija bila valjana i provedena od početka do kraja. U šestom poglavlju je moguće vidjeti sve rezultate provedenih simulacija, od samih metrika u kojemu su prikazane vrijednosti i performanse mreže bez zlonamjernih senzora, pa do metrika, tablica i dijagrama u kojima se vrši analiza posljedica mreže u kojoj se nalazi jedan ili više zlonamjernih senzora. Te su na kraju još predložene neke od metoda i tehnika s kojima je moguće poboljšati mrežu i zaštititi je od zlonamjernih napada.

Korisnici prije implementacije senzora, pametnih uređaja ili nekih drugih komponenti u svoj dom uvijek moraju biti svjesni da ranjivosti postoje. Prva linija obrane je najvažnija i zbog toga je potrebno prilikom postavljanja novih uređaja onemogućiti pristup i značajke koje nisu potrebne, te promijeniti slabe zadane lozinke

kako bi se napadaču onemogućio lak ulazak u mrežu. Također je potrebno koristiti i višestruku autentikaciju koja omogućava slanje jednokratnog koda korisniku za potvrdu identiteta i time onemogućiti napad te je potrebno ažurirati softver jer u zastarjelim softverima napadač može iskoristiti te slabe i zastarjele sigurnosne značajke i time ugroziti uređaj, mrežu te samog korisnika. Odgovornost također leži i na pružateljima IoT aplikacija koji bi trebali osigurati implementaciju koncepata zaštite podataka i sigurnosti. Kako bi to potvrdile, tvrtke koje koriste IoT aplikacije moraju provesti procjenu učinka zaštite podataka i osigurati da senzori ne prikupljaju više podataka nego što je apsolutno potrebno za ispunjavanje relevantne komercijalne svrhe.

Literatura

[1] "*20 Surprising IoT Statistics You Don't Already Know*", Dostupno na: https://securityboulevard.com/2019/09/20-surprising-iot-statistics-you-dont-already-know/ (Zadnje pristupano: 28.6.2022.)

[2] "*Croatia Industry 4.0 Opportunities*", Dostupno na: https://hamagbicro.hr/wp-content/uploads/2019/12/CROATIA-INDUSTRY-4.0_WEB.pdf, 2019. (Zadnje pristupano: 30.6.2022.)

[3] "IoTnet, SigFox operator", Dostupno na: https://www.iotnet.hr/novosti.aspx (Zadnje pristupano: 30.6.2022)

[4] Hall F., Maglaras L., Aivaliotis T., Xagoraris L., Kantzavelou I.: *Smart Homes: Security Challenges and Privacy Concerns*, 2020., Dostupno na: https://www.researchgate.net/publication/344971583_Smart_Homes_Security_Challenges_and_Privacy_Concerns (Zadnje pristupano: 1.7.2022.)

[5] Khalifa E.: *Smart Cities: Opportunities, Challenges and Security Threats*, 2019., Dostupno na: https://www.researchgate.net/publication/342328737_Smart_Cities_Opportunities_Challenges_and_Security_Threats (Zadnje pristupano: 1.7.2022.)

[6] Bašić S., Vezilić Strmo N., Sladoljev M.: *Pametni gradovi i zgrade*, 2019., Dostupno na: https://hrcak.srce.hr/file/330159 (Zadnje pristupano: 3.7.2022.)

[7] Krishnan S., Anjana M. S., Rao S.: *Security Considerations for IoT in Smart Buildings*, 2017., Dostupno na: https://www.researchgate.net/publication/328817861_Security_Considerations_for_IoT_in_Smart_Buildings (Zadnje pristupano: 3.7.2022.)

[8] Manivannan T., Radhakrishnan P.: *A Comprehensive Analysis of Simulation Tools for Internet of Things,* 2020., Dostupno na: https://www.researchgate.net/publication/346411781_A_Comprehensive_Analysis_of_Simulation_Tools_for_Internet_of_Things (Zadnje pristupano: 5.7.2022.)

[9] Tabane E., Zuva T.: *Is there a Room for security and Privacy in IoT?*, 2020., Dostupno na: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8073758&isnumber=8073703 (Zadnje pristupano: 5.7.2022.)

[10] Liu X., Zhao M., Li S., Zhang F., Trappe, W.: *A Security Framework for the Internet of Things in the Future Internet Architecture, 2017.,* Dostupno na: www.mdpi.com/1999-5903/9/3/27/pdf (Zadnje pristupano: 7.7.2022.)

[11] Tilley A.: *How Hackers Could Use a Nest Thermostat As An Entry Point Into Your Home*, 2015., Dostupno na: https://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/#6266ed343986 (Zadnje pristupano: 7.7.2022.)

[12] Abomhara M., Koien G.: *Security and Privacy in the Internet of Things: Current Status and Open Issues*, 2014., Dostupno na: https://ieeexplore.ieee.org/document/6970594 (Zadnje pristupano: 10.7.2022.)

[13] Mahmoud R., Yousuf T., Aloul F., Zualkernan I.: *Internet of things (IoT) Security: Current Status, Challenges and Prospective Measures*, 2015., Dostupno na: https://ieeexplore.ieee.org/document/7412116 (Zadnje pristupano: 12.7.2022.)

[14] Banafa A.: *IoT Standardization and Implementation Challenges*, 2016., Dostupno na: https://iot.ieee.org/newsletter/july-2016/iot-standardization-and-implementation-challenges.html (Zadnje pristupano: 15.7.2022.)

[15] Gomez C., Paradells J.: *Wireless Home Automation Networks: A Survey of Architectures and Technologies*, Dostupno na: https://ieeexplore.ieee.org/document/5473869 (Zadnje pristupano: 15.7.2022.)

[16] Davis BD., Mason JC., Anwar M.: *Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study*, Dostupno na: https://ieeexplore.ieee.org/abstract/document/9050664 (Zadnje pristupano: 18.7.2022.)

[17] Forrest S.: *Smart Architectures for Smart Home Gateways*, Dostupno na: https://www.mips.com/blog/smart-architectures-for-smart-home-gateways/ (Zadnje pristupano: 18.7.2022.)

[18] Alabdulsalam S., Schaefer K., Kechadi T., Le-Khac NA.: *Internet of Things Forensics: Challenges and Case Study*, 2018., Dostupno na: https://www.researchgate.net/publication/322851720_Internet_of_things_forensics_Challenges_and_Case_Study (Zadnje pristupano: 20.7.2022.)

[19] Kent K., Chevalier S., Grance T., Dang H.: *Guide to Integrating Forensic Techniques into Incident Response*, Dostupno na: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf (Zadnje pristupano: 20.7.2022.)

[20] Heartfield R., Loukas G., Budimir S., Bezemskij A., Fontaine J., Filippoupolitis A., Roesch E.: *A Taxonomy of Cyber-physical Threats and Impact in the Smart Home,* 2018., Dostupno na: http://www.georgeloukas.com/publications/HeartfieldLoukas Budimir-COSE2018.pdf (Zadnje pristupano: 21.7.2022.)

[21] Wang Z.: *Personal Information Security Risks and Legal Prevention From the Perspective of Network Security*, 2020., Dostupno na: https://books.google.hr/books (Zadnje pristupano: 21.7.2022.)

[22] Day M., Turner G., Drozdiak N.: *Amazon Workers Are Listening to What You Tell Alexa*," Bloomberg, 2019., Dostupno na: https://www.bloomberg.com/ news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio#xj4y7vzkg (Zadnje pristupano: 22.7.2022.)

[23] „*German parents told to destroy doll that can spy on children*", Dostupno na: https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children (Zadnje pristupano: 22.7.2022.)

[24] „*Smart Home Security: Security and Vulnerabilities*", Dostupno na: https://www.wevolver.com/article/smart-home-security-security-and-vulnerabilities (Zadnje pristupano: 26.7.2022.)

[25] „*9 Ways to Improve IoT Device Security*", Dostupno na: https://www.hpe.com/us/en/insights/articles/9-ways-to-make-iot-devices-more-secure-1701.html (Zadnje pristupano: 28.7.2022.)

[26] „*How To Secure The IoT Environment*", Dostupno na: https://hitachi-systems-security.com/infographic-how-to-secure-the-iot-environment/ (Zadnje pristupano: 30.7.2022.)

[27] „*IoT Security: Risks, Examples and Solutions*", Dostupno na: https://www.emnify.com/blog/iot-security (Zadnje pristupano: 30.7.2022.)

[28] BITAG (Broadband Internet Technical Advisory Group: *Internet of Things (IoT) Security and Privacy Recommendations*, Dostupno na: https://www.bitag.org/ documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_ Recommendations.pdf (Zadnje pristupano: 2.8.2022.)

[29] „Why IoT Security Is Important for Your Home Network“, Dostupno na: https://www.kaspersky.com/resource-center/threats/secure-iot-devices-on-your-home-network (Zadnje pristupano: 2.8.2022.)

[30] „*Smart Cities: Threat and Countermeasures*“, Dostupno na: https://www.rambus.com/iot/smart-cities/ (Zadnje pristupano: 10.8.2022.)

[31] Javaid S., Afzal H., Arif F., Iltaf N., Abbas H., Iqbal W.: *CATSWoTS: Context Aware Trustworthy Social Web of Things System*, 2019., Dostupno na: https://www.mdpi.com/1424-8220/19/14/3076 (Zadnje pristupano: 15.8.2022.)

[32] Chi P., Wang M.: *Privacy-Preserving Broker-ABE Scheme for Multiple Cloud-Assisted Cyber Physical Systems*, 2019., Dostupno na: https://www.mdpi.com/1424-8220/19/24/5463 (Zadnje pristupano: 15.8.2022.)

[33] Tabassum T., Hossain A., Rahman A., Alhamid M., Hossain M.: *An Efficient Key Management Technique for the Internet of Things*, Dostupno na: https://www.mdpi.com/1424-8220/20/7/2049 (Zadnje pristupano: 16.8.2022.)

[34] „*Network Simulator, NetSim, Emulator, 5G, Military Communications*“, Dostupno na: https://www.tetcos.com/index.html (Zadnje pristupano: 17.8.2022.)

[35] Manna M., Amphawan A.: *Review Of Syn_Flooding Attack Detection Mechanism*, 2012., Dostupno na: https://www.researchgate.net/publication/224894855_Review_Of_Syn-Flooding_Attack_Detection_Mechanism (Zadnje pristupano: 9.9.2022.)

[36] Kibirige G., Sanga C.: *A survey on Detection of Sinkhole Attack in Wireless Sensor Network*, Dostupno na: https://arxiv.org/ftp/arxiv/papers/1505/1505.01941.pdf (Zadnje pristupano: 9.9.2022.)

Popis kratica

IoT	(Internet of Things) - Internet stvari
IIoT	(Industrial IoT) - industrijski IoT
IT	(Information Technology) - informacijska tehnologija
FPGA	(Field Programmable Gate Array) – integrirani krug dizajniran da ga konfigurira kupac ili dizajner nakon proizvodnje
TCP/IP	(Transmission Control Protocol/Internet Protocol) – grupa komunikacijskih protokola koji se koriste za međusobno povezivanje mrežnih uređaja na internetu
DoS	(Denial of Service) – napad uskraćivanjem usluga
RFID	(Radio Frequency Identification) – tehnologija koja koristi radio frekvenciju za razmjenjivanje informacija između uređaja
CA	(Certificate Authority) – entitet koji izdaje digitalne certifikate
SLA	(Service Level Agreement) – ugovor o razini usluge
IPv6	Internet protokol verzija 6
M2M	(Machine to Machine) - izravna komunikacija između uređaja koji koriste bilo koji komunikacijski kanal
SSID	(Service Set Identifier) – skupina bežičnih mrežnih uređaja koji dijele identifikator skupa usluga
WEP	(Wired Equivalent Privacy) – algoritam za sigurnu komunikaciju putem IEEE 802.11 bežičnih mreža
WPA	(Wi-Fi Protected Access) - algoritam za sigurnu komunikaciju putem IEEE 802.11 bežičnih mreža
MITM	(Man in the Middle) – čovjek u sredini, napad gdje napadač potajno prenosi i mijenja komunikaciju između dviju strana
DDoS	(Distributed Denial of Service) – distribuirano uskraćivanje usluge
PDoS	(Permanent Denial of Service) – trajno uskraćivanje usluge
SIM	(Subscriber Identity Module) – modul na kojem je pohranjen unikatni broj

eSIM	Digitalna SIM kartica koja omogućuje aktivaciju podatkovnog plana operatora bez upotrebe fizičke SIM kartice
IMEI	(International Mobile Equipment Identity) – jedinstveni broj koji je dodijeljen svakom mobitelu
VPN	(Virtual Private Network) – virtualna privatna mreža
HTTPS	(HyperText Transfer Protocol Secure) – internetski protokol koji je nastao kombinacijom HTTP i SSL/TLS protokola
TLS	(Transport Layer Security) – protokol koji omogućuje sigurnu komunikaciju putem interneta
SFTP	(Secure File Transfer Protocol) – sigurni protokol za prijenos datoteka
DNS	(Domain Name System) protokol za davanje imena mrežnim adresama
FTP	(File Transfer Protocol) – protokol za prijenos datoteka
HRoT	(Hardware Root of Trust) – povezuje sigurnost s jezgrom hardvera
SoC	(System on Chip) – integrirani krug koji integrira sve komponente sustava
OTA	(Over The Air) – različite metode distribucije softver, postavki i ključeva
OEM	(Original Equipment Manufacturer) – proizvođač originalne opreme
CATSWoTS	(Context-Aware Trustworthy Social Web of Things System) – sistem koji ocjenjuje pružatelje usluga i zatim identificira odgovarajuću uslugu
QoS	(Quality of Service) – kvaliteta usluge, mjerenje ukupnog učinka usluge
WoT	(Web of Things) – skup standarda konzorcija WWW za interoperabilnost različitih platformi IoT-a i aplikacijskih domena
ABE	(Attribute Based Encryption) – vrsta šifriranja javnim ključem u kojem tajni ključ korisnika i šifrirani tekst ovise o atributima
MQTT	(Message Queuing Telemetry Transport) – standardni protokol za razmjenu poruka za Internet stvari
LoWPAN	(Low Power Wireless Personal Area Network) – bežična osobna mreža male snage

NFC	(Near Field Communication) – kratkodometna tehnologija pomoću koje dva uređaja mogu razmjenjivati podatke
WSN	(Wireless Sensor Network) – bežična mreža koja sadrži senzore koji prate i bilježe fizičke uvjete okoliša te prosljeđuju prikupljene podatke
AODV	(Ad hoc On-Demand Distance Vector) – protokol usmjeravanja za bežične ad hoc mreže
WAN	(Wide Area Network) – mreža širokog područja
RPL	(Routing Protocol for Low Power and Lossy Networks) – protokol usmjeravanja za mreže male snage i gubitaka
DIS	(DODAG Information Solicitation) – koristi se kako bi susjedni čvorovi zatražili informacije o grafu za pridruživanje mreži
DODAG	(Destination Oriented Directed Acyclic Graph) – graf sastavljen od čvorova i veza koji čine staze koje pokazuju prema i završavaju na posebnom čvoru
DIO	(DODAG Information Object) – koristi se za distribuciju ranga i funkcije cilja za izračunavanje ranga
DAO	(DODAG Advertisement Object) – koristi se za širenje odredišne informacije prema korijenu za podržavanje silaznog RPL prometa
UDP	(User Datagram Protocol) – komunikacijski protokol koji se nalazi u dijelu transportne razine OSI modela
IDS	(Intrusion Detection Systems) – sustav za otkrivanje upada
IPS	(Intrusion Prevention Systems) – sustav za sprječavanje upada
SOS	(Secure Overlay Service) – preventivna tehnika protiv napada u IoT mreži

Popis slika

Slika 1. IoT primjena u industrijama 2
Slika 2. Primjeri pametnih uslužnih sustava grada 6
Slika 3. Pametni uslužni sustavi zgrade 7
Slika 4. Odabir komponenti koje se žele instalirati 23
Slika 5. Početni zaslon NetSim alata 24
Slika 6. Mrežna topologija okruženja pametnog doma 27
Slika 7. Prikaz zaslona za postavljanje komponenti i simulaciju 27
Slika 8. Topologija okruženja pametnog doma u alatu NetSim 28
Slika 9. Skočni prozor za postavljanje vremena trajanja simulacije 29
Slika 10. Prikaz NetSim izvornog koda u alatu Visual Studio 30
Slika 11. Prvi scenarij koji prikazuje mrežu bez zaraženog senzora 32
Slika 12. Drugi scenarij koji prikazuje mrežu sa jednim zaraženim senzorom 32
Slika 13. Treći scenarij koji prikazuje mrežu sa dva zaražena senzora 33
Slika 14. Prikaz scenarija koji se koristi u simulaciji Sink Hole napada 34
Slika 15. Prikaz scenarija koji se koristi u simulaciji DIS Flood napada 35
Slika 16. Prikaz vrijednosti Link metrike 36
Slika 17. Prikaz vrijednosti metrice aplikacija 37
Slika 18. Prikaz rezultata simulacije u mreži bez zaraženog senzora 37
Slika 19. Propusnost kod simulacije Sink Hole napada 38
Slika 20. Opcija praćenja paketa u alatu NetSim 39
Slika 21. Usporedba stope generiranja u odnosu na propusnost 40
Slika 22. Usporedba stope generiranja u odnosu na kašnjenje 40
Slika 23. Usporedba DIS intervala u odnosu na propusnost 41

Popis tablica

Tablica 1. Prednosti NetSim mrežnog simulatora u odnosu na druge simulatore..... 22
Tablica 2. Vrijednosti potrebnih parametara za provođenje simulacije SYN Flood napada..... 31
Tablica 3. Propusnost koju vide korisničke aplikacije 38
Tablica 4. Usporedba propusnosti i kašnjenja sa i bez DIS Flood-a..... 39
Tablica 5. Različiti DIS interval (ms) u odnosu na propusnost (Mbps)..... 41

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je **diplomski rad**
(*vrsta rada*)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom **Istraživanje sigurnosnih rizika u okruženju Internet stvari**, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, **9.9.2022.**

(ime i prezime, *potpis*)