UNIVERZITET CRNE GORE
ELEKTROTEHNIČKI FAKULTET

Jovan Crnogorac

Predlog metoda za određivanje broja i pozicije snifera u višekanalnim bežičnim senzorskim mrežama

- magistarski rad -

Podgorica, 2021.

UNIVERZITET CRNE GORE
ELEKTROTEHNIČKI FAKULTET

Jovan Crnogorac

Predlog metoda za određivanje broja i pozicije snifera u višekanalnim bežičnim senzorskim mrežama

- magistarski rad -

Podgorica, 2021.

PODACI I INFORMACIJE O MAGISTRANTU

Ime i prezime: **Jovan Crnogorac**
Datum i mjesto rođenja: 06.06.1995. Nikšić, Crna Gora
Prethodno završene studije:

Osnovne studije: Elektrotehnički fakultet Podgorica, Univerzitet Crne Gore, smjer: Elektronika, telekomunikacije i računari, 180 ECTS kredita, 2017. godine
Specijalističke studije: Elektrotehnički fakultet Podgorica, Univerzitet Crne Gore, smjer: Telekomunikacije, 60 ECTS kredita, 2018. godine

INFORMACIJE O MAGISTARSKOM RADU

Elektrotehnički fakultet
Studijski program: Elektronika, telekomunikacije i računari - Telekomunikacije
Naslov rada: **Predlog metoda za određivanje broja i pozicije snifera u višekanalnim bežičnim senzorskim mrežama**
Mentor: Prof. dr Enis Kočan

UDK, OCJENA I ODBRANA MAGISTARSKOG RADA

Datum prijave magistarskog rada: 29.01.2021.
Datum sjednice Vijeća na kojoj je prihvaćena tema: 26.05.2021.
Komisija za ocjenu teme i podobnosti magistranta:

1. Prof. dr Milica Pejanović-Đurišić
2. Prof. dr Zoran Veljović
3. Prof. dr Enis Kočan

Komisija za ocjenu rada:

1. Prof. dr Milica Pejanović-Đurišić
2. Prof. dr Zoran Veljović
3. Prof. dr Enis Kočan

Komisija za odbranu rada:

1. Prof. dr Milica Pejanović-Đurišić
2. Prof. dr Zoran Veljović
3. Prof. dr Enis Kočan

Datum odbrane: 12.01.2022.

Sadržaj

Sažetak 1
Abstract 2
1. Uvod 3
2. Bežične senzorske mreže i aktuelni standardi 6
2.1. Bežične senzorske mreže 6
2.1.1. Oblast primjene bežičnih senzorskih mreža 7
2.1.2. Mrežna arhitektura bežičnih senzorskih mreža 10
2.1.3. Trendovi u razvoju i potencijal u budućnosti 13
2.2. IEEE 802.15.4e *Time Slotted Channel Hopping* 15
2.3 6TiSCH protokol 17
2.3.1. 6TiSCH mrežna arhitektura 17
3. Modelovanje 6TiSCH mreža 23
3.1. 6TiSCH Simulator 23
3.2. *Trace-based* 6TiSCH simulacije 28
4. Metode za odabir broja i pozicija za snifere 30
4.1 Sniferi u višekanalnim WSNs 30
4.1.2 *BeamLogic 802.15.4 Site Analyzer* 32
4.2 Metoda za odabir broja i pozicija za snifere zasnovana na teoriji grafova 32
4.3 Metoda za odabir broja i pozicija za snifere zasnovana na teoriji vjerovatnoće i kombinatorici 37
4.3.1 Broj dostupnih snifera kao ulazni parametar za Metodu II 38
4.3.2 Prosječna vjerovatnoća detekcije paketa kao ulazni parametar za Metodu II 41
5. Analiza simulacionih rezultata 43
5.1 Analiza rezultata za Metodu I 46
5.2 Analiza rezultata za Metodu II 53
5.3 Poređenje Metode I i Metode II 56
Zaključak 59
Literatura 62
Lista skraćenica 65

Sažetak

Kako bežične senzorske mreže (engl. *Wireless Sensor Networks* – WSNs) postaju veće, kompleksnije i njihova uloga sve značajnija, od posebne je važnosti imati uvid u razmijenjeni paketski saobraćaj. Sniferi su uređaji koji koriste specijalizovani hardver i softver i omogućavaju detekciju i analizu mrežnog saobraćaja. Sniferi imaju ograničenu osjetljivost prijemnika, pa je neophodno koristiti više od jednog snifera, da bi se omogućilo hvatanje cjelokupnog saobraćaja razmijenjenog u velikim *multi-hop* mrežama.

U radu je predstavljeno rješenje koje omogućava definisanje potrebnog broja i pozicija snifera, tako da mogu uhvatiti što veći procenat saobraćaja razmijenjenog u WSN, i na taj način omogućiti kvalitetnu analizu rada mreže, kao i protokola koji se u njoj koriste. U radu su predstavljene dvije metode koje se zasnivaju na upotrebi teorije grafova i teorije vjerovatnoće sa kombinatorikom. Predstavljene metode su realizovane i testirane u simulacionom okruženju. Postojeći 6TiSCH Simulator (engl. *IPv6 over the TSCH mode of IEEE 802.15.4e*) koji vrši simuliranje senzorskih mreža je nadograđen, na način da je modelovana upotreba snifera i implementirane su dvije predložene metode za određivanje njihovog broja i pozicije.

Prva predložena Metoda omogućava određivanje lokacija za snifere u velikim senzorskim mrežama, kakva je i modelovana WSN sa 50 čvorova raspoređenim na prostoru od 2×2 km, gdje je ostvareno hvatanje oko 90% paketa sa 10 snifera. Druga Metoda je prilagođena analizi rada manjih WSNs, odnosno mreža u kojima se koristi manji broj snifera.

Predložene metode omogućavaju određivanje lokacija, ili broja i lokacija, za snifere u višekanalnim *multi-hop* WSNs. Efikasan rad snifera uz visok procenat detekcije razmijenjenog saobraćaja, omogućava kvalitetniju analizu WSNs, protokola koji se koriste, odabrane mrežne topologije i senzorskih čvorova, što značajno može ubrzati razvoj ove trenutno aktuelne oblasti.

Ključne riječi: Bežične senzorske mreže, Internet stvari, *Multi hop,* Snifer, *Testbed*

Abstract

As wireless sensor networks (WSNs) grow larger, more complex and their role becomes more significant, it is of particular importance to get an insight into the network traffic. For this purpose, sniffers play an irreplaceable role. Sniffers are devices with specialized software that can capture and analyze network traffic. Since a sniffer is a device of limited range, it is necessary to deploy multiple sniffers in order to cover a multi-hop network.

This motivates the research on the optimal number and position of sniffers in the network. We present two solutions based on a minimal dominant set from graph theory and probabilistic theory with combinatorics. We evaluate these two solutions and implement it as an extension of the 6TiSCH (*IPv6 over the TSCH mode of IEEE 802.15.4e*) Simulator. 6TiSCH Simulator is extended with a special type of a device, a sniffer, which can listen on all 16 channels, as well as with the algorithms for sniffer selection.

The first solution enables determination of locations for sniffers in large sensor networks, such as the modeled WSN with 50 nodes distributed in an area of 2×2 km, where the proposed solution achieved 10% of packet drops over all channels using 10 sniffers. The second solution is suitable for deployment of traffic analysis in small WSNs, i.e., WSNs with fewer number of sniffers.

The proposed solutions allow the determination of locations, or number and locations for sniffers in multi-hop multi-channel WSNs. Efficient operation of sniffers with a high percentage of detected traffic, allows better analysis of WSNs, protocols, network topologies and sensor nodes, which can significantly improve the development of this field.

Keywords: Wireless sensor network, Internet of Things, Multi hop, Snifer, Testbed

Glava 1

1. Uvod

Bežične senzorske mreže (engl. *Wireless Sensor Networks* – WSNs) predstavljaju distribuirane sisteme, koji se sastoje od senzorskih čvorova povezanih radio linkovima. Njihova primjena se zasniva na upotrebi malih, jeftinih i više-funkcionalnih uređaja, koji međusobno komuniciraju i razmjenjuju podatke i tako formiraju ad hok (engl. *ad hoc*) mrežu. Prikupljeni podaci se nakon jednostavne obrade na senzorima prosljeđuju ka krajnjim korisnicima. WSNs se mogu primjenjivati u različitim oblastima kao što su vojna industrija, zdravstvo, kućna automatizacija, poljoprivreda, saobraćaj i drugo.

Tokom razvoja telekomunikacionih mreža, a posebno WSNs, korisno je imati uvid u razmijenjeni paketski saobraćaj. Analiza razmijenjenog saobraćaja olakšava detekciju grešaka do kojih može doći usljed distribuirane obrade podataka, ograničenih komunikacionih, procesorskih i memorijskih resursa senzorskih čvorova.

Sniferi su uređaji koji koriste specijalizovani hardver i softver i omogućavaju detekciju i analizu mrežnog saobraćaja. Ovi uređaji mogu biti od koristi tokom detekcije i otklanjanja grešaka, analize rada WSNs, razvoja novih standarda i protokola i implementacije u realnim mrežnim okruženjima. Sniferi omogućavaju detaljan uvid u rad mreže, sa akcentom na praćenje rada svakog senzora, analizu rutiranja, uzroka gubitaka pri prenosu i kašnjenja u mreži [1]. Pošto postoji potreba da određene WSNs pokrivaju veće prostore, a samim tim i da uključe veći broj senzora, onda u takvim scenarijima primjena samo jednog snifera ne bi omogućila snimanje kompletnog ili velikog dijela saobraćaja razmijenjenog u mreži. Razlog za to je sama priroda radio kanala, ograničena osjetljivost prijemnika snifera, mala emisiona snaga senzora, interferencija i feding. Zato je potrebno koristiti više snifera, koji će detektovati što više paketa razmijenjenih u mreži i na taj način omogućiti kvalitetniju analizu.

Tradicionalne WSNs za komunikaciju koriste jedan frekvencijski kanal, a naprednije senzorske mreže sve češće koriste više kanala za komunikaciju. Danas se komunikaciona rješenja najvećeg broja WSNs zasnivaju na IEEE 802.15.4 standardu za bežične personalne mreže male brzine prenosa podataka (engl. *Low-Rate Wireless Personal Area Networks* – LR-WPANs), koji definiše fizički nivo i nivo linka [2]. Postoje brojni protokoli i skupovi protokola, koji su razvijeni za više komunikacione slojeve u WSNs. Iznad dva sloja koja

definiše IEEE 802.15.4 standard, najčešće se koriste ZigBee, XBee, 6TiSCH (engl. *IPv6 over the TSCH mode of IEEE 802.15.4e*) i drugi.

6TiSCH kombinuje industrijske performanse IEEE 802.15.4e standarda, koji koristi tehniku frekvencijskog skakanja u definisanim vremenskim slotovima (engl. *Time Slotted Channel Hopping* – TSCH), sa višim nivoima mrežne arhitekture koji se primjenjuju u standardima Interneta stvari (engl. *Internet of Things* – IoT), definisanih od strane IETF-a (engl. *Internet Engineering Task Force*). 6TiSCH na fizičkom nivou najčešće koristi frekvencijske opsege na 868 MHz, 915 MHz i 2.4 GHz, koji su namijenjeni za industrijsku, naučnu i medicinsku primjenu (engl. *Industrial, Science and Medical* – ISM). IEEE 802.15.4e standard koristi 16 ortogonalnih kanala za komunikaciju, a TSCH vrši promjenu frekvencijskog kanala u svakom vremenskom slotu i pored toga omogućava *multi-hop* komunikaciju. Cilj česte promjene radio kanala je smanjenje štetnog uticaja prostiranja signala višestrukim putanjama (engl. *Multipath Fading* – MPF), uticaja kolizije i eksterne interferencije [3].

Prije postavljanja snifera u ovim višekanalnim *multi-hop* mrežama, potrebno je razmotriti pozicije za njihovo postavljanje i oblast koju jedan snifer može pokriti. Zbog ograničene osjetljivosti radio prijemnika, jedan snifer ne može snimati sav saobraćaj u velikim WSNs koje koriste *multi-hop* tehniku. Ova tehnika podrazumijeva razmjenu paketa između čvorova u kojoj se paketi ne moraju uvijek razmjenjivati direktno od izvora ka odredištu, već posredstvom više usputnih čvorova, dok konačno ne stignu do svog odredišta. Veliki broj snifera bi omogućio detekciju velikog broja razmijenjenih paketa, ali u isto vrijeme to bi dovelo do dodatnih troškova pri postavljanju i održavanju mreže. Takođe, dio saobraćaja bi bio snimljen sa više snifera, što bi dovelo do pojave višestrukih kopija paketa na prijemu. Ove pakete je potrebno filtrirati kako bi se klijentima prikazao samo stvarni saobraćaj razmijenjen u mreži. Optimalno rješenje predstavlja postavljanje minimalnog broja snifera koji bi omogućili hvatanje cjelokupnog mrežnog saobraćaja ili hvatanje dovoljne količine paketa kako bi analiza bila efikasna.

Pri razmatranju pozicija za snifere u WSN, u radu se podrazumijeva da snifer može istovremeno snimati saobraćaj na svim frekvencijskim kanalima koji se koriste u mreži i da je poznata matrica konektivnosti mreže u koju se postavljaju sniferi. Matrica konektivnosti sadrži podatke o radio linkovima između svih senzora u mreži, predstavljene odgovarajućim odnosom uspješno prenesenih paketa i ukupnog broja paketa (engl. *Packet Delivery Ratio* – PDR). U radu su predstavljena rješenja koja koriste teoriju grafova zasnovanu na analizi

matrica konektivnosti u WSNs, a zatim pristup zasnovan na teoriji vjerovatnoće i kombinatorici, na osnovu poznatih karakteristika linkova u velikim bežičnim senzorskim mrežama. Takođe, za unaprijed zadati broj snifera, predložene metode omogućavaju određivanje pozicija za snifere u posmatranoj WSN, na način da će se ostvariti snimanje najvećeg mogućeg procenta mrežnog saobraćaja [4]. Pri tome, u zavisnosti od dostupnih karakteristika mreže, potrebno je odabrati odgovarajuću metodu za odabir broja i pozicije snifera, i podesiti ulazne parametre.

Rad je organizovan na sledeći način. U drugoj Glavi opisan je razvoj bežičnih senzorskih mreža, njihove glavne karakteristike, oblasti primjene, mrežna arhitektura i trendovi u budućem razvoju. Pored ovoga opisan je IEEE 802.15.4e standard i 6TiSCH protokol. Treća Glava govori o 6TiSCH Simulatoru, njegovoj strukturi, načinu rada i mogućnostima primjene. Četvrta Glava opisuje predložene metode za određivanje broja i pozicije snifera u višekanalnim bežičnim senzorskim mrežama. Na početku je opisan značaj snifera u WSNs, objašnjen pojam matrica konektivnosti i naveden primjer komercijalno dostupnog snifera. Prvo je opisana metoda za odabir broja i pozicija za snifere koja je zasnovana na teoriji grafova (Metoda I), gdje je prikazan njen pseudokod i detaljno objašnjen način rada. Nakon toga, na isti način, opisana je i druga metoda za odabir broja i pozicija za snifere zasnovana na teoriji vjerovatnoće i kombinatorici (Metoda II). Peta Glava prikazuje analizu simulacionih rezultata za Metode I i II, gdje se vrši pregled više grafika za različite ulazne parametre metoda. Na kraju se vrši poređenje dvije metode i daju se zaključci o načinu njihovog korišćenja.

Glava 2

2. Bežične senzorske mreže i aktuelni standardi

2.1. Bežične senzorske mreže

Napredak u oblasti bežičnih komunikacionih tehnologija, interneta i elektronike doveo je do razvoja malih, jeftinih i više-funkcionalnih senzorskih čvorova, koji međusobno mogu komunicirati na malim rastojanjima, i formirati bežične senzorske mreže. Ovi jednostavni uređaji mogu vršiti monitoring različitih parametara iz okoline, obrađivati i razmjenjivati prikupljene podatke i prosljeđivati ih putem interneta ili drugih telekomunikacionih tehnologija ka krajnjim korisnicima.

Početne ideje o primjeni WSNs se, kao i za većinu naprednih tehnoloških rješenja, javljaju u vojnoj industriji. Prvi sistem koji podsjeća na današnje WSNs se javlja u Ratnoj mornarici Sjedinjenih Američkih Država (SAD) i nazvan je SOSUS (engl. *Sound Surveillance System*). Razvijen je pedesetih godina prošlog vijeka i njegov zadatak je bio detekcija i praćenje Sovjetskih podmornica u Atlantskom i Tihom okeanu. Danas se ova tehnologija koristi za istraživanje okeana i praćenje seizmičkih aktivnosti [5]. Takođe, tokom Hladnog rata razvijena je mreža radara koji su služili za ranu detekciju i praćenje letjelica koje bi mogle ugroziti SAD i Kanadu. Sistem je izgrađivan i razvijan godinama i uključuje više zemaljskih radarskih stanica koje rade u kooperaciji sa specijalno opremljenim avionima tipa AWACS (engl. *Airborne Warning and Control System*), koji posjeduju osjetljive radarske sisteme za nadzor velikih područja. Ove senzorske mreže koriste hijerarhijsku strukturu obrade podataka, koja se vrši na različitim nivoima prije nego što podaci dođu do krajnjeg korisnika. Svaki senzor (radar) djelimično vrši obradu podataka, prije nego što ih pošalje ka glavnoj kontrolnoj stanici koja analizira sve podatke i korisniku prikazuje cjelokupnu sliku područja koje se nadzire. Nakon razvoja interneta, agencija Ministarstva odbrane SAD (engl. *Defense Advanced Research Projects Agency* – DARPA) tokom 1980. godine radi na razvoju distribuiranih senzorskih mreža (engl. *Distributed Sensor Network* – DSN). U početnim fazama rada interneta, ispitivane su mogućnosti njegovog korišćenja za povezivanje senzorskih čvorova. Radilo se na razvoju distribuirane obrade podataka, novih komunikacionih protokola i kreiranju dinamičnog testnog okruženja. Daljim razvojem

računarskih i komunikacionih tehnologija pojavljuju se mali i jeftini senzori, unaprjeđuje se bežična komunikacija i razvijaju se efikasni procesori koji su omogućili razvoj bežičnih *ad-hoc* senzorskih mreža. Nakon ekspanzije primjene ovih tehnologija u civilne, komercijalne i naučnoistraživačke svrhe, počinje široka primjena i ubrzan razvoj WSNs [6].

Realizacija WSNs u većini slučajeva zahtijeva upotrebu bežične *ad-hoc* komunikacije. Bežične *ad-hoc* mreže predstavljaju decentralizovanu vrstu bežičnih mreža, u kojima se razmjena podataka ne ostvaruje posredstvom postojeće mrežne infrastrukture, kao što su ruteri ili pristupne tačke. Umjesto toga, svaki čvor u mreži učestvuje u rutiranju i zbog toga mora posjedovati određene podatke o drugim čvorovima, koji mu omogućavaju izvršavanje operacija rutiranja. Algoritmi i protokoli rutiranja za tradicionalne *ad-hoc* mreže nisu dobro prilagođeni radu u WSNs koje imaju karakteristične osobine, zato se za njih razvijaju posebni protokoli. U osobine koje su karakteristične za bežične senzorske mreže spadaju:

- koristi se veliki broj senzorskih čvorova koji mogu biti raspoređeni na malom ili velikom prostoru,
- sposobnost rada u različitim okruženjima,
- robusnost na otkazivanje pojedinačnih senzora,
- ograničene procesorske i memorijske sposobnosti, kao i dostupna energija na senzorskim čvorovima,
- senzori za napajanje najčešće koriste litijum-jonske ili druge baterije koje omogućavaju dugotrajno napajanje, nekad i više godina,
- topologija mreže je sklona čestim izmjenama,
- najčešće se koristi *broadcast* i *multi-hop* bežična komunikacija.

2.1.1. Oblast primjene bežičnih senzorskih mreža

WSNs zbog svoje prilagodljivosti i male cijene mogu naći primjenu u različitim industrijskim i komercijalnim okruženjima, kao što su u vojna i teška industrija, zdravstvo, kućna automatizacija, poljoprivreda, saobraćaj, zaštita životne sredine i drugo. U početku su primjenjivane za jednostavne operacije kao što su kontrola kvaliteta vazduha i vode, detekcija požara i seizmičkih aktivnosti, praćenje saobraćaja. Danas sve češće nalaze primjenu u industrijskim postrojenjima za kontrolu proizvodnje, transporta i distribucije električne energije, preradu otpadnih voda i automatizaciju u različitim tehnološkim granama, itd.

Zbog široke oblasti primjene, senzorski čvorovi se mogu postavljati u različitim okruženjima. U zavisnosti od pristupačnosti terena mogu se postavljati po precizno definisanom rasporedu, ili na slučajnim pozicijama u teško pristupačnim područjima. Zbog toga, mrežni protokoli i algoritmi za komunikaciju moraju biti prilagodljivi različitim scenarijima pri formiranju mreže. Takođe, baterije moraju biti dugotrajne, kako bi se omogućio višegodišnji rad senzora, koje je u nepristupačnim područjima teško servisirati.

Zaštita životne sredine

Nadzor prirodnih područja se nameće kao logičan izbor za primjenu bežičnih senzorskih mreža koje mogu vršiti praćenje različitih parametara kao što su temperatura, vlažnost zemljišta i vazduha, osvijetljenost, vazdušni pritisak i drugo. WSNs omogućavaju analizu velikih i teško dostupnih područja. Trenutna istraživanja u oblasti efekata staklene bašte i njenog uticaja na globalno zagrijavanje imaće veliki značaj u budućnosti, kako bi se detaljno istražio njen uticaj i smanjile negativne posljedice na biljni i životinjski svijet.

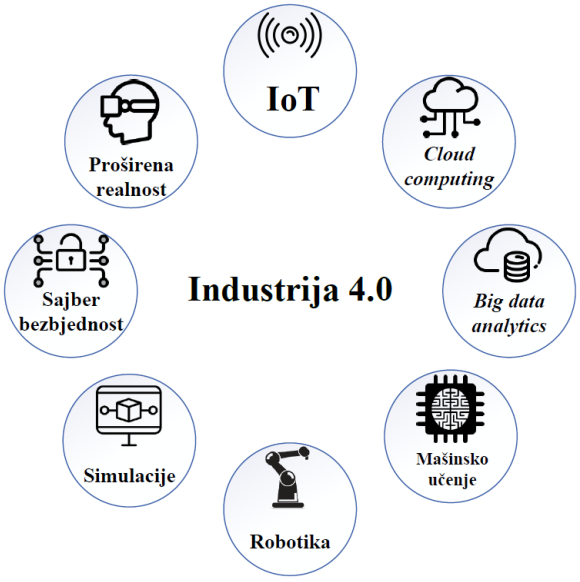
SIVAM (engl. *Amazon Surveillance System*) predstavlja kompleksan sistem za nadzor oblasti Amazonije u Brazilu. Ova oblast obuhvata Brazilske kišne šume koje su nepristupačne i teško prohodne, i često se koriste za krijumčarenje narkotika i ljudi. Ovo područje obuhvata više od polovine kišnih šuma na našoj planeti, i karakteriše ga veliki biodiverzitet, što ovu oblast čini vrlo osjetljivom na klimatske promjene i uticaj čovjeka. SIVAM omogućava praćenje različitih parametara u svrhu zaštite biljnog i životinjskog svijeta, detekciju požara i nelegalnih aktivnosti. Koristi senzore na zemlji, koji služe za praćenje različitih hidrometeoroloških parametara, satelite koji vrše snimanje velikih područja i avione za detaljnije snimanje manjih oblasti i nadzor iz vazduha [7].

Industrija

Upotreba WSNs u industriji može smanjiti troškove i povećati efikasnost i sigurnost. Nadzor rada industrijskih mašina, kao što je praćenje temperature, vibracija i nivoa podmazivanja mehaničkih sklopova, kao i mogućnost postavljanja senzora u nepristupačnim i opasnim okruženjima gdje ljudsko prisustvo nije moguće, može značajno doprinijeti daljem razvoju industrije. Koncept Industrijskog Interneta stvari (engl. *Industrial Internet of Things* – IIOT) podrazumijeva povezivanje različitih industrijskih mašina sa naprednim informacionim sistemom, gdje se uz obradu velike količine podataka prikupljenih uz pomoć različitih senzora, vrši kontrola industrijskih procesa kako bi se postigla veća efikasnost i visok stepen automatizacije.

Fleksibilnost i prilagodljivost u različitim radnim okruženjima su neophodni za IIoT. Nedavno su se pojavili prvi standardi specijalno dizajnirani za ovu oblast, WirelessHART [8] i ISA100.11 [9]. Ipak, postoje određena ograničenja po pitanju skalabilnosti, posebno u velikim WSNs, koje pokrivaju velike prostore u industrijskim postrojenjima. Celularne mreže treće (3G), četvrte (4G) i pete (5G) generacije, omogućavaju dobru pokrivenost na velikom prostoru, ali zahtijevaju kompleksnu mrežnu infrastrukturu i rad u licenciranim frekvencijskim opsezima. Iako IIoT senzori koriste linkove sa malim protokom podataka, potrebno je povezati veliki broj uređaja, koji imaju ograničene procesorske sposobnosti i dostupnu energiju, a da pri tome komunikacija bude sa malim kašnjenjem (od 10 do 100 ms), sigurna od neovlašćene upotrebe i pouzdana (99.99%).

Koncept Industrije 4.0 (gdje 4.0 predstavlja četvrtu industrijsku revoluciju), treba da obezbijedi korišćenje internet tehnologija u industriji, kako bi se povećala efikasnost proizvodnje uz pomoć različitih servisa koji će biti omogućeni u naprednim „pametnim“ fabrikama [10].



Slika 2.1 Tehnologije koje će omogućiti realizaciju koncepta Industrija 4.0

Na *Slici 2.1*, prikazane su tehnologije koje će se koristiti u naprednim industrijskim procesima, koji će omogućiti realizaciju koncepta Industrije 4.0. Osnovu ovog sistema čini veliki broj senzora koji će nadgledati različite parametre. Velika količina podataka se obrađuje uz pomoć algoritama koji uključuju i mašinsko učenje, i na osnovu dobijenih rezultata vrše se određene akcije i kontroliše rad industrijskih robota i proizvodnih mašina. Proširena realnost se može koristiti tokom dizajniranja novih proizvoda, kako bi se lakše

kreirali prototipi i uočili nedostaci. Čitav sistem mora da bude veoma pouzdan i zaštićen od sajber napada, jer je većina uređaja povezana na Internet.

Saobraćaj

Razvoj senzorskih mreža i smanjenje cijena senzora otvaraju nove mogućnosti za primjenu u ovoj oblasti. Danas je mnogo lakše pratiti veliki broj saobraćajnih dionica, vršiti obradu podataka i na taj način generisati detaljniju sliku stanja saobraćaja na većim područjima. Broj vozila koji učestvuju u saobraćaju se eksponencijalno povećava, a putna infrastruktura često ne može da isprati ovaj nivo rasta. Zbog toga, saobraćajne gužve su sve češće, što doprinosi i značajnom povećanju zagađenosti vazduha, posebno u gradskim sredinama. Upravljanje i kontrola saobraćajnica postaje veoma važan faktor, kako bi se povećala efikasnost i što bolje iskoristila putna infrastruktura. WSNs se zbog jednostavne instalacije, brzine prenosa podataka i robusnosti, mogu koristiti za praćenje broja vozila, detekciju zagađenosti vazduha, gužvi i saobraćajnih nezgoda. U bliskoj budućnosti se predviđa korišćenje različitih senzora na svakom automobilu i komunikacija između vozila (engl. *Vehicle-to-vehicle* – V2V). Na ovaj način značajno se može povećati i sigurnost saobraćaja.

Kućna automatizacija

Jedan od načina primjene WSNs u stambenim objektima odnosi se na nadzor i kontrolu temperature i vlažnosti vazduha u čitavom objektu. Na ovaj način se može poboljšati energetska efikasnost kao i kvalitet života u njima. Senzorskim mrežama se može pratiti i seizmička stabilnost objekata nakon zemljotresa, kako bi se lakše utvrdilo da li su sigurni za dalje korišćenje.

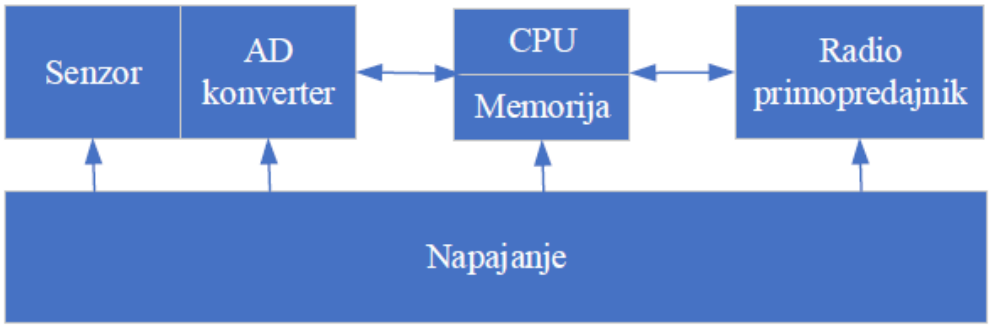
Poljoprivreda

Značajna primjena WSNs se može ostvariti u poljoprivredi. Senzori temperature, vlažnosti i hemijskog sastava zemljišta se mogu primjenjivati za kontrolu uzgoja različitih sorti biljaka. Senzori brzo mogu detektovati različite promjene prije nego one počnu negativno uticati na biljke.

2.1.2. Mrežna arhitektura bežičnih senzorskih mreža

Senzorski čvor predstavlja osnovnu i najvažniju gradivnu jedinicu WSNs. Mreže mogu sadržati stotine ili hiljade senzorskih čvorova koji međusobno komuniciraju. Jedan

čvor može koristiti više različitih senzora koji snimaju parametre okoline. Najčešće se koristi temperaturni senzor, senzor pritiska, detektor zvuka, senzor vlažnosti vazduha, senzor vidljive i infracrvene svjetlosti, detektor kretanja, različiti senzori za hemijske promjene (mjerač pH vrijednosti, detektori radijacije, ugljen-monoksida i ugljen-dioksida itd.). Šematski prikaz senzorskog čvora je predstavljen na *Slici 2.2*.

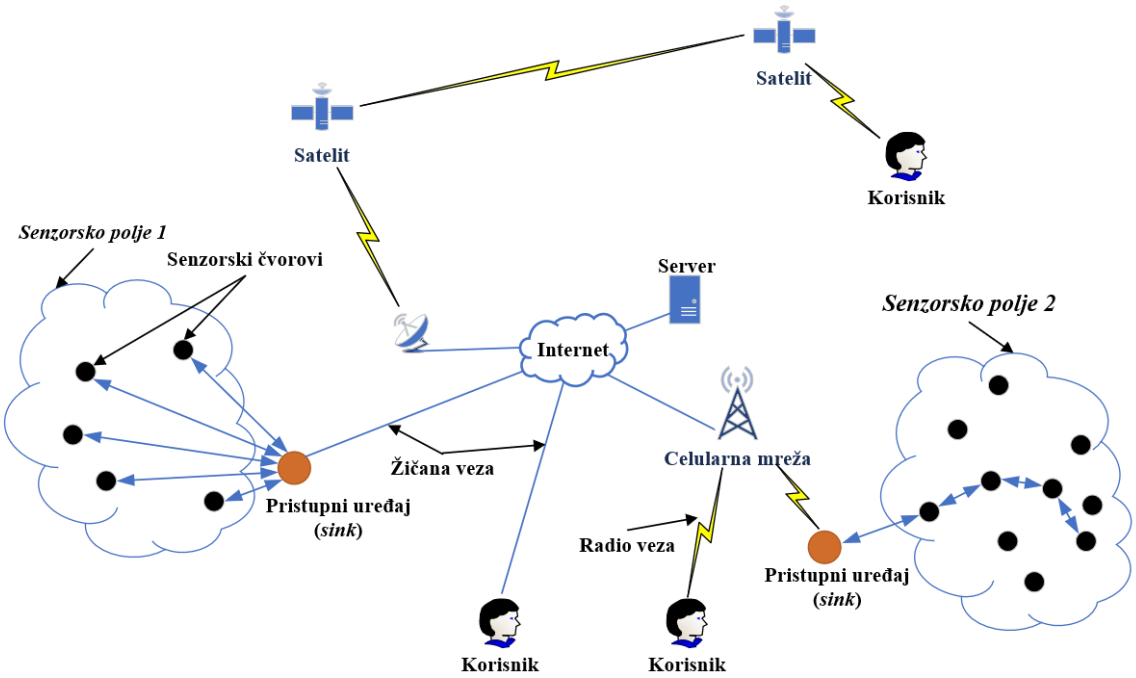


Slika 2.2 Šematski prikaz senzorskog čvora

Svaki senzorski čvor se sastoji od procesora, memorije, radio primopredajnika, analogno-digitalnog konvertera, izvora napajanja (najčešće litijum-jonske baterije) i jednog ili više senzora. Procesori koji se koriste na čvorovima su najčešće jednostavni i zahtijevaju malu količinu energije za rad. Njihov zadatak je prikupljanje i obrada podataka, koji preko analogno-digitalnog konvertera stižu od elektronskih senzora. Radio primopredajnik služi za slanje prikupljenih podataka i prijem kontrolnih poruka. Veličina i cijene čvorova mogu biti različite, u zavisnosti od primjene za koju se koriste i složenosti senzora koji se na njima nalaze.

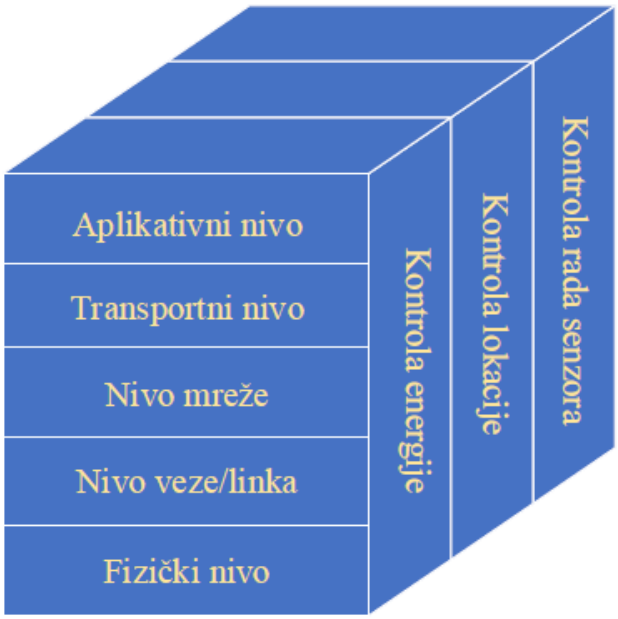
Primjer mrežne arhitekture bežične senzorske mreže je prikazan na *Slici 2.3*. Prikazane su dvije WSNs, koje su označene kao *Senzorsko polje 1* i *Senzorsko polje 2*. Ova polja sadrže više senzorskih čvorova koji prikupljaju podatke. *Senzorsko polje 1* razmjenjuje podatke po principu *single-hop* komunikacije, gdje se podaci sa svakog čvora pojedinačno šalju ka pristupnom uređaju (engl. *Sink*). Dok *Senzorsko polje 2*, koristi *multi-hop* tip komunikacije, tako da se korisni podaci preko više usputnih čvorova takođe šalju ka pristupnom uređaju, koji ih prosljeđuje dalje van WSN. Podaci se djelimično obrađuju na svakom senzoru, a zatim objedinjuju na serveru, ili na korisničkoj strani, gdje se prikupljeni podaci prikazuju korisnicima ili čuvaju za kasnije analize. Podaci koje su senzori prikupili se mogu prosljeđivati preko satelitske komunikacije, celularnih mreža, interneta, ili bilo koje dostupne telekomunikacione tehnologije ka krajnjim korisnicima. Dizajn WSNs i odabir

tehnologija za komunikaciju sa klijentima zavisi od više faktora, uključujući veličinu mreže i broj senzora, kvalitet usluga, bezbjednost, broj korisnika, cijenu i drugo [6].



Slika 2.3 Primjer mrežne arhitekture bežičnih senzorskih mreža

Model arhitekture protokola kod WSNs se može predstaviti preko referentnog modela prikazanog na *Slici 2.4.* Sastoji se od fizičkog nivoa, nivoa veze/linka, nivoa mreže, transportnog i aplikativnog nivoa.



Slika 2.4 Model arhitekture protokola za bežične senzorske mreže

Fizički nivo je zadužen za prenos toka bita između mrežnih sistema. Definiše radnu frekvenciju, modulacionu tehniku i tip enkripcije podataka. IEEE 802.15.4 standard definiše rad na opsezima 868 MHz, 915 MHz i 2.4 GHz. Najčešće se koriste kanali na opsegu 2.4 – 2.485 GHz, koji spada u nelicencirane ISM opsege, slobodne za upotrebu. Izbor modulacije zavisi od uslova na radio kanalu, dostupne energije na senzorima i količine informacija koje je potrebno prenijeti. Binarne modulacione tehnike koriste jednostavan hardver i malo energije i mogu biti dobar izbor za WSNs. Pokazuje se da su ultra-širokopojasne modulacije (engl. *Ultra Wide Band* – UWB) pogodnije za WSNs zbog jednostavnosti i linearnog rada [11].

Pošto fizički nivo obezbjeđuje samo prenos toka bita, nivo linka čini fizičku vezu pouzdanom. Vrši kontrolu protoka podataka i kontroliše da li je senzor u aktivnom ili pasivnom stanju, detektuje greške pri prenosu i vrši njihovu korekciju ili pokreće ponovno slanje. Pored ovoga, nivo linka vrši multipleks paketa, adresiranje i kontrolu zaglavlja.

Nivo mreže kontroliše formiranje mrežne topologije, konfiguriše i adresira uređaje, prati topologiju mreže i detektuje susjedne čvorove. Takođe, kontroliše i planira putanje paketa od izvora ka destinaciji kako bi se smanjila potrošnja energije.

Transportni nivo kontroliše tok podataka ka nižim nivoima, povezivanje senzora na druge mreže kao što je internet, ukoliko senzor ima takvu mogućnost, i vrši kontrolu pouzdanosti mehanizma razmjene podataka.

Aplikativni nivo omogućava komunikaciju aplikacijama koje koristi senzorski čvor.

2.1.3. Trendovi u razvoju i potencijal u budućnosti

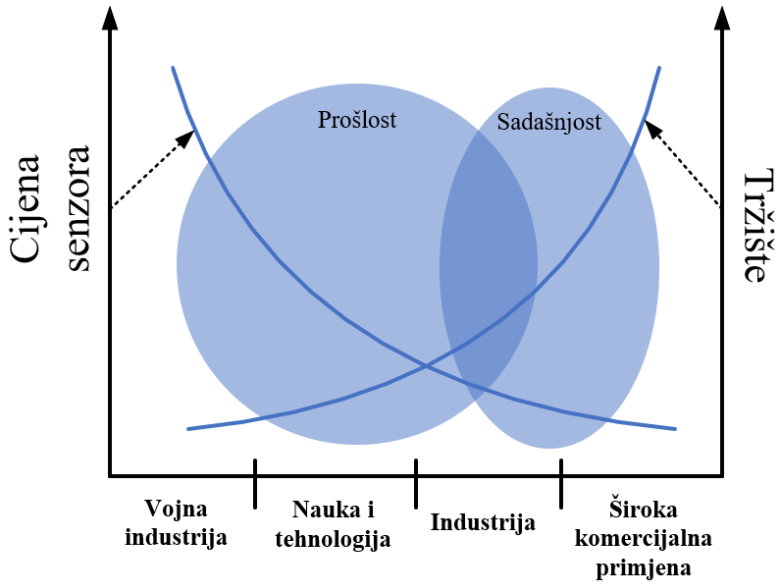
Tržište bežičnih senzorskih mreža 2020. godine iznosilo je 46.76 milijardi američkih dolara i očekuje se da će dostići 124 milijarde do 2026. godine, sa predviđenim godišnjim rastom od 17.64% u periodu 2021-2026. godina. Uvođenje naprednih tehnologija, kao što je vještačka inteligencija (engl. *Artificial Intelligence* – AI), IoT koncepta i 5G mreža, značajno ubrzava razvoj i otvara nova tržišta za WSNs. Sve veća primjena automatike i robotike u industriji povećala je potrebe za primjenom WSNs koje se koriste za nadzor, kontrolu i povećanje pouzdanosti i bezbjednosti, što takođe značajno utiče na nagli rast ove nove grane privrede [12]. Značajna su i ulaganja u razvoj rješenja za realizaciju koncepta pametnih gradova i autonomnih vozila.

U zavisnosti od zahtjeva tržišta, razvoj WSNs se može podijeliti na unaprjeđenje hardvera, softvera i analizu i razvoj za primjene u novim oblastima.

Danas je dostupan veliki broj različitih i preciznih senzora svijetlosti različitih talasnih dužina, senzora pokreta i lokacije, temperature, vlažnosti, ubrzanja, pulsa, krvnog pritiska, nivoa glukoze i kiseonika u krvi, nivoa ugljen-dioksida i ugljen-monoksida u vazduhu, radijacije, hemijskog sastava zemljišta, senzora za detekciju pješaka i vozila i drugih. Razvojem novih vrsta senzora i smanjenjem njihove cijene otvaraju se različite mogućnosti primjene svakog od njih.

Za bežičnu komunikaciju dostupne su različite tehnologije i standardi, kao što su Wi-Fi (IEEE 802.11), *Bluetooth* (IEEE 802.15.1), *Bluetooth/WLAN* (IEEE 802.11/IEEE 802.15.1 *coexistence*), celularne mreže, *Bluetooth Smart*/BLE, *ZigBee* (IEEE 802.15.4), *NFC* (engl. *Near Field Communication*), *Wireless HART*, ISA100, ANT+, 6TiSCH i sistemi za navigaciju kao što su GPS (engl. *Global Positioning System*), GLONASS (engl. *Global Navigation Satellite System*), BDS (engl. *BeiDou Navigation Satellite System*) i Galileo. Sve ove tehnologije i novi specijalizovani protokoli namijenjeni isključivo za WSNs će omogućiti njihov brži razvoj i primjenu.

Iako na tržištu postoji velika potražnja i interesovanje za ovim tehnologijama, do predviđenog nivoa sveobuhvatne primjene bežičnih senzorskih mreža u različitim oblastima i dalje nije došlo. Upotreba u vojnoj i teškoj industriji se zasniva na korišćenju skupih kompleksnih i specijalizovanih senzora sa protokolima koji nisu dostupni za šire tržište. Ovdje se primat daje na poboljšanju bezbjednosti, funkcionalnosti i performansi sistema, dok su drugi faktori kao što je jednostavna i jeftina proizvodnja hardvera, mala potrošnja električne energije, skalabilnost i široka dostupnost ostavljeni po strani. Trenutni cilj naučne zajednice je omogućavanje masovne primjene WSNs u široj industriji i potrošačkom tržištu, tako što će se smanjiti troškovi razvoja, proizvodnje i održavanja senzorskih mreža [13], *Slika 2.5*. Razvoj u oblasti CMOS (engl. *Complementary metal–oxide–semiconductor*) poluprovodničkih komponenti, mrežnih protokola i različitih tehnologija skladištenja električne energije, doprinose smanjenu cijena senzora i poboljšanu njihove efikasnosti i funkcionalnosti. Jedan od glavnih pokretača razvoja WSNs je koncept IoT, gdje se više različitih fizičkih objekata, vozila, zgrada i drugih stvari sa ugrađenim elektronskim komponentama i softverom međusobno umrežavaju.



Slika 2.5 Pregled tržišta WSNs sa padom prosječnih cijena senzora

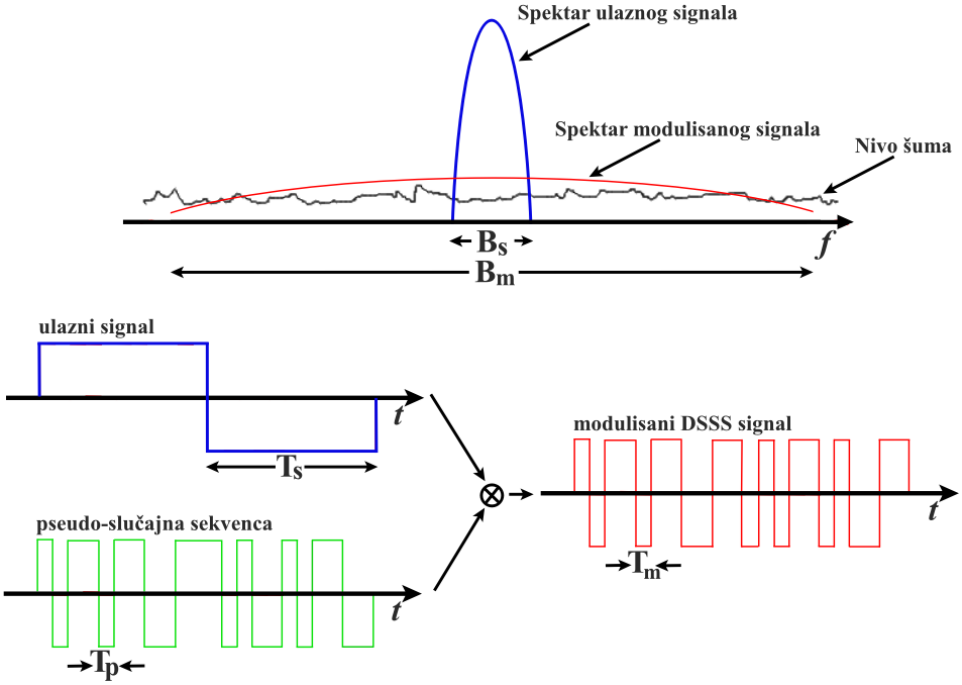
Mogućnosti primjene WSNs su veoma velike. Aktuelna su istraživanja za primjenu i razvoj protokola u oblastima kao što su: zdravstvo, automobilska industrija i saobraćaj, istraživanje i eksploatacija nafte i gasa, poljoprivreda, vazduhoplovstvo, vojna industrija i drugo. Zbog širokog spektra primjene, WSNs moraju ispuniti različite zahtjeve, kao što su energetska efikasnost i pouzdanost mreže, malo kašnjenje, niska cijena, sigurnost, distribuirana obrada podataka i drugo [14].

2.2. IEEE 802.15.4e *Time Slotted Channel Hopping*

IEEE 802.15.4e standard [15] je objavljen 2012. godine, kao dopuna na nivou linka za IEEE 802.15.4-2011 standard. IEEE 802.15.4e ima za cilj razvoj jeftine i jednostavne radio komunikacije, koja koristi malu količinu energije za rad. Tehnika TSCH se kombinuje sa IEEE 802.15.4 standardom, kako bi se postigla bolja energetska efikasnost i pouzdanost. Osnovni princip rada TSCH tehnike je kombinovanje vremenskog multipleksa (engl. *Time Division Multiple Access* – TDMA) za izbjegavanje kolizije, sa promjenama frekvencije kanala pri svakom vremenskom slotu (engl. *Channel hopping*), koje se izvršava po pseudo-slučajnom rasporedu, i na taj način se povećava otpornost na MPF i eksternu interferenciju, [16], [17]. MPF izaziva brze fluktuacije amplitude radio signala na mjestu prijema u toku kratkog vremenskog intervala, ili duž malog pređenog rastojanja, ako je senzor mobilan. TDMA slotovi su dovoljno veliki (obično 10 ms), tako da je moguće slanje najdužeg paketa od 127 bajta, prijem potvrde o dospijeću, obrada podataka i izvršavanje sigurnosnih provjera

na senzorskim čvorovima. Dužina vremenskih slotova nije definisana standardom, već se može podešavati u zavisnosti od aplikacije za koju se koristi. Serija vremenskih slotova koji se ponavljaju naziva se *slotframe.*

IEEE 802.15.4 standard definiše primjenu direktne sekvence proširenog spektra (engl. *Direct-sequence spread spectrum* – DSSS), gdje se ulazni signal množi se pseudo-slučajnom sekvencom, znatno veće učestanosti nego što je učestanost signala koji se prenosi, *Slika 2.6*. Pošto su promjene pseudo-slučajne sekvence brze ($T_s \gg T_p$), spektar modulisanog signala se širi ($B_m \gg B_s$), pa je maksimalna frekvencija signala nakon množenja sa pseudo-slučajnom sekvencom značajno veća nego maksimalna frekvencija u spektru ulaznog signala. Na ovaj način poboljšava se otpornost na smetnje lokalizovane u uskom dijelu spektra i omogućava se pristup većeg broja korisnika. IEEE 802.15.4g uvodi ortogonalno frekvencijsko multipleksiranje (engl. *Orthogonal frequency-division multiplexing* – OFDM), gdje se signal dijeli i prenosi paralelno preko više frekvencijski ortogonalnih podnosilaca. Ovom metodom se kod IEEE 802.15.4g standarda omogućava se prenos paketa veličine do 2047 bajta.



Slika 2.6 Prikaz ulaznog i modulisanog signala u frekvencijskom i vremenskom domenu za DSSS tehniku

Svi čvorovi u TSCH *multi-hop* mrežama su sinhronizovani na nivou vremenskog slota. Sinhronizacija se odvija prilikom komunikacije između senzorskog čvora i njegovog susjeda, prema kome se on sinhronizuje. Sinhronizacija se može vršiti prilikom razmjene

paketa, ili potvrde o prijemu (engl. *Acknowledgment* – ACK), kada se vrši provjera i podešavanje lokacije vremenskog slota, kako bi čvorovi bili što preciznije sinhronizovani.

TSCH funkcioniše na nivou linka. Na ovaj način su omogućene različite optimizacije, kako bi rad sa višim nivoima koji koriste Internet protokol verzije 6 (engl. *Internet Protocol version 6* – IPv6) za LLN (engl. *Low-Power and Lossy*) mreže bio jednostavniji. TSCH ne definiše način rutiranja *muti-hop* paketa, za ovo su zaduženi protokoli rutiranja kao što je RPL (engl. *IPv6 Routing Protocol for Low-Power and Lossy Networks*), [18]. Signalizacioni paketi se koriste za detekciju susjednih čvorova, praćenje mrežne topologije, konfiguraciju IP adresa i drugo.

Da bi se omogućio pravilan rad IPv6 u kombinaciji sa IEEE 802.15.4e standardom, IETF je razvio 6TiSCH protokol.

2.3 6TiSCH protokol

IETF u posljednjih desetak godina radi na razvoju protokola koji će omogućiti korišćenje Internet protokola (IP) za hardverski jednostavne uređaje, koji će se koristiti u IoT aplikacijama. 6TiSCH protokol je rješenje prvenstveno namijenjeno za povećanje pouzdanosti i energetske efikasnosti WSNs, radi ispunjenja komunikacionih zahtjeva u različitim industrijskim aplikacijama, kao što je nadzor i kontrola proizvodnih procesa. Podrazumijeva korišćenje IPv6, kao i primjenu TSCH tehnike promjene kanala pri svakom vremenskom slotu iz skupa od 16 ortogonalnih frekvencijskih nosilaca. Cilj ovog "frekvencijskog skakanja" je smanjenje štetnog uticaja MPH, kolizije i eksterne interferencije [19]. 6TiSCH radna grupa je imala za cilj kreiranje posebnog režima rada senzorskog čvora, nazvanog *minimal mode*. Ovaj režim definiše osnovne protokole koji se moraju koristiti kako bi se omogućio funkcionalan rad mreže. Svi uređaji za koje je navedeno da podržavaju 6TiSCH protokol, moraju imati mogućnost pokretanja ovog režima rada.

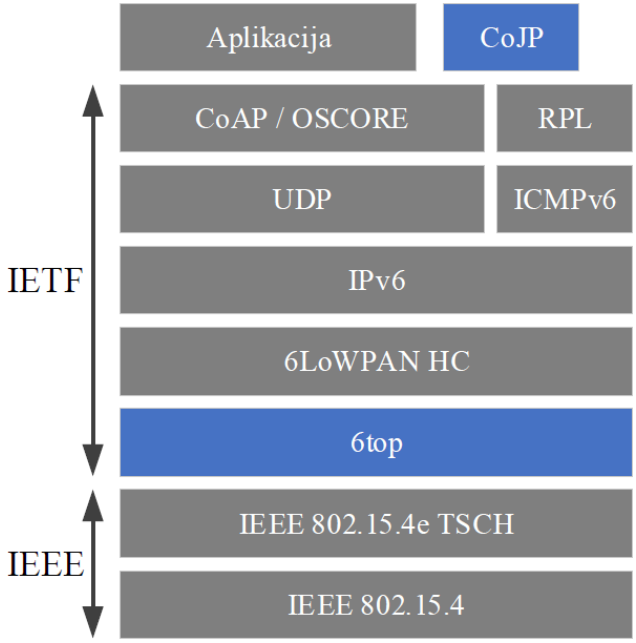
2.3.1. 6TiSCH mrežna arhitektura

6TiSCH mrežna arhitektura treba da omogući rutiranje u centralizovanim, distribuiranim ili kombinovanim senzorskim mrežama kako bi omogućio rad različitih IoT aplikacija. Ova mrežna arhitektura zasniva se na uvođenu novog nivoa nazvanog 6top (engl. *6TiSCH Operation Sublayer Protocol*) [20], [21]. Ovaj dodatni nivo radi iznad IEEE 802.15.4e TSCH nivoa linka i koristi njegove performanse. Viši nivoi koriste IoT protokole za jednostavne senzore, kao što su 6LoWPAN (engl. *IPv6 over Low-Power Wireless*

Personal Area Networks), IPv6, RPL i CoAP (engl. *Constrained Application Protocol*) i drugi.

6TiSCH definiše način povezivanja novih čvorova u mrežu. Vrši se sigurnosna kontrola koja podrazumijeva autorizaciju i autentifikaciju, prije povezivanja na mrežu. Ovu kontrolu vrši CoJP protokol (engl. *Constrained Join Protocol*).

6TiSCH *protocol stack* je prikazan na *Slici 2.7*. Protokoli koje je razvila 6TiSCH radna grupa su označeni plavom bojom. Čitav *protocol stack* je razvijen u okviru OpenWSN projekta [22].

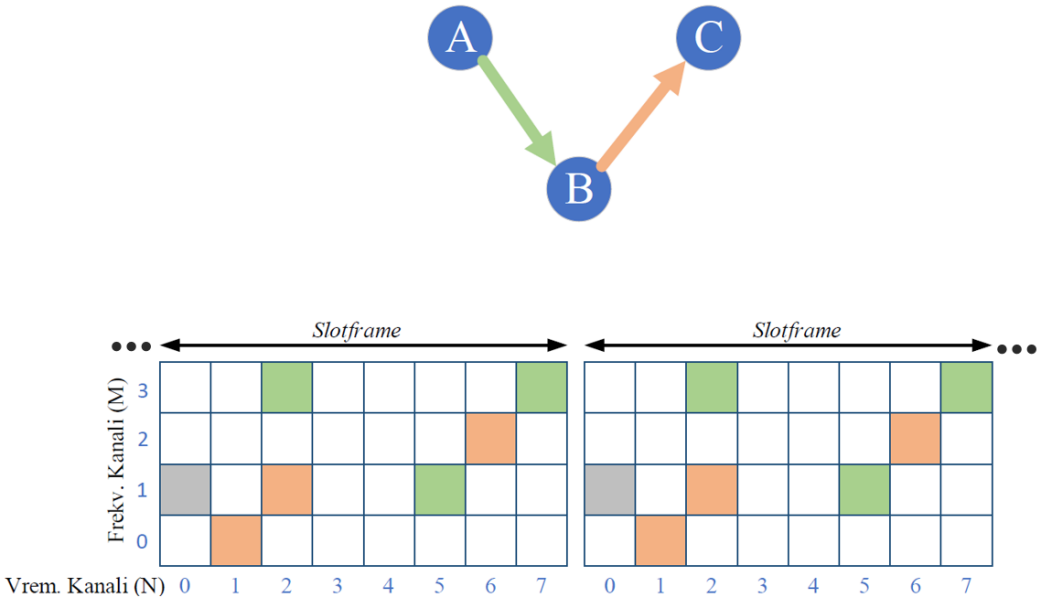


Slika 2.7 6TiSCH protocol stack

6top je specijalni nivo koji je uveden u 6TiSCH okruženje. Sastoji se od 6P protokola i jedne ili više funkcija raspoređivanja (engl. *Scheduling Function* - SF). 6P omogućava dodavanje, brisanje ili pomjeranje vremensko-frekvencijskih ćelija iz matrice raspoređivanja, *Slika 2.8*. Alociranje ćelija se pokreće kada jedan od senzorskih čvorova ima potrebu promjene trenutnog rasporeda komunikacije sa nekim od svojih susjeda. Može se odvijati u dva ili tri koraka, nakon čega oba senzorska čvora moraju promijeniti svoje matrice raspoređivanja. Alokacija u dva koraka se vrši kada čvor *A* zahtijeva otvaranje linka ka čvoru *B* i sam bira ćelije koje čvor *B* u svom odgovoru potvrđuje, dok se alokacija u tri koraka vrši kada čvor *A* inicira povezivanje, čvor *B* „ponudi“ ćelije na kojima će se vršiti komunikacija, a čvor *A* u svom odgovoru potvrđuje predložene ćelije. 6P protokol pri alokaciji ćelija može imati sledeće akcije [23]:

1. Dodavanje novih ćelija u matricu – Izvršavanje komande *ADD;*
2. Brisanje ćelija – Izvršavanje komande *DELETE;*
3. Preseljenje ćelije – Izvršava se komanda *RELOCATE* i ćelija mijenja svoje mjesto u matrici raspoređivanja;
4. Brojanje dostupnih ćelija – Izvršava se komanda *COUNT*, koja vraća broj ćelija koje su dostupne za komunikaciju između dva čvora;
5. Pregled dostupnih ćelija – Izvršava se komanda *LIST*, koja vraća lokacije svih ćelija koje su dostupne za komunikaciju;
6. Brisanje rasporeda – Izvršava se komanda *CLEAR*, koja briše sve trenutno dostupne ćelije za komunikaciju;
7. Signalna poruka – Omogućava pokretanje komunikacije između funkcija raspoređivanja na dva senzorska čvora;

SF odlučuje da li senzor vrši slanje, osluškivanje i prijem, ili se nalazi u uspavanom režimu (engl. *sleep mode*) uštede energije. Raspoređivanje se može predstaviti u vidu matrice *M*×*N*, gdje je *M* broj dostupnih frekvencijskih kanala, a *N* je broj vremenskih slotova u *slotframe*-u, *Slika 2.8.* Svaki element matrice predstavlja jedinstvenu vremensko-frekvencijsku ćeliju, koja definiše vrijeme i frekvenciju komunikacije između dva čvora. Apsolutni broj slota (engl. *Absolute Slot Number* – ASN) predstavlja broj vremenskih slotova koji su se izvršili od kada je počeo rad mreže.



Slika 2.8 Primjer TSCH matrice raspoređivanja za WSN sa tri senzorska čvora (A, B i C), koji koriste četiri kanala za komunikaciju i osam vremenskih slotova

Na *Slici 2.8,* sivom bojom predstavljane su ćelije koje služe za kontrolu i uspostavljanje komunikacije pri inicijalizaciji mreže. Narandžastom bojom predstavljen je usmjereni link između čvorova *A* i *B,* a zelenom bojom predstavljene su ćelije za komunikaciju čvora *B* ka čvoru *C*. Upravljanje matricom raspoređivanja može biti centralizovano ili distribuirano. Važno je obezbijediti dovoljno komunikacionih ćelija kako bi rad mreže bio efikasan. Kod centralizovanog pristupa se koristi funkcija Element Proračuna Putanje (engl. *Path Computation Element* – PCE) koja prikuplja informacije o mreži i prati zahtjeve za povezivanje pojedinačnih čvorova. Na ovaj način je dostupan širi pogled na mrežu uz pomoć kojeg se kreira matrica raspoređivanja, tako da svi čvorovi dobiju dovoljan broj komunikacionih ćelija kako bi mreža radila ispravno. Distribuirani pristup podrazumijeva postepeno otvaranje pojedinačnih linkova između čvorova, koje zavisi od potreba aplikacija koje se pokreću na njima.

Primjer dvije funkcije raspoređivanja, *Minimal Scheduling Function* i *Scheduling Function Zero* je predstavljen u [24].

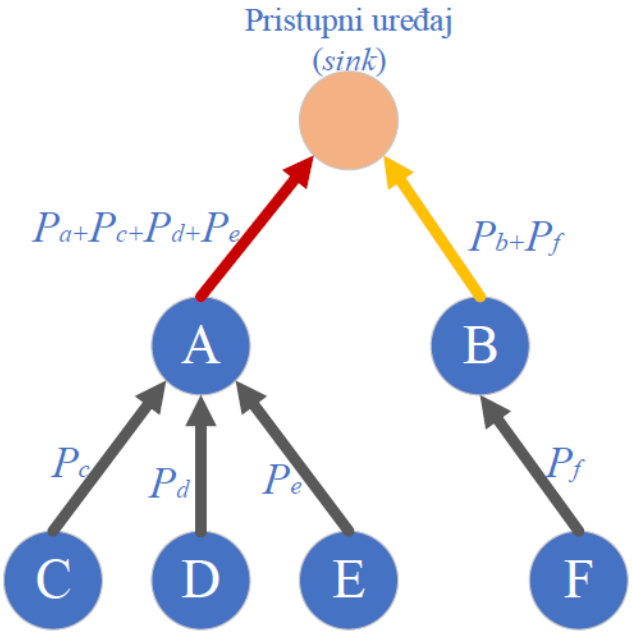
Minimal Scheduling Function (MSF) je distribuirani tip funkcije raspoređivanja koja je definisana za 6TiSCH mreže. MSF pored raspoređivanja definiše i način priključivanja novih čvorova u mreži, koje se vrši u sedam koraka. Nakon što se senzorski čvor uspješno priključi mreži, on je sinhronizovan, izvršena je autentifikacija, dodijeljen mu je jedan roditeljski čvor i definisana je ćelija za komunikaciju ka svakom susjednom čvoru u mreži. Nakon ovoga, čvor može vršiti sve akcije koje su dostupne u okviru 6P protokola.

Svi čvorovi koji koriste MSF moraju u svojim matricama raspoređivanja imati ćeliju zvanu *minimal cell,* koja se uvijek nalazi u prvom vremenskom slotu. Ova ćelija, koju koriste svi čvorovi u mreži, omogućava razmjenu signalizacionih paketa u koje spadaju EB (engl. *Enhanced Beacon*) i DIO (engl. *DODAG Information Objects*). Na ovoj komunikacionoj ćeliji paketi se razmjenjuju između svih čvorova u mreži (engl. *Broadcast*), pa postoji veća mogućnost da dođe do kolizije. Za izbjegavanje kolizije koristi se CSMA/CA mehanizam (engl. *Carrier Sense Multiple Access Collision Avoidance*). Svaki čvor u mreži inicira *unicast* ćelije ka svim svojim susjedima, pri čemu se izbjegava prvi vremenski slot, kako bi se smanjila vjerovatnoća da dođe do kolizije sa *minimal* ćelijama.

Scheduling Function Zero (SF0) je decentralizovani tip funkcije raspoređivanja koja vrši dodavanje ili uklanjanje komunikacionih ćelija, tako da svi čvorovi u mreži mogu nesmetano raditi. Zahtijevani prenos podataka se računa na osnovu *Bandwidth Estimation* algoritma koji koristi parametar o broju potrebnih ćelija (engl. *requiredCells*). SF0 koristi i

parametar SF0THRESH koji kontroliše maksimalan broj ćelija koje se mogu dodijeliti svakom čvoru. Pošto funkcija slučajnim izborom odabira ćelije za komunikaciju, bez podataka o svim čvorovima u mreži, više senzora može odabrati iste ćelije što može dovesti do kolizije. SF0 može detektovati koliziju i izvršiti zamjenu pozicije ćelija [25].

Osnovni režim rada (engl. *Minimal mode*) 6TiSCH protokola omogućava osnovne funkcionalnosti mreže. Međutim, postoje određeni nedostaci posebno prilikom sinhronizacije u mreži [26] i RPL rutiranja [27]. Da bi se omogućio efikasniji rad mreže i veći protok, moraju se primijeniti određena unaprjeđenja [28]. Kašnjenje i gubici paketa se dešavaju u *multi-hop* mrežama na čvorovima koji imaju veliki broj susjeda, a koji preko njih komuniciraju sa pristupnim *sink* čvorom, *Slika 2.9*.



Slika 2.9 Primjer multi-hop mreže

Na *Slici 2.9* crvenom bojom označen je primjer preopterećenog linka između čvora *A* i pristupnog uređaja. Čvorovi C, D i E svoje pakete prosljeđuju *multi-hop* komunikacijom preko čvora *A* ka pristupnom uređaju. Link između čvora *A* i pristupnog uređaja, pored svog paketa, treba da prenese i pakete od čvorova C, D i E. Da bi se spriječilo kašnjenje i gubici, ovakvi linkovi moraju da dobiju veći protok tj. dodatne ćelije za komunikaciju. Jedan od predloga za rješavanje ovog problema je i agregacija tj. spajanje paketa [29]. U većini slučajeva, korisni dio paketa je značajno manji od maksimalne dužine koju je moguće prenijeti u jednom vremenskom slotu. U ovakvim situacijama paket nije optimalno

iskorišćen, zbog toga se primjenjuje agregacija paketa. Kada čvor *A* primi pakete od čvorova C, D ili E koji su niži u hijerarhijskoj strukturi mreže sa *Slike 2.9*, vrši se spajanje korisnih dijelova svih paketa u jedan zajednički paket, koji se prosljeđuje ka višem nivou u mreži, u ovom slučaju pristupnom uređaju. Ova metoda se može primjenjivati u mrežama u kojima je korisni dio paketa u najvećem broju slučajeva manji od maksimalne veličine. Na ovaj način se povećava protok podataka i smanjuju se gubici, ali se u isto vrijeme povećava kašnjenje usljed agregacije, kada se čekaju paketi koji će se koristiti za kreiranje zajedničkog paketa za prenos [30].

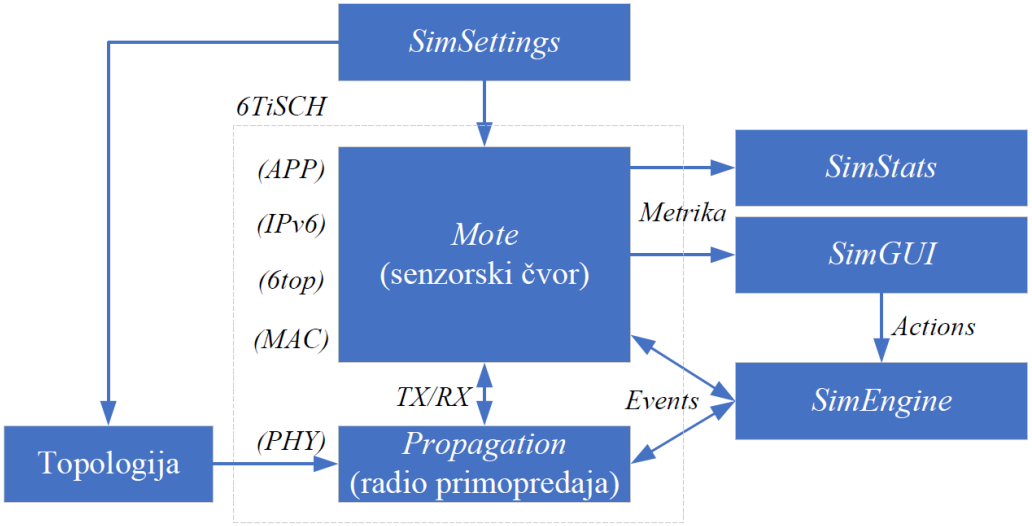
Glava 3

3. Modelovanje 6TiSCH mreža

3.1. 6TiSCH Simulator

Računarske simulacije predstavljaju moćan alat koji značajno može doprinijeti brzini i kvalitetu razvoja telekomunikacionih mreža, a posebno WSNs u kojima se koristi veliki broj senzorskih čvorova koji međusobno komuniciraju. WSNs je teško eksperimentalno testirati u realnim okruženjima, zbog potrebe za velikim brojem senzora i kreiranjem različitih scenarija u kojima se ove mreže mogu koristiti. Simulaciona metoda omogućava brže dobijanje rezultata nego eksperimentalna, zbog jednostavnosti, prilagodljivosti i brzine rada simulacionih alata. Pored toga, simulaciona metoda omogućava testiranje rada mreže u zavisnosti od različitih ulaznih parametara, koji se mogu prilagođavati dok se ne postignu željene performanse. Zatim se podešeni parametri mogu prenijeti u realna mrežna okruženja, kako bi se eksperimentalno potvrdili rezultati iz simulacione analize.

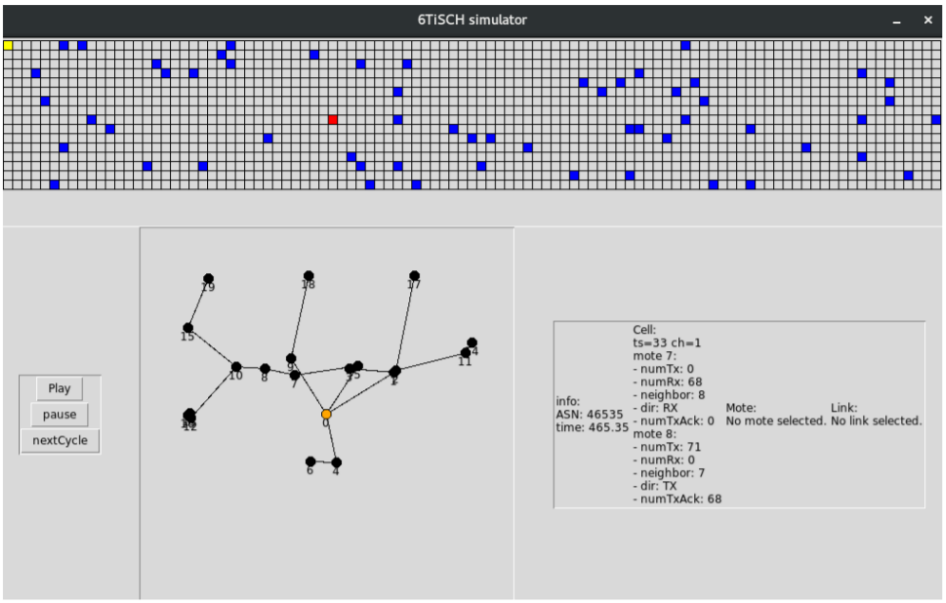
6TiSCH Simulator je simulator diskretnih događaja (engl. *Discrete Event Simulator* – DES), koji je napisan u programskom jeziku Pajton (engl. *Python*). DES je sistem koji se modeluje tako da se stanja mijenjaju u diskretnim vremenskim trenucima. Događaji predstavljaju trenutne pojave koje mijenjaju stanje sistema. 6TiSCH Simulator ne modeluje fizičke osobine sistema koje se mogu ispitivati samo u stvarnom okruženju kao što su: greške u sinhronizaciji zbog nepreciznosti kristalnih oscilatora, greške na pojedinačnim bitima tokom prenosa i kašnjenje usljed nesavršenosti elektronskih komponenti. Fokus je stavljen na modelovanje mreže na nivou linka, i izvršena je apstrakcija protoka vremena, tako da je ono podijeljeno na TSCH vremenske slotove, kao i apstrakcija poruka, tako da se prenose samo parametri koji su značajni za rad protokola. Sa ove dvije apstrakcije omogućeno je praćenje rada SF, ispitivanje uticaja mrežne topologije na protokole rutiranja, praćenje rada 6P protokola u situacijama kada dolazi do grešaka na nivou linka i praćenje rada aplikacije i njen uticaj na niže mrežne nivoe. Simulacija se može pokretati paralelno na više jezgara, gdje je testom potvrđen uspješan rad na 56 jezgara. Simulator je napisan na oko 8000 linija, a čini ga 6 osnovnih fajlova i grafički interfejs [31]. Šematski prikaz simulatora se nalazi na *Slici 3.1.*



Slika 3.1 Šematski prikaz 6TiSCH Simulatora

Glavna komponenta simulatora je objekat *Mote*, koji modeluje senzorski čvor, u kome je najveći dio 6TiSCH protokola implementiran. Kroz *SimSettings* blok se vrši konfigurisanje simulatora podešavanjem različitih parametara, koje korisnik može da mijenja. *Mote* generiše izlazne podatke (*Metrika*) za blokove *SimStats* i *SimGUI*, i definiše diskretne događaje (*Events*), koje obrađuje i pokreće blok *SimEngine*. Akcije koje se tiču radio primopredaje se prosljeđuju bloku *Propagation*, koji na osnovu topologije vrši obradu ovih akcija.

Simulator omogućava prikaz matrice raspoređivanja i mrežne topologije u grafičkom interfejsu, *Slika 3.2.*



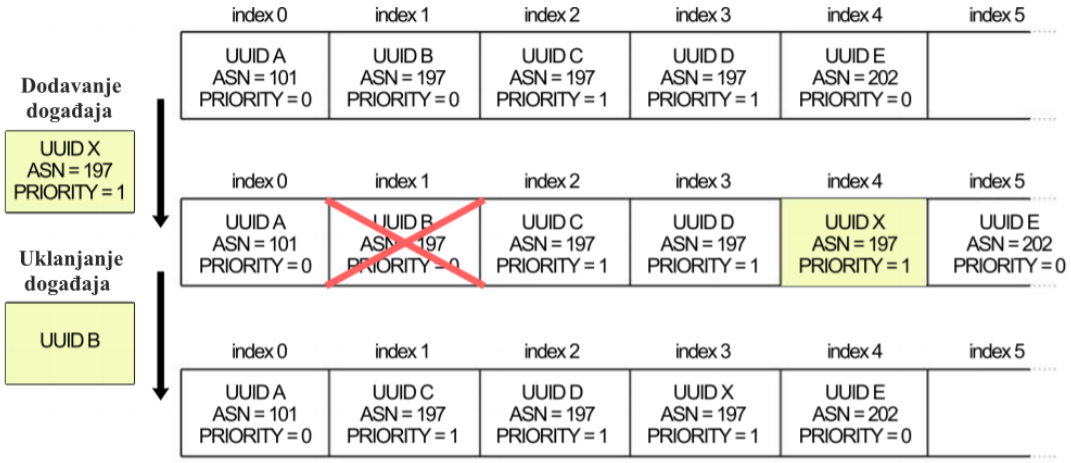
Slika 3.2 Grafički interfejs 6TiSCH Simulatora

Preko grafičkog interfejsa simulacija se može pokretati, pauzirati, može se pratiti trenutno stanje matrice raspoređivanja na svim čvorovima, i različiti podaci o čvorovima, linkovima i vremensko-frekvencijskim ćelijama iz matrice raspoređivanja. Simulacije se mogu pokretati i u autonomnom režimu bez grafičkog interfejsa. U ovom režimu, izlazni podaci se dobijaju preko *log*-fajlova i grafike, koji se automatski generišu nakon završetka simulacije [31].

SimEngine blok

Glavni modul koji prati sve događaje u simulatoru je *SimEngine*. Događaji koji treba da se pokrenu se generišu u *Mote* modulu. Svaki događaj ima svoj prioritet i označen je jedinstvenom brojnom oznakom nazvanom UUID. Događaji se smještaju u Pajton listu nazvanu *Future Event Set* (FES), i izvršavaju se po ASN-u i dodijeljenom prioritetu. Ako dva događaja imaju isti ASN i isti prioritet izvršavanja, tada prednost ima onaj događaj koji je prvi stigao u FES listu. Nije moguće dodavanje ili uklanjanje novih događaja u ASN koji se u tom trenutku izvršava.

Na *Slici 3.3*, prikazan je primjer dodavanja i uklanjanja događaja u FES listu. Prilikom dodavanja novog događaja sa UUID oznakom X na ASN-u 197 i prioritetom 1, funkcija prolazi kroz FES listu dok ne dođe do događaja sa većim ASN-om ili događaja sa istim ASN-om i manjim prioritetom od novog događaja, na tom mjestu se vrši njegovo dodavanje. Uklanjanje događaja sa UUID oznakom B na ASN-u 197 se vrši prolaskom kroz listu dok se ne dođe do traženog događaja, kada se isti uklanja i desni ostatak liste se pomjera za jedno mjesto ulijevo.



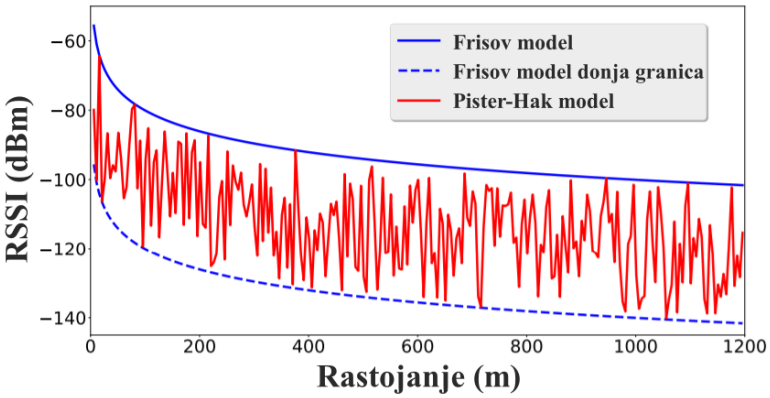
Slika 3.3 Primjer dodavanja i uklanjanja događaja iz FES liste 6TiSCH Simulatora

Topologija

Kako bi se spriječio uticaj mrežne topologije na rad mreže, prilikom svake simulacije generiše se nova slučajna topologija. Kroz ulazne parametre, korisnik može definisati broj senzorskih čvorova i fizički prostor koji mreža zauzima. Senzori se postavljaju na slučajne lokacije, ali tako da svaki senzor ima stabilan radio link sa izabranim brojem susjednih čvorova. I ovi ulazni parametri se mogu podešavati. Pored slučajne *mesh* topologije dostupna je i linearna i zvijezda topologija.

Propagacioni model

Simulator koristi Pister-Hak propagacioni model, koji vraća RSSI (engl. *Received Signal Strength Indicator*) vrijednost na svim radio linkovima u mreži. Ove vrijednosti se dobijaju kada se uniformna varijansa od 40 dB oduzme od Frisovog modela [32]. Nakon toga RSSI se prevodi u PDR vrijednosti, po tabeli koja je dobijena eksperimentalnim rezultatima. Ova tabela precizno definiše odnos RSSI-PDR u velikim industrijskim okruženjima, na opsegu od 2.4 GHz. Pister-Hak propagacioni model i RSSI-PDR konverziona tabela su prikazani na *Slici 3.4.*



RSSI	PDR
-97 dBm	0.0000
-96 dBm	0.1494
-95 dBm	0.2340
-94 dBm	0.4071
-93 dBm	0.6359
-92 dBm	0.6866
-91 dBm	0.7476
-90 dBm	0.8603
-89 dBm	0.8702
-88 dBm	0.9324
-87 dBm	0.9427
-86 dBm	0.9562
-85 dBm	0.9611
-84 dBm	0.9739
-83 dBm	0.9745
-82 dBm	0.9844
-81 dBm	0.9854
-80 dBm	0.9903
-79 dBm	1.0000

Slika 3.4 Pister-Hak propagacioni model sa pratećom tabelom za RSSI-PDR konverziju

Simulator određuje da li je radio prenos uspješan, na osnovu PDR vrijednosti i slučajno dobijenog decimalnog broja od 0 do 1, koji se sa njom upoređuje. Ako je slučajno dobijeni broj manji od PDR vrijednosti, prenos je uspješan i obrnuto. Interferencijom se smatraju svi signali koji dolaze od susjednih čvorova na istim kanalu i istom vremenskom slotu. RSSI vrijednosti ovih signala se dodaju šumu, kako bi se dobio odnos signal-(interferencija+šum) (engl. *Signal-to-Interference-Plus-Noise Ratio* – SINR), na osnovu koga

se računa nova (umanjena) PDR vrijednost, koja se upoređuje sa pomenutim slučajnim brojem od 0 do 1.

Model potrošnje energije

Model potrošnje električne energije posmatra različite tipove vremenskih slotova i na osnovu trajanja radio prenosa ili osluškivanja, količine prenesenih podataka, brzine prenosa i rada procesora, računa se ukupna energija potrebnu za rad senzora [33]. Nakon završetka vremenskog slota, proračunava se iskorišćena energija. Količina utrošene električne energije za svaki tip vremenskog slota je podešena tako, da se simulira upotreba *OpenMote-CC2538* senzorskog uređaja. Ove parametre je moguće mijenjati i prilagođavati upotrebi drugih senzorskih čvorova.

Mote blok

Kroz *Mote* blok je izvršena apstrakcija senzorskog čvora. Pri pokretanju simulacije vrši se inicijalizacija mreže, u kojoj se kreira poseban *Mote* objekat za svaki čvor u mreži. Jedan od čvorova postaje *root* čvor, koji ima zadatak da pokrene formiranje mreže tako što će periodično slati EB i RPL DIO pakete za signalizaciju, dok ostali čvorovi u mreži vrše osluškivanje na slučajno odabranom radio kanalu. *Root* čvor vrši slanje samo tokom *minimal* ćelije, dok ostali čvorovi vrše slanje ili prijem po svojim matricama raspoređivanja. U svakom slotu, propagacioni model vrši provjeru koji su čvorovi izvršili prenos, a koji osluškuju.

Kada neki od čvorova primi EB paket, vrši se sinhronizacija i počinje proces pristupanja mreži [34]. Nakon što se čvor priključi mreži kroz *Join Proxy* [35] proces, on može primati DIO poruke koje mu omogućavaju da izabere svoj roditeljski (engl. *Parent*) čvor, i odredi ćeliju za komunikaciju sa njim.

Svaki podnivo u *Mote* bloku se može podešavati kroz *SimSettings* blok. Na primjer, moguće je podešavati veličinu TSCH frejma, *timeout* vrijeme, trajanje vremenskih slotova, EB perioda, itd. 6top nivo i funkcija raspoređivanja MSF se mogu prilagođavati promjenom različitih parametara kao što je MAX_NUMCELLS, LIM_NUMCELLSUSED_LOW, HOUSEKEEPINGCOLLISION_PERIOD, itd. Generisanje mrežnog saobraćaja u simulatoru može biti konstantno ili promjenljivo. Kod promjenljivog generisanja saobraćaja, moguće je modelovati različite raspodjele i generisati velike količine paketa u kratkim vremenskim intervalima.

Metrika

Simulator omogućava uvid u preko 50 izlaznih parametara, a jednostavno je implementirati i nove metrike. Promjene različitih parametara se mogu pratiti na nivou svakog TSCH slota, ili kao apsolutne vrijednosti nakon završetka simulacije. Apsolutne vrijednosti parametara (npr. količina utrošene električne energije) se mogu pratiti za pojedinačne čvorove u mreži, ili za cjelokupnu mrežu. RSSI vrijednosti za svaki radio link su dostupne u *log* fajlu. U 6TiSCH Simulator su dodate i posebne skripte, koje olakšavaju obradu dobijenih podataka i crtanje različitih grafika.

3.2. *Trace-based* 6TiSCH simulacije

Jedan od glavnih nedostataka analize bežičnih mreža simulacionom metodom je potreba za korišćenjem različitih radio propagacionih modela, koji ne mogu precizno modelovati nepredvidljive fenomene pri prostiranju radio talasa, kao što je uticaj MPF. Zbog nepreciznog modelovanja radio kanala, rezultati simulacione analize se mogu značajno razlikovati od rezultata iz stvarnog okruženja. Iz tog razloga je predstavljeno rješenje koje simulatoru omogućava korišćenje matrice konektivnosti iz stvarnog okruženja, koje su snimljene u eksperimentalnim *testbed* platformama, ili realnim mrežnim okruženjima [36]. Dva alata koja omogućavaju prikupljanje matrica konektivnosti su *OpenTestbed* i *Mercator*.

OpenTestbed [37], je specijalna platforma sa otvorenim kodom, koja omogućava jednostavno konfigurisanje *testbed* okruženja uz pomoć *Raspberry Pi single-board* računara i *OpenMote B* [38] senzorskih čvorova. Na *Slici 3.5* je prikazan *OpenTestbed* čvor nazvan *OTBox*, kojeg čini jedan *Raspberry Pi* računar koji kontroliše četiri senzorska uređaja *OpenMote B*. *Raspberry Pi* je serijskom vezom povezan sa senzorima, dok se preko Wi-Fi konekcije na 5 GHz vrši njegova kontrola. Glavna komponenta ovog rješenja je Pajton program *otbox*, koji se pokreće na *Raspberry Pi* računaru koji preko korisničkog interfejsa i MQTT konekcije omogućava kontrolu i praćenje rada senzorskih čvorova. Na ovaj način je omogućeno jednostavno mijenjanje *firmware*-a koji se nalazi na senzorskim čvorovima, kao i pristup njihovim izlaznim podacima.

Slika 3.5 OpenTestbed OTBox

Mercator [39] je softversko rješenje koje omogućava proračun PDR vrijednosti na radio linkovima u WSNs. *Mercator* se može pokretati na *OpenTestbed* platformi ili na drugim *testbed* platformama kao što je npr. FIT IoT-LAB [40]. *Mercator* se sastoji od *firmware*-a i *software*-a. *Firmware* se pokreće na svim senzorskim čvorovima, a prateći *software* na računaru koji kontroliše njihov rad putem serijske konekcije. Računar prikuplja podatke o kvalitetu linkova u posmatranoj mreži, tako što vrši razmjenu paketa između svih senzora i računa odnos poslatih i uspješno prenesenih paketa (PDR). Nakon toga se generiše izlazni fajl u K7 formatu koji sadrži podatke o kvalitetu svih linkova iz mreže.

SimEngine blok 6TiSCH Simulatora, koristi klasu nazvanu *Connectivity*, koja definiše matricu konektivnosti za mrežu koja se simulira. Linkovi između svaka dva čvora u mreži su definisani sa parovima PDR i RSSI vrijednosti. Kao što je ranije napomenuto, 6TiSCH Simulator koristi Pister-Hak propagacioni model, koji na osnovu rastojanja između čvorova računa PDR i RSSI vrijednosti. *Trace-based* 6TiSCH simulacija predstavlja upotrebu stvarnih matrica konektivnosti generisanih na osnovu podataka iz fajlova u K7 formatu, koji se dobijaju uz pomoć *Mercator* rješenja. Ovi fajlovi sadrže informacije o kvalitetu linkova između svih čvorova i na svim frekvencijskim kanalima koji se koriste u mreži. Na ovaj način, radio okruženje u simulatoru je identično stvarnom okruženju koje je snimljeno na *testbed* platformama ili realnom mrežnom okruženju.

Glava 4

4. Metode za odabir broja i pozicija za snifere

4.1 Sniferi u višekanalnim WSNs

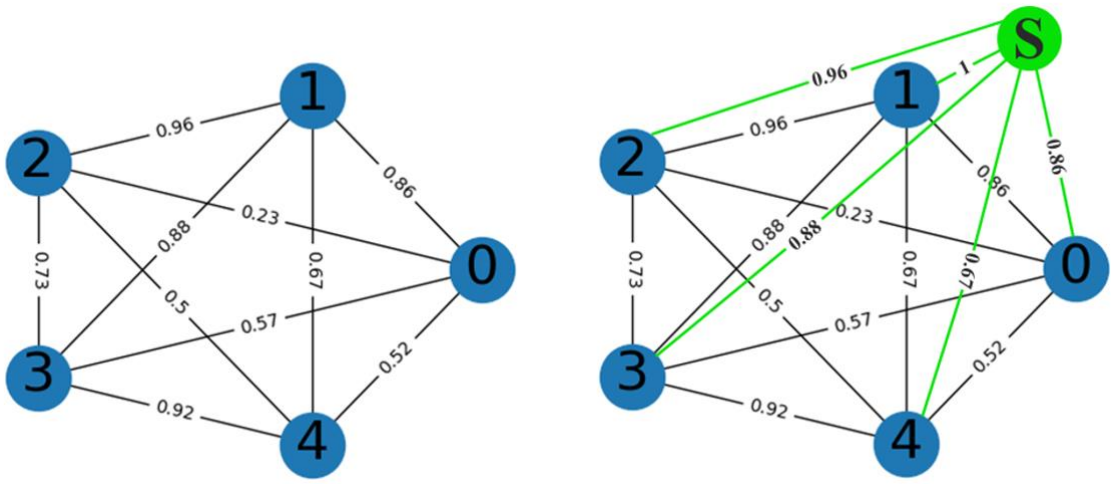
Za analizu rada i performansi WSNs, kao i za razvoj novih standarda i protokola, neophodan je uvid u razmijenjeni paketski saobraćaj. Sniferi su uređaji koji mogu vršiti snimanje i analizu paketskog radio saobraćaja u višekanalnim WSNs. Međutim, da bi sniferi efikasno vršili monitoring u većim WSNs, u kojima jedan snifer ne može snimiti sav saobraćaj zbog prirode radio linkova, ograničene osjetljivosti prijemnika na sniferu, male predajne snage senzora i interferencije, potrebno je definisati broj i pozicije snifera, tako da hvataju što veći procenat saobraćaja. Tokom razmatranja potencijalnih lokacija za snifere u senzorskim mrežama, važno je da svi senzorski čvorovi sa barem jednim sniferom, imaju radio link većeg kvaliteta od definisane minimalne vrijednosti koja će omogućiti hvatanje određenog procenta paketa koje dati senzor šalje.

U nastavku će biti predložene dvije metode za određivanje pozicije, ili broja i pozicije snifera u velikim višekanalnim WSNs. Odabrani sniferi omogućavaju efikasno snimanje mrežnog saobraćaja u višekanalnim WSNs, a sve na osnovu poznatih karakteristika radio linkova između senzora. Prva metoda za određivanje lokacija za snifere se zasniva na upotrebi teorije grafova, a druga na upotrebi teorije vjerovatnoće i kombinatorike. Na osnovu broja senzora u mreži, prostora koji mreža zauzima, kao i karakteristika linkova između senzora, daje se predlog broja i pozicije snifera, kao i procjena koji je procenat paketa moguće snimiti koristeći predloženo rješenje. Takođe će se analizirati i pristup u kojem se na osnovu zadatog broja snifera predlažu pozicije za njihovo postavljanje u WSN, tako da se omogući snimanje što većeg procenta saobraćaja razmijenjenog u mreži.

Metode za odabir pozicija za snifere, koje su predstavljene u radu, kao ulazni parametar koriste matricu konektivnosti posmatrane senzorske mreže na svim kanalima, a kao moguće lokacije za postavljanje snifera razmatraju se samo lokacije senzorskih čvorova. Kada se odabere lokacija za snifer u mreži, cilj je postaviti snifer tako da on bude što bliže senzoru čije je mjesto odabrano. Na ovaj način, postavljeni snifer će imati približno isti kvalitet radio linkova kao i senzor na čijem se mjestu nalazi. Zbog njihove blizine,

komunikacija između snifera i senzora na čijem se mjestu nalazi je ograničena samo internom interferencijom, zato se u pomenutim metodama ovaj link smatra idealnim, sa PDR vrijednosti 1.

Na *Slici 4.1 a)* je šematski prikaz matrice konektivnosti za jedan frekvencijski kanal, u formi grafa. Čvorovi na prikazanom grafu predstavljaju senzorske čvorove u mreži, dok grane predstavljaju radio linkove sa odgovarajućim PDR vrijednostima. Prikazana mreža sadrži pet čvorova i deset neusmjerenih radio linkova koji povezuju sve čvorove. *Slika 4.1 b)* prikazuje matricu konektivnosti nakon dodavanja jednog snifera (čvor sa oznakom S) na lokaciju čvora sa oznakom 1. Snifer gradi linkove istog kvaliteta sa svim susjedima kao čvor na čijem se mjestu nalazi, dok sa senzorskim čvorom 1 gradi idealan link sa PDR vrijednosti 1, jer su snifer i čvor na veoma maloj fizičkoj udaljenosti jedan od drugog.



a) *b)*

Slika 4.1 a) Šematski prikaz matrice konektivnosti u formi grafa za mrežu sa 5 čvorova; b) Šematski prikaz matrice konektivnosti nakon dodavanja jednog snifera u mrežu

6TiSCH protokol za komunikaciju koristi 16 frekvencijskih kanala, pa je tokom analize ovih mreža potrebno razmatrati komunikaciju na svim kanalima. Eksterna interferencija najčešće pogađa samo neke od radio kanala koji se koriste. Wi-Fi mreže utiču na kvalitet komunikacije u IEEE 802.15.4 mrežama [41], zbog široke upotrebe Wi-Fi tehnologije u svim okruženjima i zbog toga što koristi iste frekvencijske opsege na 2.4 GHz kao pomenuti standard. ISM opsege na 2.4 GHz koriste i mnoge druge tehnologije koje mogu izazvati interferenciju u WSNs. Zbog toga se matrice konektivnosti na različitim kanalima, mogu međusobno razlikovati. Predložene metode za odabir broja i pozicija snifera tokom rada vrše analizu matrica konektivnosti na svim kanalima.

4.1.2 *BeamLogic 802.15.4 Site Analyzer*

Jedan od komercijalno dostupnih snifera za višekanalne WSNs je *BeamLogic 802.15.4 Site Analyzer* [42], *Slika 4.2.* Ovaj uređaj omogućava snimanje i analizu saobraćaja u mrežama koje koriste IEEE 802.15.4 standard. *BeamLogic 802.15.4 Site Analyzer* se povezuje sa računarom preko USB konekcije. Na računaru se pokreće specijalizovani softver koji kontroliše rad snifera i omogućava hvatanje paketa i njihovo prikazivanje na *WireShark* analizatoru paketa, kao i čuvanje u *log* fajlovima za kasniju analizu. Omogućeno je paralelno hvatanje paketa na svih 16 kanala na 2.4 GHz, što je neophodno zbog primjene TSCH tehnike. Pored snimanja paketa, ovaj snifer omogućava trenutni prikaz energetskih nivoa (RSSI) na svim kanalima.

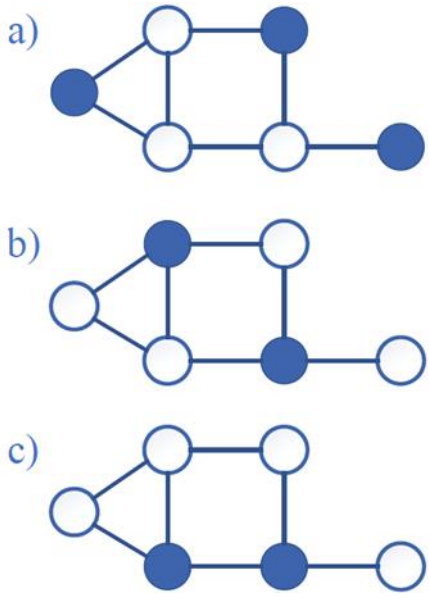
Slika 4.2 BeamLogic 802.15.4 Site Analyzer

4.2 Metoda za odabir broja i pozicija za snifere zasnovana na teoriji grafova

Metoda za odabir broja i pozicija za snifere (u nastavku Metoda I), se zasniva na upotrebi teorije grafova za određivanje lokacija koje su pogodne za postavljanje snifera. Metoda kao ulazni podatak koristi matrice konektivnosti, na svim kanalima koji se koriste u mreži. Kao rezultat, daje se predlog lokacija za postavljanje snifera i izračunava se procenat paketa koje je moguće snimiti sa datim predlogom. Kao potencijalne lokacije, razmatraju se samo pozicije senzorskih čvorova u mreži, jer matrice konektivnosti daju podatke o stanju radio kanala samo za lokacije senzora.

Definicija 1: Dominantan skup (engl. *Dominating Set* – DS) grafa $G = (V, E)$ je podskup $V' \subseteq V$ takav da, za svaki čvor $u \in V \backslash V'$, postoji čvor $v \in V'$, za koji važi da je $(u, v) \in E$. Dominantan skup V' grafa G je minimalan, ako ne postoji podskup skupa V' koji je dominantan skup grafa G.

Za objašnjenje rada Metode I potrebno je uvesti pojmove dominantnog skupa (DS) i minimalnog dominantnog skupa (MDS) iz teorije grafova, Definicija 1. Na *Slici 4.3*, plavom bojom su označeni primjeri dominantnih skupova za prikazani graf. Na *Slici 4.3 b) i c)*, prikazani su DS sa dva čvora, što predstavlja MDS za prikazani graf. Dakle, DS grafa $G = (V, E)$ je podskup V'od V, takav da je svaki čvor iz grafa ili u dominantnom skupu, ili je njegov susjed u dominantnom skupu. MDS je najmanji DS za dati graf. Minimalnih dominantnih skupova u jednom grafu može biti više. Pronalazak dominantnog skupa predstavlja NP-kompletan problem odlučivanja u računarskoj teoriji kompleksnosti, i za sada ne postoji efikasan algoritam koji pronalazi MDS za odabrani graf [43]. NP klasa je klasa svih problema odlučivanja, koji mogu biti riješeni nekim Nedeterminističkim algoritmom za Polinomijalno vrijeme.



Slika 4.3 Dominantni skupovi (boldovani čvorovi) za prikazani graf

Kao što je i ranije pomenuto, pri određivanju lokacija za snifere važno je da svi senzori u mreži budu povezani sa barem jednim sniferom, sa linkom definisanog minimalnog kvaliteta. Pored matrica konektivnosti na svim kanalima, i ovaj podatak se definiše kao ulazni parametar za Metodu I, i nazvan je *sniffer_link_pdr*. Prvi dio Metode I, u kome se obavlja početna kandidatura lokacija za snifere je prikazan na *Pseudokodu 4.1*.

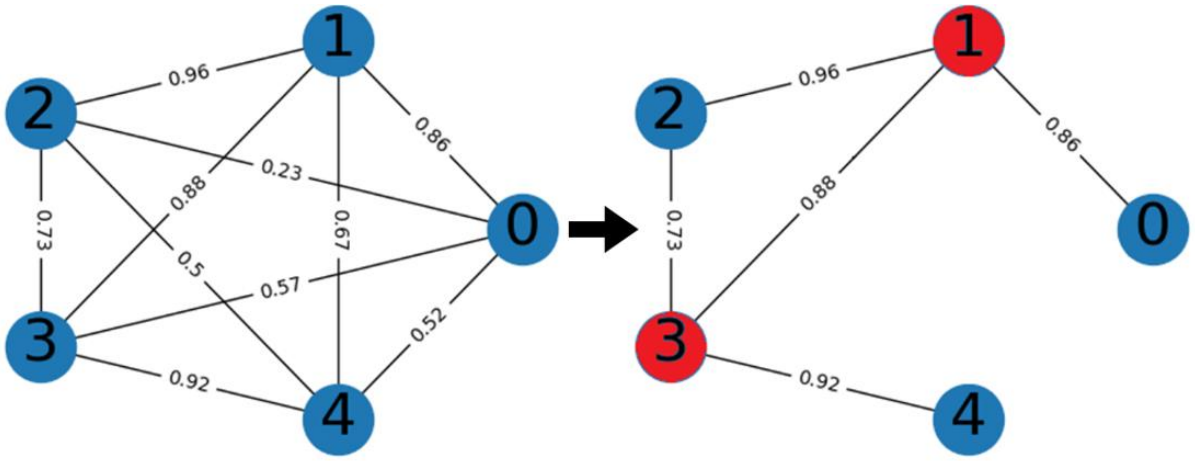
Dio I: Odabir snifera koji pokrivaju čitavu mrežu

Ulaz: Matrice konektivnosti $G_1 ... G_{16}$, sniffer_link_pdr
Izlaz: sniffer_candidates

```
1 sniffer_candidates = empty set
2 for kanal in 1 .. 16 do
      // Graf G_s sadrži linkove kojima je PDR veći od sniffer_link_pdr
3     G_p = napravi_graf(G_kanal, sniffer_link_pdr)
4
5     singleChLoc = min_dominating_set(G_p)
6     sniffer_candidates = sniffer_candidates ∪ singleChLoc
```

Pseudokod 4.1 Prikaz prvog dijela Metode I

Na početku, petlja (linija 2) prolazi kroz sve matrice konektivnosti u formi grafa, i kreiraju se pomoćni grafovi G_p (linija 3), koji sadrže samo one grane (radio linkove) čija je PDR vrijednost veća od vrijednosti ulaznog parametra *sniffer_link_pdr*, *Slika 4.4.* Odabir potencijalnih lokacija za snifere, na jednom kanalu, se vrši tako što se odredi MDS za pomoćni graf G_p i odabrani čvorovi se upišu u promjenljivu *singleChLoc* (linija 5). Zatim se ista funkcija ponavlja na pomoćnim grafovima svih kanala, i vrši se unija predloženih lokacija u promjenljivu *sniffer_candidates*, koja predstavlja izlazni parametar prvog dijela Metode I.



a) *b)*

Slika 4.4 a) Šematski prikaz matrice konektivnosti za mrežu sa pet čvorova; b) Šematski prikaz pomoćnog grafa G_p za vrijednost parametra sniffer_link_pdr = 0.7. Označeni čvorovi (1 i 3) predstavljaju minimalan dominantan skup prikazanog grafa.

Izlazna lista *sniffer_candidates* sadrži sve čvorove koji čine minimalne dominantne setove pomoćnih grafova na svim kanalima. Na ovaj način formirana lista je zasigurno DS za sve pomoćne grafove $G_{p1...}G_{p16}$. Zbog primjene unije na rješenja za pojedinačne kanale,

dobija se predlog lokacija za postavljanje snifera koji u nekim slučajevima može biti uporediv sa brojem senzora u mreži. Predlog velikog broja snifera se dešava u slučajevima kada postoje razlike između matrica konektivnosti, pa se MDS na svakoj od njih međusobno razlikuje. Takođe, predlog velikog broja snifera može biti posljedica aproksimativnosti algoritma koji određuje MDS. Matrice konektivnosti na svim kanalima nisu međusobno potpuno različite, tj. postoji korelacija između matrica konektivnosti na različitim kanalima. Zato se u drugom dijelu Metode I vrši korekcija početnog predloga lokacija za snifere, kako bi se smanjio broj snifera koje treba postaviti u datu mrežu.

Kao ulazni parametar za drugi dio Metode I, koristi se predložena lista *sniffer_candidates,* i parametar *removal_load*, decimalni broj između 0 i 1. Sa parametrom *removal_load* definiše se procenat snifera koji se pokušavaju ukloniti iz početnog predloga *sniffer_candidates.* Ako je ovaj parametar podešen na vrijednost 1, algoritam pokušava ukloniti što više snifera iz početne liste, a da uslov, da svaki senzor u mreži bude povezan sa barem jednim sniferom sa linkom definisanog kvaliteta (*sniffer_link_pdr*) ostane ispunjen. Kada je vrijednost parametra *removal_load* podešena na 0, ne vrši se uklanjanje snifera, već se sve lokacije iz liste *sniffer_candidates* predlažu za lokacije snifera.

Veći broj snifera omogućava snimanje većeg broja paketa i kvalitetniju analizu, ali u isto vrijeme povećava troškove zbog potrebe za dodatnim hardverom. Zbog toga je potrebno optimalno odabrati vrijednosti ulaznih parametara *sniffer_link_pdr* i *removal_load* za mrežu koja se analizira. Matrice konektivnosti imaju značajne sličnosti na većini kanala, i početni predlog (*sniffer_candidates*), koji je dobijen unijom, pokriva iste senzorske čvorove sa više snifera. Neki od ovih snifera mogu biti uklonjeni bez značajnog smanjena pokrivenosti mreže i uticaja na broj paketa koje je moguće snimiti sa datim predlogom.

Drugi dio algoritma u kome se vrši uklanjanje snifera iz početne liste prikazan je u *Pseudokodu 4.2.*

```
Dio II: Smanjenje broja snifera iz početnog predloga
   Ulaz: Pomoćni grafovi G_p1...G_p16, sniffer_candidates,
         removal_load
   Izlaz: reduced_candidates, average_pdr
   // Proračun ciljnog broja snifera
1  target_sniff_num =
   length(sniffer_candidates)*(1-removal_load)
   // Graf G_s sadrži čvorove iz liste sniffer_candidates
2  G_s = make_graph(sniffer_candidates)
3  sniffer_candidates = order_by(sniffer_candidates)
4  for sniffer in sniffer_candidates do
       // Uklanja se jedan čvor iz grafa G_s
5      G_s.remove_node(sniffer)
       // Provjera da li je umanjeni graf i dalje MDS na svim
          kanalima
6      if not is_dominating_set(G_s, G_p1...G_p16) then
           // Vraćanje uklonjenog čvora u graf
7          G_s.add_node(sniffer)
       // Prekida se smanjenje broja snifera kada se dostigne
          željeni broj
8      if length(G_s) ≤ target_sniff_num then
9          break
10 reduced_candidates = nodes from G_s
```

Pseudokod 4.2 Prikaz drugog dijela Metode I

Promjenljiva *target_sniffer_num* definiše broj snifera koji želimo da zadržimo iz početnog predloga *sniffer_candidates*, i izračunava se na osnovu ulaznog parametra *removal_load*. Nakon što se kreira pomoćni graf G_s, koji sadrži sve čvorove iz početnog predloga (*sniffer_candidates*) lokacija za snifere, drugi dio algoritma pokušava da ukloni neke od predloženih lokacija.

Na početku se predložena lista sortira (linija 3) funkcijom *order_by*, po sumi PDR vrijednosti po rastućem redosljedu, *Pseudokod 4.3*. Ova suma predstavlja zbir svih PDR vrijednosti na linkovima koje odabrani čvor (potencijalna lokacija za snifer) povezuju sa svim njegovim susjedima na svim kanalima. Petlje na linijama 2 i 4 prolaze kroz sve predložene sniferske lokacije, a zatim kroz sve čvorove i vrše sumu PDR vrijednosti za svaku predloženu lokaciju. Nakon toga se izvrši sortiranje po opadajućem redosljedu za navedenu sumu. Na ovaj način definisana je mjera „kvaliteta“ neke lokacije da se na nju postavi snifer. Što je ova suma veća to će snifer koji se postavi na datu lokaciju hvatati više paketa, ako se pretpostavi da svi senzorski čvorovi generišu približno istu količinu saobraćaja.

```
Order_by: Suma PDR vrijednosti
  Input: sniffer_candidates, all_sensors
  Output: ordered_sniffer_candidates
1 ordered_sniffer_candidates = empty set
2 for sniffer in sniffer_candidates do
3 |   pdr_sum[sniffer] = 0
4 |   for sensor in all_sensors do
  |   |   // Suma PDR vrijednosti na svim kanalima
5 |   |   pdr_sum[sniffer] = pdr_sum[sniffer] + get_pdr(sniffer,
  |   |    sensor)
  // Sortiranje po opadajućem redosljedu
6 ordered_sniffer_candidates = descending_order(pdr_sum)
```

Pseudokod 4.3 Sortiranje predloženih lokacija po PDR sumi

Nakon toga, petlja na liniji 4 (*Pseudokod 4.2)* prolazi kroz sve potencijalne lokacije za snifere iz liste *sniffer_candidates.* Zatim se iz grafa G_s uklanja snifer sa najmanjom sumom tj. prvi snifer iz sortirane liste (linija 5) i vrši se provjera da li je novi graf i dalje DS za sve pomoćne grafove $G_{p1} \dots G_{p16}$ (linija 6). Ako novoformirani graf nije DS na bilo kom od pomoćnih grafova kreiranih u prvom dijelu Metode I, uklonjeni čvor vraćamo u graf G_s (linija 7), i njega nije moguće ukloniti, a da minimalni uslov o povezanosti sa sniferima bude i dalje ispoštovan. Algoritam se prekida kada se dostigne ciljni broj snifera (linija 8), ili kada petlja (linija 4) prođe kroz sve predložene lokacije. Izlazni podatak Metode I je lista (*reduced_candidates*) senzorskih čvorova koji se predlažu kao lokacije za snifere, kao i prosječna vjerovatnoća (*average_pdr*) da barem jedan od odabranih snifera detektuje paket poslat sa bilo kod senzorskog čvora u mreži i na bilo kom kanalu. Ova prosječna vjerovatnoća se računa pod pretpostavkom da svi senzori u mreži generišu približno istu količinu saobraćaja na svim kanalima, pri čemu se zanemaruje uticaj interne interferencije koji može smanjiti procenat detektovanog saobraćaja.

4.3 Metoda za odabir broja i pozicija za snifere zasnovana na teoriji vjerovatnoće i kombinatorici

Metoda za odabir broja i pozicija za snifere, u nastavku Metoda II, je zasnovana na teoriji vjerovatnoće i kombinatorici. Kao u Metodi I, i ovdje se kao ulazni podatak koriste matrice konektivnosti na svim kanalima i kao potencijalne lokacije za snifere razmatraju se samo lokacije senzora u mreži. Metoda II daje predlog lokacija za zadati broj snifera, koji će omogućiti najveću vjerovatnoću hvatanja paketa, ili daje predlog lokacija za snifere koji će

omogućiti hvatanje paketa sa zadatom vjerovatnoćom, koja je proslijeđena kao ulazni parametar. Sve ovo uz pretpostavku da senzorski čvorovi u mreži generišu približno istu količinu saobraćaja.

4.3.1 Broj dostupnih snifera kao ulazni parametar za Metodu II

Na Pseudokodu 4.4 prikazana je Metoda II, za slučaj kada se kao ulazni parametar zadaje dostupni broj snifera (*number_of_sniffers*). Na početku se definišu sve moguće kombinacije (*all_combs*) lokacija čvorova u mreži na koje je moguće postaviti dostupni broj snifera, linija 1.

Algoritam II:

Ulaz: Matrice konektivnosti $G_1 ... G_{16}$, number_of_sniffers
Izlaz: sniffers_locations, average_pdr

```
1  all_combs = combinations(sensors, number_of_sniffers)
   // Petlja kroz sve kombinacije za zadati broj snifera
2  for combination in all_combs do
3      pdr_sum_comb = 0
       // Petlja kroz sve sensorske čvorove u mreži
4      for sensor in sensors do
           // Petlja kroz sve radio kanale
5          for channel in channels do
               // Petlja kroz sve snifere iz date kombinacije
6              for sniffer in combination do
                   // Vjerovatnoća greške pri prenosu
7                  p_err = p_err*(1-get_pdr(sensor,sniffer,channel))
               // Vjerovatnoća uspješnog prenosa
8              p_success = 1 - p_err
9              pdr_sum_sens = pdr_sum_sens + p_success
10         avg_pdr_sens = pdr_sum_sens/16
11         pdr_sum_comb = pdr_sum_comb + avg_pdr_sens
12     avg_pdr_comb = pdr_sum_comb / number_of_sensors
13     if avg_pdr_comb > max_avg_pdr_comb then
14         best_comb = combination
15         max_avg_pdr_comb = avg_pdr_comb
16 sniffers_locations = best_comb
17 average_pdr = max_avg_pdr_comb
```

$$\prod_{z=1}^{N}(1-P_{i,j,z})$$

$$\sum_{j=1}^{C}(1-\prod_{z=1}^{N}(1-P_{i,j,z}))$$

$$\frac{1}{C}\sum_{j=1}^{C}(1-\prod_{z=1}^{N}(1-P_{i,j,z}))$$

$$\frac{1}{C}\sum_{i=1}^{M}\sum_{j=1}^{C}(1-\prod_{z=1}^{N}(1-P_{i,j,z}))$$

$$\frac{1}{M}\frac{1}{C}\sum_{i=1}^{M}\sum_{j=1}^{C}(1-\prod_{z=1}^{N}(1-P_{i,j,z}))$$

Pseudokod 4.4 Metoda II sa brojem dostupnih snifera kao ulaznim parametrom sa prikazom dobijanja jednačine (4.2)

Broj ovih kombinacija je jednak binomnom koeficijentu ukupnog broja senzora u mreži i broja dostupnih snifera, jednačina (4.1), gdje je M ukupan broj senzora u mreži, a N broj dostupnih snifera. Prikazana jednačina definiše broj kombinacija bez ponavljanja, što znači da se na jednu lokaciju senzora ne može postaviti više od jednog snifera.

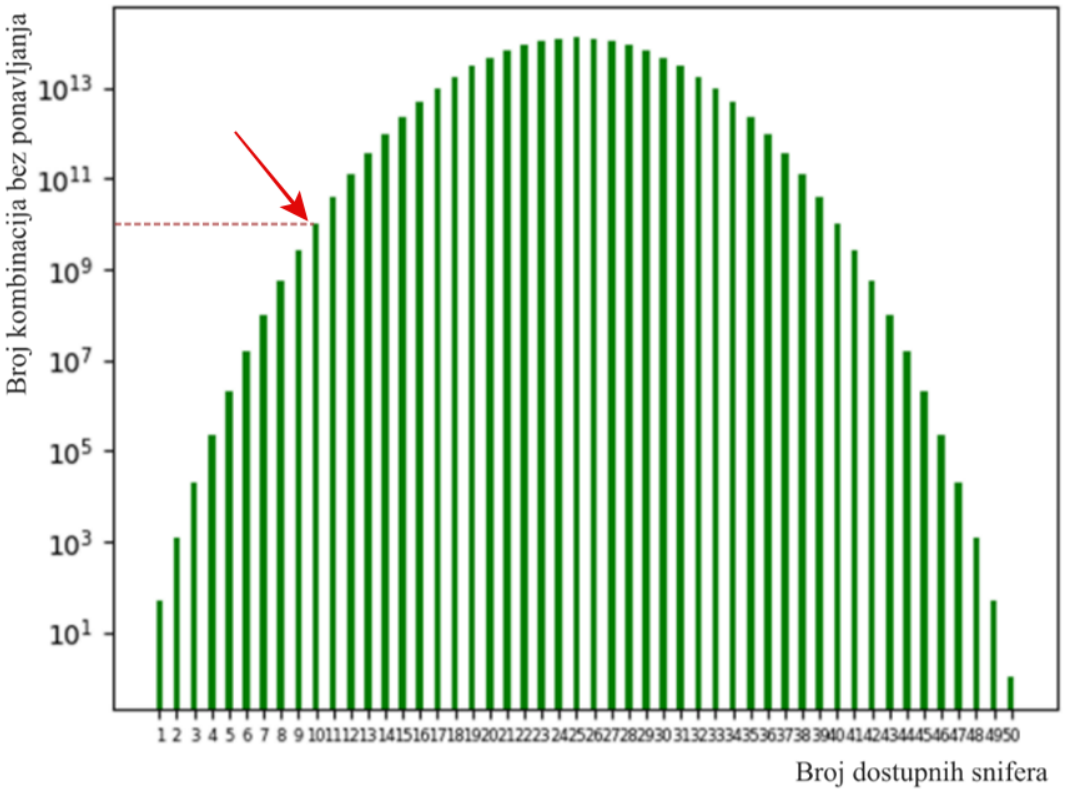
$$Broj\ kombinacija\ bez\ ponavljanja\ = \binom{M}{N} = \frac{M!}{N!\,(M-N)!} \tag{4.1}$$

Kada su definisane sve moguće kombinacije, neophodno je za svaku od njih izračunati prosječnu vjerovatnoću hvatanja paketa sa barem jednim sniferom, za sve senzore u mreži i na svim kanalima. Prva petlja, na liniji 2, prolazi kroz sve definisane kombinacije, i pomenuta prosječna vjerovatnoća se podešava na 0. Zatim, petlja na liniji 4, prolazi kroz sve senzore iz mreže, a petlja na liniji 5 kroz sve kanale koji se koriste. Zadnja *for* petlja, na liniji 6, prolazi kroz sve senzore iz date kombinacije tj. kroz potencijalne lokacije za snifere i računa se vjerovatnoća greške pri prenosu paketa između snifera na datoj lokaciji i definisanog senzora na odabranom kanalu. Ova vjerovatnoća se povlači iz matrice konektivnosti koja je dostupna kao ulazni parametar. Pretpostavka je da bi snifer na datoj lokaciji imao linkove istog kvaliteta sa ostalim senzorima kao i sam senzor na toj lokaciji, dok se komunikacija između senzora i snifera na istoj lokaciji smatra idealnom, tj. PDR je 1. Nakon toga, na liniji 8, vjerovatnoća greške se pretvara u vjerovatnoću uspješnog prenosa. Na liniji 10, računa se prosječna vjerovatnoća na svim kanalima, a na liniji 12 prosječna vjerovatnoća da bar jedan snifer iz odabrane kombinacije uspješno uhvati paket za sve senzore u mreži, što predstavlja i mjeru kvaliteta odabrane kombinacije, jednačina (4.2). Algoritam pronalazi kombinaciju iz liste *all_combs* kod koje je jednačina (4.2) najveća i tu kombinaciju daje kao izlazni parametar *sniffers_locations.*

$$P(s) = \frac{1}{M}\frac{1}{C}\sum_{i=1}^{M}\sum_{j=1}^{C}(1 - \prod_{z=1}^{N}(1 - P_{i,j,z})) \tag{4.2}$$

Jednačina (4.2) prikazuje prosječnu vjerovatnoću da barem jedan snifer iz izabrane kombinacije, detektuje paket za sve senzore iz mreže na svim kanalima, gdje je M broj senzora u mreži, C broj kanala koji se koriste i N broj dostupnih snifera. $P_{i,j,z}$ je PDR vrijednost linka između senzora i i senzora j, na kanalu z.

Jedno od glavnih ograničenja kod ovog pristupa je veliki broj kombinacija koje je potrebno obraditi. Kako raste broj senzora u mreži i broj dostupnih snifera, tako se povećava i broj mogućih kombinacija bez ponavljanja do tačke kada broj snifera dostiže $M/2$, gdje je M broj senzora u mreži, a zatim opada do M. Sa *Slike 4.5* se vidi da u mreži sa 50 čvorova, za 10 dostupnih snifera, postoji preko **deset milijardi** mogućih kombinacija raspoređivanja.

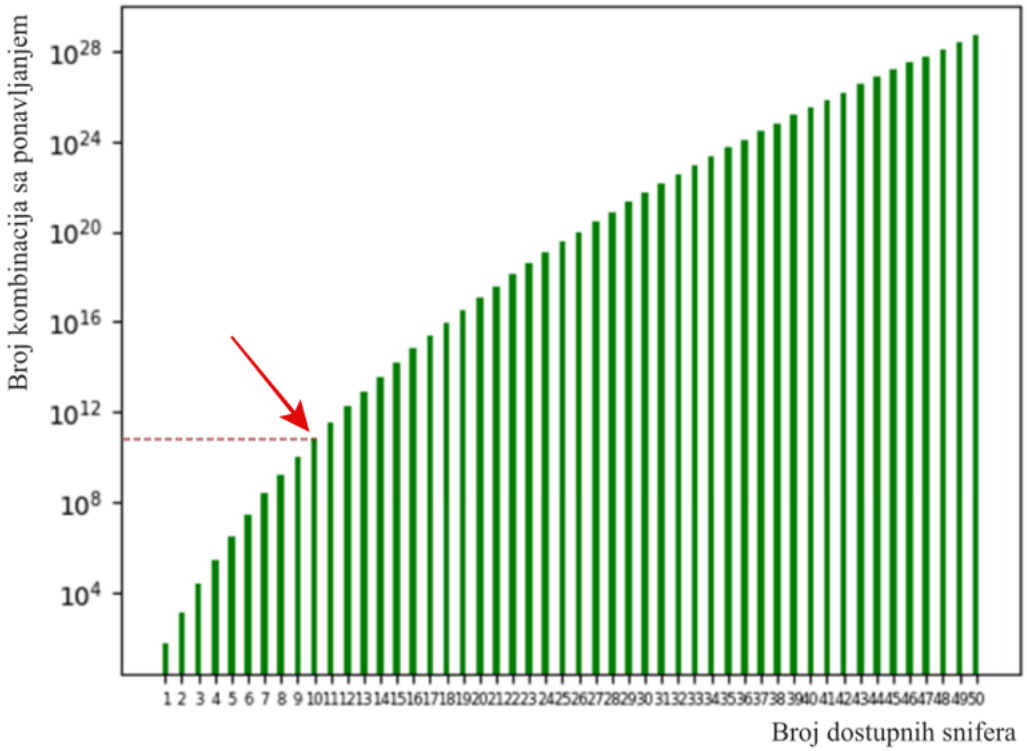


Slika 4.5 Prikaz broja kombinacija bez ponavljanja za različite brojeve dostupnih snifera u mreži sa 50 čvorova

Razmatran je i pristup u kome se analiziraju i kombinacije sa ponavljanjem. U ovom slučaju na mjestu jednog senzora moguće je postaviti više od jednog snifera, a da je pri tome maksimalan broj snifera jednak broju senzora u mreži. Tada je ukupan broj kombinacija izražen u jednačini (4.3), gdje je *M* ukupan broj senzora u mreži, a *N* broj dostupnih snifera.

$$Broj\ kombinacija\ sa\ ponavljanjem = \binom{M+N-1}{N} = \frac{(M+N-1)!}{N!\,(M-N)!} \qquad (4.3)$$

Ovdje se broj kombinacija povećava pri povećanju broja dostupnih snifera, *Slika 4.6.* Sa slike se vidi da u mreži sa 50 čvorova, za 10 dostupnih snifera, postoji preko **šezdeset milijardi** mogućih kombinacija raspoređivanja. Možemo zaključiti da Metoda II nije praktična za upotrebu u mrežama sa velikim brojem senzora i kada je dostupan veći broj snifera, jer je potrebno analizirati veliki broj kombinacija.



Slika 4.6 Prikaz broja kombinacija sa ponavljanjem za različite brojeve dostupnih snifera u mreži sa 50 čvorova

4.3.2 Prosječna vjerovatnoća detekcije paketa kao ulazni parametar za Metodu II

U drugom pristupu, kao ulazni parametar zadaje se prosječna vjerovatnoća uspješnog hvatanja paketa (*target_pdr*) koju je moguće ostvariti sa sniferima na predloženim lokacijama, jednačina (4.2). Na *Pseudokodu 4.5* prikazana je Metoda II sa ulazim parametrom *target_pdr*.

```
Algoritam II:
   Ulaz: Matrice konektivnosti G_1...G_16, target_pdr
   Izlaz: sniffers_locations, average_pdr
1  for number_of_sniffers in 1 .. M do
2      all_combs = combinations(sensors, number_of_sniffers)
       // Petlja kroz sve kombinacije za zadati broj snifera
3      for combination in all_combs do
4          pdr_sum_comb = 0
           // Petlja kroz sve sensorske čvorove u mreži
5          for sensor in sensors do
               // Petlja kroz sve radio kanale
6              for channel in channels do
                   // Petlja kroz sve snifere iz date kombinacije
7                  for sniffer in combination do
                       // Vjerovatnoća greške pri prenosu
8                      p_err =
                       p_err*(1-get_pdr(sensor,sniffer,channel))
                   // Vjerovatnoća uspješnog prenosa
9                  p_success = 1 - p_err
10                 pdr_sum_sens = pdr_sum_sens + p_success
11             avg_pdr_sens = pdr_sum_sens/16
12             pdr_sum_comb = pdr_sum_comb + avg_pdr_sens
13         avg_pdr_comb = pdr_sum_comb / number_of_sensors
14         if  avg_pdr_comb ≥ target_pdr then
15             target_comb = combination
16             target_avg_pdr_comb = avg_pdr
17             break
18 sniffers_locations = target_comb
19 average_pdr = target_avg_pdr_comb
```

Pseudokod 4.5 Metoda II sa prosječnom vjerovatnoćom uspješnog hvatanja paketa kao ulaznim parametrom

Ovdje postoji dodatna petlja na liniji 1, koja prolazi kroz listu cijelih brojeva od 1 do M, gdje je M broj senzora u mreži i ujedno maksimalni broj snifera koje je moguće postaviti na lokacije senzora, ako se koriste kombinacije bez ponavljanja. Nakon toga se, kao i na *Pseudokodu 4.4* formiraju kombinacije i izračunavaju se prosječne vjerovatnoće uspješne detekcije paketa sa barem jednim sniferom. Međutim, ovdje se algoritam prekida kada se dostigne ciljana prosječna vjerovatnoća i kombinacija koja to omogućava se prikazuje kao izlazni parametar algoritma. Cilj je dostići traženu vjerovatnoću sa što manjim brojem snifera. U tu svrhu prva *for* petlja kreće od jednog snifera i povećava njihov broj, dok ne se dođe do cilja. Prilikom svakog povećanja dostupnog broja snifera (*number_of_sniffers*) vrši se generisanje novih kombinacija.

Glava 5

5. Analiza simulacionih rezultata

Za analizu rada metoda za određivanje broja i pozicija za snifere i pregled njihovih performansi i efikasnosti, korišćen je 6TiSCH Simulator, koji je opisan u Glavi 3. Postojeće simulaciono rješenje je prošireno, tako što je uveden snifer kao novi tip uređaja. Dodato je novo stanje radio primopredajnika RADIO_STATE_SNIFFER, koje definiše da objekat *Mote* može raditi i kao snifer tj. da ne vrši slanje paketa i da može osluškivati saobraćaj na svih 16 kanala istovremeno. U simulatoru su implementirani i algoritmi za metode opisane u Glavi 4, koji prije pokretanja simulacije vrše odabir lokacija za snifere.

Uvedeni su novi ulazni parametri koji se prosljeđuju kroz konfiguracioni fajl simulatora (*config.json*). Na početku, novi parametar *sniffer_deploy* je potrebno podesiti na vrijednost *True*, što znači da se sniferi koriste u simulaciji. Metoda koji se koristi se upisuje u novi parametar nazvan *selection_algorithm*, u koji se može upisati vrijednost '*Graph*' za Metodu I ili '*Probabilistic*' za Metodu II. Ostali parametri vezani za pojedinačne metode su opisani u Glavi 4, i njihove vrijednosti se prosljeđuju kroz isti konfiguracioni fajl.

Odgovarajući algoritmi za prikazane metode su implementirani u modulu *SimEngine*, gdje se nakon inicijalizacije klase *Connectivity* koja definiše matricu konektivnosti i mrežnu topologiju, vrši odabir lokacija za snifere na osnovu podataka iz pomenute klase. 6TiSCH Simulator omogućava automatsko generisanje slučajnih mrežnih topologija ili preuzimanje *trace-based* topologija iz stvarnog okruženja, što je opisano u poglavlju 3.2. Kada se koriste slučajne topologije, parametar *conn_class* se podešava na vrijednost „*Random*“, dok se kod *trace-based* topologija ovaj ulazni parametar podešava na vrijednost „*K7*“. Nakon odabira lokacija, sniferi se sa novom funkcijom *add_sniffers* iz klase *Connectivity* „ugrađuju“ u kreiranu matricu konektivnosti, koja kod *Random* topologije sadrži *x* i *y* koordinate na kojima se senzori nalaze. Sniferi dobijaju iste koordinate kao i senzori, čije je mjesto odabrano za poziciju svakog od njih. Na ovaj način radio linkovi sa susjedima, koji u ovom slučaju zavise od prostorne udaljenosti, će biti identični za snifer i senzor, na čijem se mjestu nalazi. Komunikacija između snifera i senzora, na čijem se mjestu nalazi, odvija se kao da se nalaze na udaljenosti od 10 cm. Kada se koriste *trace-based* topologije iz stvarnog okruženja,

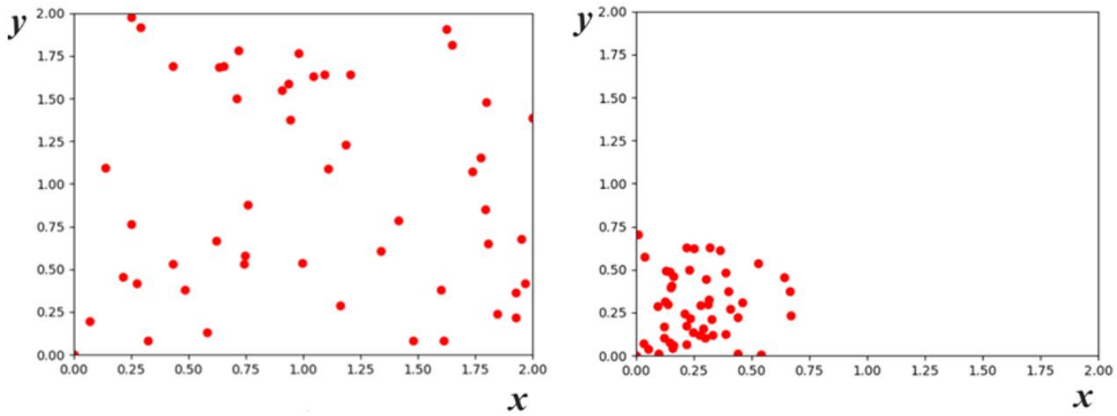
matrice konektivnosti, umjesto prostornih koordinata, sadrže linkove sa odgovarajućim PDR vrijednostima. U ovom slučaju, sniferi preuzimaju iste linkove sa svim susjedima kao senzor na čijem se mjestu postavljaju, dok je njihova međusobna komunikacija idealna, sa PDR vrijednosti podešenom na 1.

Kako bi se omogućila analiza rada snifera, uvedene su tri nove metrike:

- LOG_SNIFFERS_LOCATIONS_AND_PDR – nakon što algoritam izvrši odabir broja i lokacija za snifere, upisuju se podaci o sniferima koji su odabrani i prosječna vjerovatnoća hvatanja paketa sa barem jednim sniferom (*average_pdr*), akcija *sniffer.selection;*
- LOG_SNIFFER_INIT – upisuje podatke o inicijalizaciji svakog snifera, gdje je navedena akcija *sniffer.init* i ID snifera;
- LOG_SNIFFER_RXDONE – upisuje se svaki paket koji snimi neki od snifera, gdje je navedena akcija *sniffer.rxdone*, ID snifera koji je snimio paket, ASN u kome je snimljen paket i sadržaj paketa;

Posle izbora lokacija za snifere, upisuje se prva metrika LOG_SNIFFERS_LOCATIONS_AND_PDR sa podacima o odabranim lokacijama za snifere i prosječnom vjerovatnoćom hvatanja paketa. Nakon što se izmijeni matrica konektivnosti, tako što se u nju unesu podaci o sniferima, tj. njihove lokacije kod slučajnih topologija ili podaci o svim linkovima koje grade u slučaju da se koriste *trace-based* topologije, svim sniferima se podešava novo stanje radio primopredajnika RADIO_STATE_SNIFFER i izvrši se upis metrike LOG_SNIFFER_INIT. Tokom simulacije, postavljeni sniferi snimaju saobraćaj koji se razmjenjuje u mreži i podaci o detekciji se upisuju u *log* fajl (metrika LOG_SNIFFER_RXDONE), koji se nakon simulacije može dalje obrađivati i analizirati.

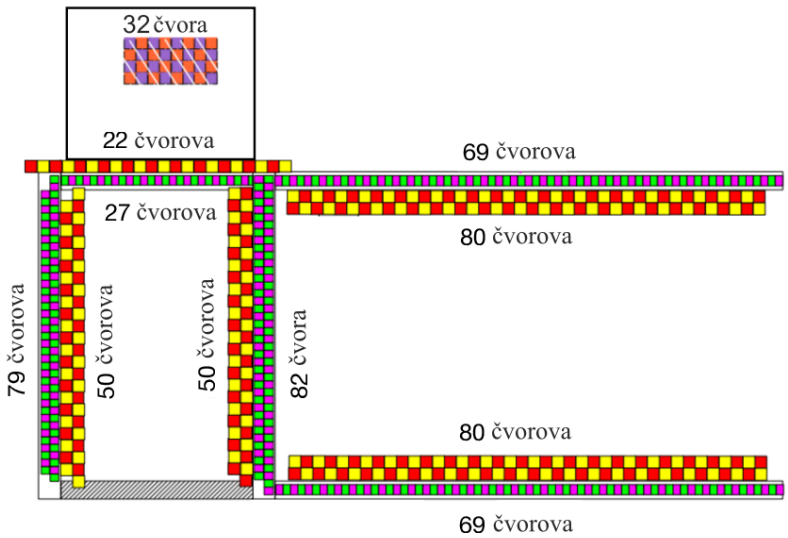
Za slučajno generisanje mrežne topologije (*Random*), simulacije su vršene sa 50 senzora, koji su slučajno raspoređeni na prostoru od 2000×2000 metara, a da pri tome budu ispoštovana podrazumijevana ograničenja postavljena u simulatoru. Svaki čvor mora imati barem 3 susjeda, sa kojima ima najmanje jedan link kome je PDR veći od 0.5, na svim kanalima. Ova podešavanja su preporučena od strane autora [44], kako bi se osiguralo generisanje mrežne topologije koja ima slične karakteristike kao WSNs u realnom okruženju. Na ovaj način vrši se automatsko grupisanje čvorova, koji su nakon generisanja mrežne topologije raspoređeni na prostoru od oko 750×750 metara, *Slika 5.1.*



a) *b)*

Slika 5.1 Prikaz prostornog rasporeda čvorova kod slučajno generisanje topologije; a) Bez podrazumijevanih ograničenja; b) Uz ograničenje da svaki čvor mora imati barem 3 susjeda, sa kojima ima najmanje jedan link kome je PDR veći od 0.5, na svim kanalima

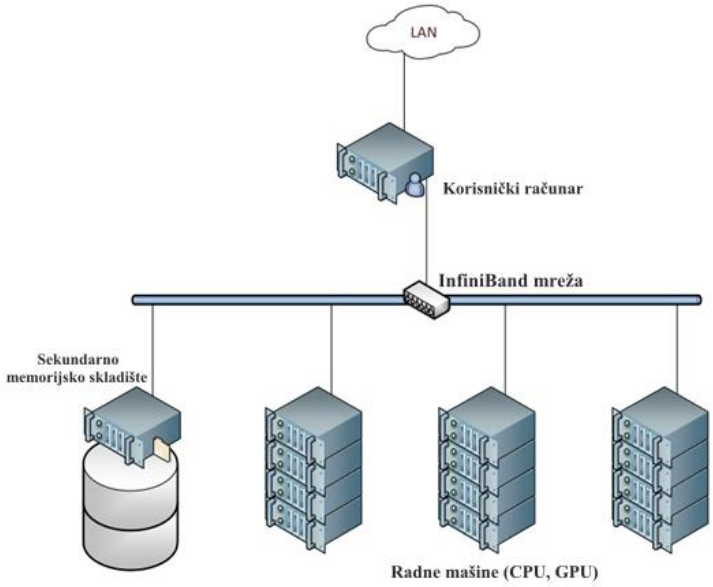
Pored slučajno generisanih mrežnih topologija, korišćena je i *trace-based* matrica konektivnosti iz stvarnog okruženja, koje je snimljena na eksperimentalnoj *testbed* platformi FIT IoT-lab Grenoble, koja koristi 384 *M3 open* čvora i 288 *A8* čvorova, *Slika 5.2*, [45]. U radu se koristi matrica konektivnosti koja je snimljena u dijelu mreže sa 50 čvorova.



Slika 5.2 Šematski prikaz FIT IoT-lab Grenoble testbed platforme

Pokretanje simulacija je vršeno na klaster računaru (engl. *Cluster computer*) CLEPS [46], koji radi u okviru Nacionalnog instituta za istraživanje u računarstvu i automatici – Inria (franc. *Institut national de recherche en informatique et en automatique*). Klaster se nalazi u Francuskoj u Parizu, a pristup je omogućen putem udaljene VPN (engl. *Virtual Private*

Network) konekcije. Rad sa klaster računarom značajno ubrzava simulacije i obradu podataka, jer se koristi paralelni rad na više jezgara, nakon čega se podaci objedinjuju u jedan izlazni *log* fajl. Korišćene su mašine koje koriste 2×*Cacade Lake Intel Xeon 5218* procesore sa 16 jezgara, sa taktom od 2.4 GHz i dostupnom radnom memorijom od 192 GB. Arhitektura klaster računara CLEPS je prikazana na *Slici 5.3.*



Slika 5.3 Arhitektura klaster računara CLEPS

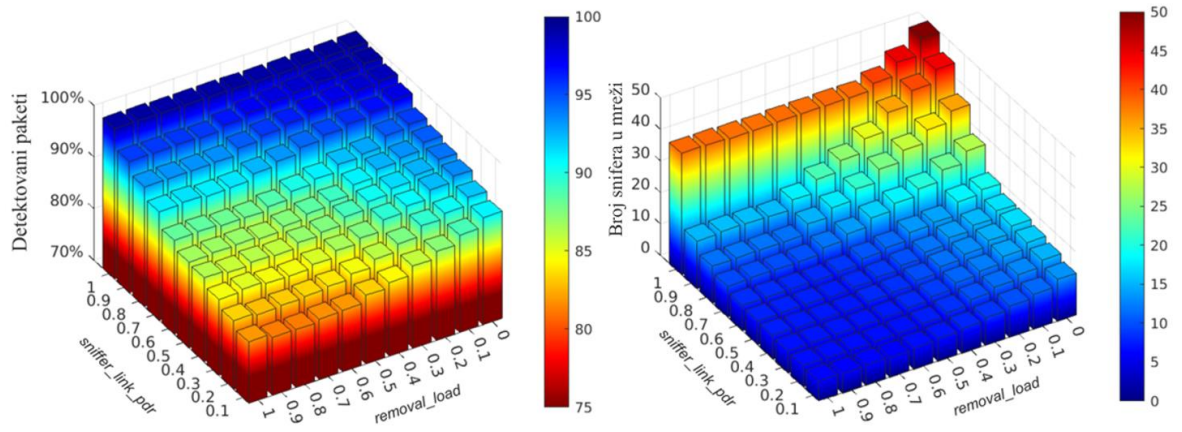
5.1 Analiza rezultata za Metodu I

U Tabeli 5.1 su prikazani značajni parametri koji su korišćeni u konfiguracionom fajlu simulatora. Za analizu grafova korištena je Pajton biblioteka NetworkX [47], čija funkcija *min_weighted_dominating_set* aproksimativno određuje MDS za dati graf. Vremenska složenost algoritma koji određuje MDS je *O(m)*, gdje je *m* broj grana u grafu.

Tabela 5.1 Prikaz ulaznih parametara za simulacije

Parametar	**Vrijednost**
numRuns	100
exec_numMotes	50
exec_numSlotframesPerRun	5000
sf_class	*MSF*
conn_class	*Random, K7 (grenoble.k7.gz)*
sniffer_deploy	*True*
selection_algorithm	*Graph*
sniffer_link_pdr	0.0,0.1,0.2,..,1.0
removal_load	0.1,0.2,0.3,..,1.0

Nakon obrade simulacionih podataka, vršena je analiza uticaja parametara *sniffer_link_pdr* za vrijednosti od 0.1 do 1 sa korakom 0.1 i *removal_load* za vrijednosti od 0 do 1 sa korakom 0.1, na procenat uhvaćenog saobraćaja i broj snifera koje Metoda I predlaže. Svaka tačka na prikazanim graficima je simulirana 100 puta i svaka od simulacija je trajala ukupno 5000 vremenskih slotova.

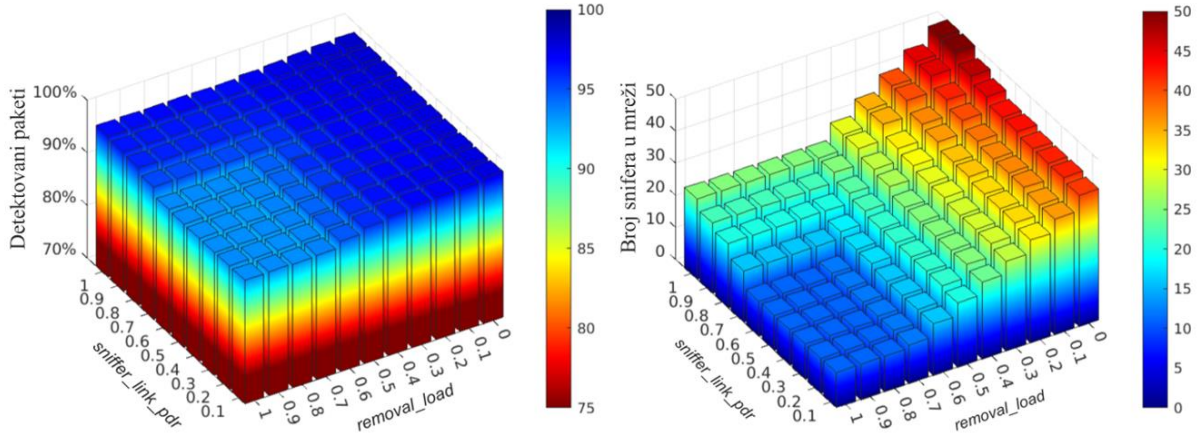


a) *b)*

Slika 5.4 Procenat detektovanih paketa (a) i broj snifera u mreži (b) za različite vrijednosti ulaznih parametara za Random topologije

Slika 5.4 prikazuje prosječan procenat detektovanih paketa i broj snifera za različite vrijednosti ulaznih parametara *sniffer_link_pdr* i *removal_load*, za *Random* topologije. Za svaku od 100 simulacija vršeno je generisanje nove slučajne topologije. Kao što je i očekivano, sa smanjenjem broja snifera u mreži, smanjuje se procenat detektovanih paketa. Tako je sa 27 snifera moguće detektovati oko 97.5% paketa, kada je parametar *sniffer_link_pdr* 0.7, a *removal_load* 0. Međutim, kada je parametar *removal_load* podešen na 1, broj snifera se spusti na 10, a u isto vrijeme procenat detektovanih paketa pada na 91%. Takođe, sa povećanjem minimalnog kvaliteta linkova za snifere (*sniffer_link_pdr*), procenat detektovanih paketa se povećava. Za slučaj kada je *sniffer_link_pdr* podešen na 1, što znači da je svaki senzor u mreži povezan sa barem jednim sniferom sa linkom 1, oko 2% paketa ne bude snimljeno. Razlog je interna interferencija, do koje dolazi kada više čvorova vrši emitovanje na istom kanalu i u istom vremenskom slotu. Sa parametrom *removal_load*, moguće je značajno smanjiti broj snifera, osim kada je *sniffer_link_pdr* podešen na 1. Iz ovoga se može zaključiti da u mreži nema dovoljno linkova gdje je PDR jednak 1, zbog toga nije moguće zadovoljiti uslov DS pri smanjivanju broja snifera u ovom slučaju. Za manje

vrijednosti parametra *sniffer_link_pdr* smanjenje broja snifera je značajno, dok se procenat detektovanih paketa ne smanjuje istom brzinom kako se uklanjaju sniferi, već sporije.



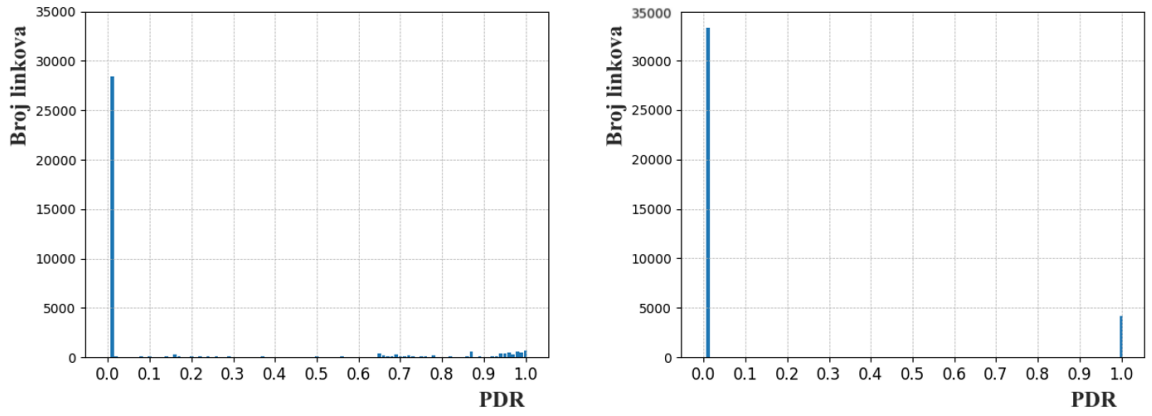
a) *b)*

Slika 5.5 Procenat detektovanih paketa (a) i broj snifera u mreži (b) za različite vrijednosti ulaznih parametara za FIT IoT-lab Grenoble topologiju

Slika 5.5 prikazuje rezultate za realnu matricu konektivnosti koja je snimljena uz pomoć softverskog rješenja *Mercator* opisanog u poglavlju 3.2, na FIT IoT-lab Grenoble *testbed* platformi sa 50 senzorskih čvorova. Za razliku od slučajnih topologija, ovdje je broj snifera veći od 40 za sve vrijednosti parametra *sniffer_link_pdr*, kada je *removal_load* jednak 0. Iz ovoga možemo zaključiti da ova topologija ima veće razlike u matricama konektivnosti na različitim kanalima, nego slučajno generisane topologije. Zbog toga se MDS međusobno razlikuju na pojedinačnim kanalima, i nakon unije, predlaže se veliki broj snifera. Ipak, u matricama konektivnosti postoji korelacija, pa se sa povećanjem parametra *removal_load*, broj snifera smanjuje. Korelacija među matricama konektivnosti je značajno manja nego kod slučajnih topologija, pa se zato minimalan broj snifera kod ove topologije ni za jednu kombinaciju ulaznih parametara ne spušta ispod 11. Smanjenje u broju snifera sa promjenama parametra *removal_load* je značajno i u slučaju kada je *sniffer_link_pdr* jednak 1, što sugeriše da u mreži postoji određeni broj linkova gdje je PDR jednak 1.

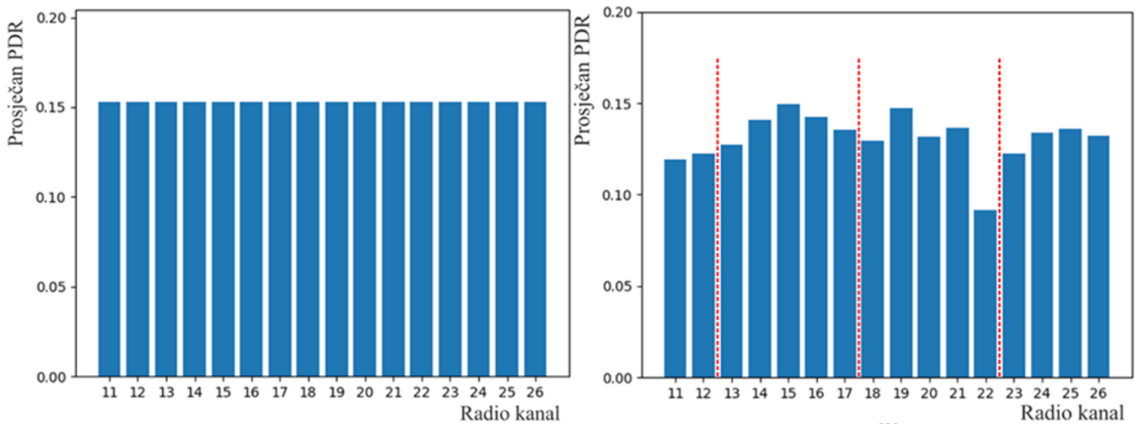
Slika 5.6 prikazuje broj linkova u odnosu na njihov kvalitet, na svim kanalima, za 100 *Random* topologija sa izračunatim prosječnim brojem linkova i FIT IoT-lab Grenoble mrežnu topologiju. Može se vidjeti da je kod obje topologije najveći broj linkova veoma slabog kvaliteta (PDR ispod 0.05). Mrežna topologija snimljena na *testbed* okruženju ima značajno veći broj linkova veoma visokog kvaliteta (PDR ~ 1), ali u isto vrijeme veći broj linkova veoma niskog kvaliteta (PDR ispod 0.05), što sugeriše da su senzorski čvorovi raspoređeni u

jednu ili više grupa koje su međusobno odvojene. Zbog toga su senzori u grupama povezani linkovima visokog kvaliteta, ali su grupe međusobno odvojene, pa ova mrežna topologija ima veliki broj linkova niskog kvaliteta. Ovakva raspodjela kvaliteta linkova odražava se na opisani procenat detekcije paketa i broj snifera koje predlaže Metoda I za slučajno generisane matrice konektivnosti i *trace-based* matricu. Zbog toga je pri određivanju broja i pozicije snifera za određenu mrežu, potrebno pažljivo izabrati ulazne parametre kako bi se omogućila detekcija željenog procenta paketa, a da se pri tome ne prekorači broj dostupnih snifera. Kod gušće raspoređenih mreža, nije potrebno koristiti veliki broj snifera, ako se oni postave na lokacije koje će omogućiti hvatanje paketa sa velikog broja senzora, tako što će sa njima biti povezani linkovima visokog kvaliteta. Važno je i da čitava mreža bude ravnomjerno pokrivena sniferima, kako neki djelovi mreže ne bi ostali izolovani.



a) *b)*

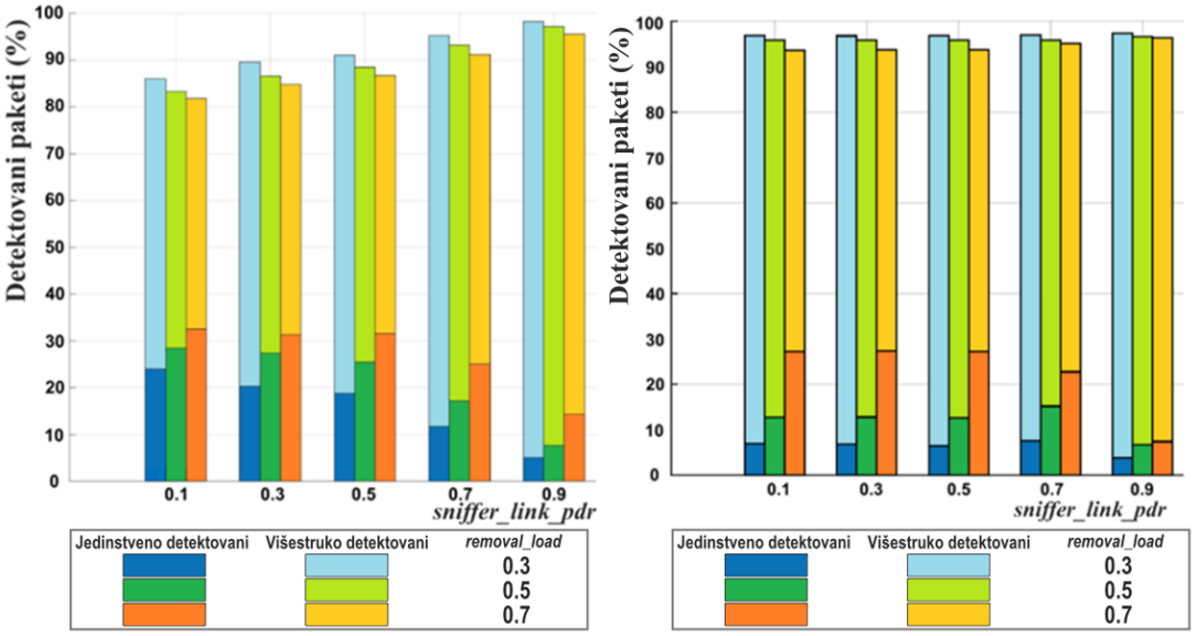
Slika 5.6 Broj linkova u mreži u odnosu na njihov kvalitet izražen u PDR vrijednostima; a) za Random topologije; b) za FIT IoT-lab Grenoble topologiju



a) *b)*

Slika 5.7 Prosječan PDR za linkove na pojedinačnim kanalima; a) za Random topologije; b) za FIT IoT-lab Grenoble topologiju

Slika 5.7 prikazuje prosječne vrijednosti PDR-a za sve linkove na pojedinačnim kanalima za 100 *Random* topologija sa izračunatom prosječnom vrijednošću i za FIT IoT-lab Grenoble topologiju. U 6TiSCH Simulatoru radio okruženje je isto za sve frekvencijske kanale, što nije slučaj u realnim okruženjima, gdje eksterna interferencija utiče samo na pojedine kanale. Na FIT IoT-lab Grenoble raspodjeli, na kanalu 22, kvaliteti linkova su značajno manji nego na ostalim kanalima, što sugeriše da još neki uređaji iz okoline koriste ovaj frekvencijski opseg. Na *Slici 5.7 b),* isprekidanim crvenim linijama su označeni frekvencijski kanali koji se koriste za Wi-Fi komunikaciju. Sa grafika se može vidjeti, da u sve tri označene oblasti postoji značajna interferencija sa Wi-Fi signalom. Ovo se odražava na rad Metode I, gdje početna unija MDS na svim kanalima kod FIT IoT-lab Grenoble topologije sadrži veliki broj snifera, a broj snifera nije moguće smanjiti ispod 11, što je i napomenuto ranije.

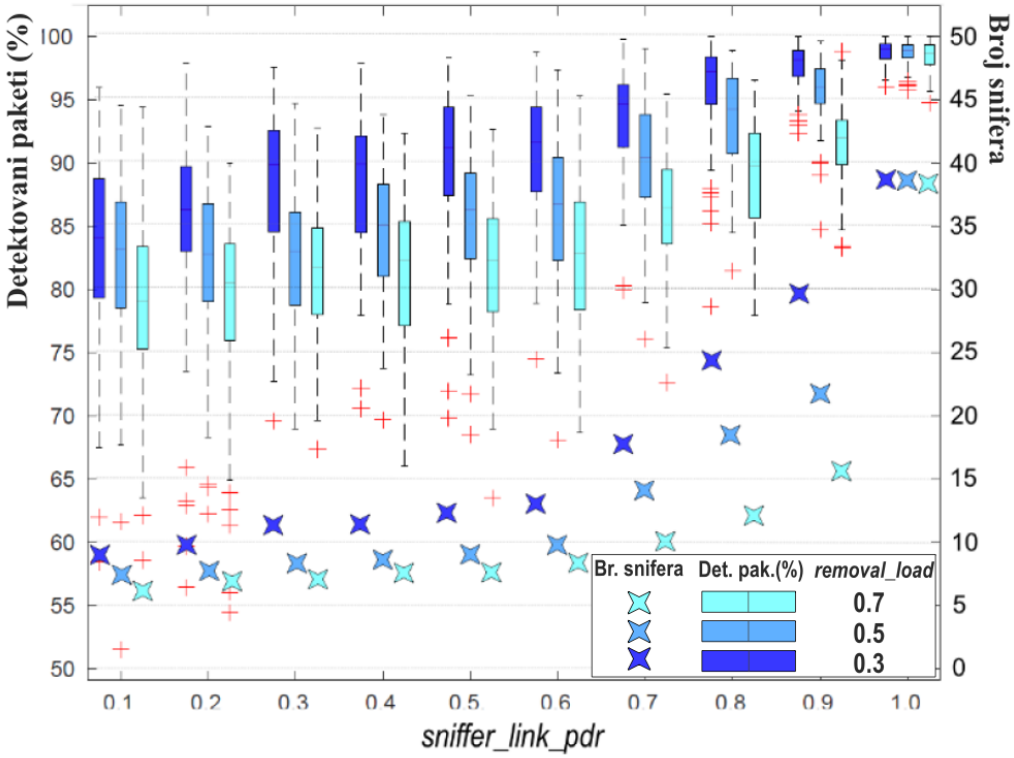


a) *b)*

Slika 5.8 Procenat jedinstveno i višestruko detektovanih paketa za karakteristične vrijednosti ulaznih parametara, za Random (a) i FIT IoT-lab Grenoble (b) topologiju

Slika 5.8 prikazuje procenat jedinstveno i višestruko detektovanih paketa za karakteristične vrijednosti ulaznih parametara. Višestruko detektovani paketi su snimljeni sa dva ili više snifera. Ova analiza je značajna, jer pruža uvid u pokrivenost nekih djelova mreže sa više snifera koji snimaju isti saobraćaj. Sa povećanjem broja snifera u mreži, raste broj detektovanih paketa, ali u isto vrijeme raste broj višestrukih detekcija i obrnuto. Za visoke

procente detekcije mrežnog saobraćaja (iznad 95%), preko 90% detektovanih paketa je snimljeno više od jednog puta. Ovo može otežati kasniju analizu snimljenog saobraćaja, jer je potrebno izvršiti filtriranje višestrukih detekcija, kako bi se korisniku prikazao samo stvarni saobraćaj. U [48] je predstavljeno rješenje koje omogućava filtriranje višestruko detektovanih paketa, u slučajevima kada se koristi više od jednog snifera u višekanalnim WSNs.

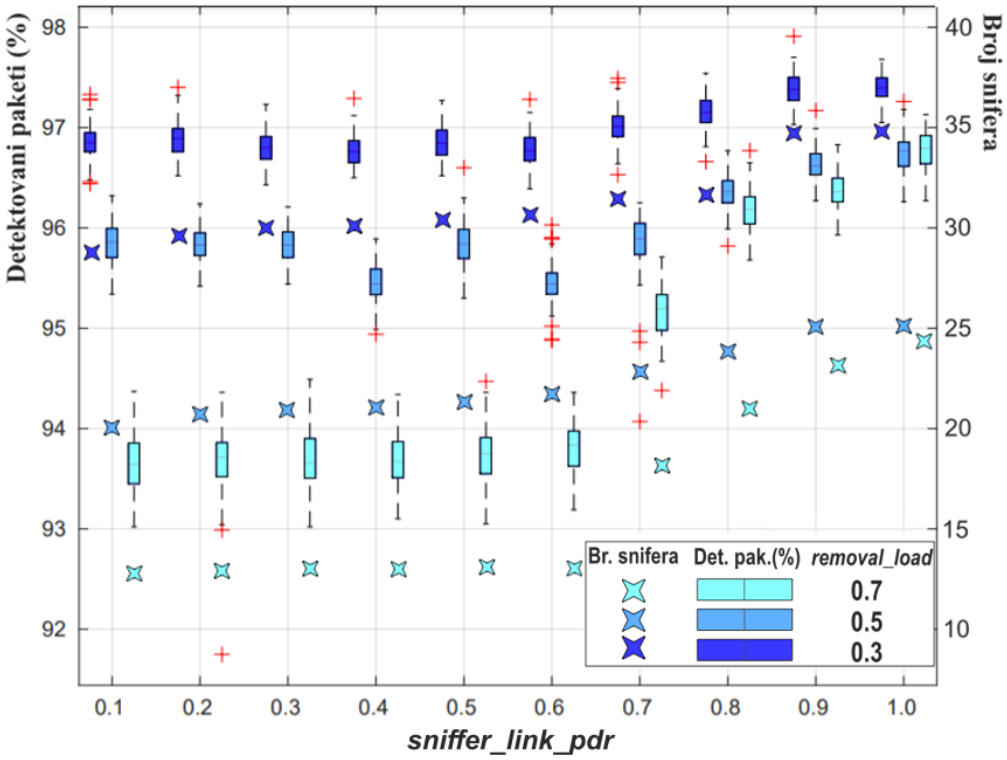


Slika 5.9 Procenat detektovanih paketa sa odgovarajućim prosječnim brojem snifera za karakteristične vrijednosti ulaznih parametara za Random topologije

Slika 5.9 prikazuje procenat detektovanih paketa i prosječan broj snifera za karakteristične vrijednosti ulaznih parametara, za *Random* topologije. Za analizu su odabrane tri vrijednosti za parametar *removal_load,* 0.3, 0.5 i 0.7 i sve vrijednosti parametra *sniffer_link_pdr*. Za manje vrijednosti parametra *sniffer_link_pdr,* varijacije procenta detektovanih paketa su veće. Ovo se događa zato što se za svaku kombinaciju ulaznih parametara generiše 100 slučajnih topologija, među kojima postoje razlike. Zbog toga algoritam odabira različitu kombinaciju snifera svakog puta, a pored toga funkcija *min_weighted_dominating_set* koja određuje MDS je aproksimativna. Takođe, kada je *sniffer_link_pdr* podešen na 0.1, tada vrijednosti linkova za MDS mogu biti između 0.1 i 1. Sa *Slike 5.6 a)* se vidi da postoji značajan broj linkova različitog kvaliteta na opsegu između

0.1 i 1, kod *Random* topologija. Zbog toga, algoritam ima veći opseg različitih MDS koje može odabrati za postavljanje snifera. Kako se vrijednost ovog parametra povećava, tako se smanjuje opseg mogućih MDS za snifere i varijacije procenta detektovanih paketa su manje.

Sa Metodom I, za slučajno generisane topologije, moguće je izabrati lokacije za snifere, koje će omogućiti detekciju oko 90% razmijenjenih paketa, kada je parametar *sniffer_link_pdr* u opsegu 0.5 do 0.8 i kada se koristi od 10 do 15 snifera. *Slika 5.9* pokazuje da postoje topologije, gdje je sa manje od 10 snifera moguće detektovati gotovo 90% paketa.



Slika 5.10 Procenat detektovanih paketa sa odgovarajućim prosječnim brojem snifera za karakteristične vrijednosti ulaznih parametara za FIT IoT-lab Grenoble topologiju

Slika 5.10 prikazuje procenat detektovanih paketa i prosječan broj snifera za karakteristične vrijednosti ulaznih parametara, za FIT IoT-lab Grenoble topologiju. Za razliku od slučajnih topologija, ovdje su varijacije procenta detektovanih paketa značajno manje, jer se koristi samo jedna mrežna topologija. Kod ove topologije gotovo svi linkovi su veoma slabog kvaliteta (PDR ispod 0.05), ili su veoma visokog kvaliteta (PDR iznad 0.95), što se može vidjeti sa *Slike 5.6 b)*. Zbog ovoga, algoritam nema veliki broj kombinacija pri izboru lokacija za snifere, kao što je to slučaj kod *Random* topologija.

Ovdje je sa Metodom I moguće detektovati oko 93.5% paketa, kada je parametar *sniffer_link_pdr* između 0.1 i 0.7, a parametar *removal_load* 0.7 i kada se u koristi oko 13 snifera.

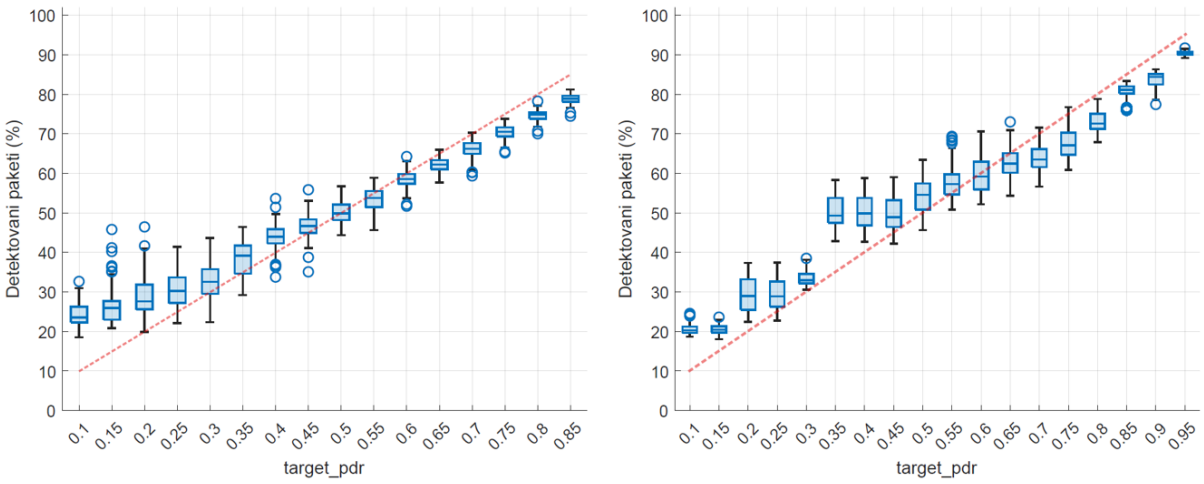
5.2 Analiza rezultata za Metodu II

U Tabeli 5.2 su prikazani značajni parametri koji su korišćeni u konfiguracionom fajlu simulatora.

Tabela 5.2 Prikaz ulaznih parametara za simulacije

Parametar	**Vrijednost**
numRuns	100
exec_numMotes	50
exec_numSlotframesPerRun	5000
sf_class	*MSF*
conn_class	*Random, K7 (grenoble.k7.gz)*
sniffer_deploy	*True*
selection_algorithm	*Probabilistic*
target_pdr	0.1,0.15,0.2,..,1.0
number_of_sniffers	1, 2, 3, 4, 5

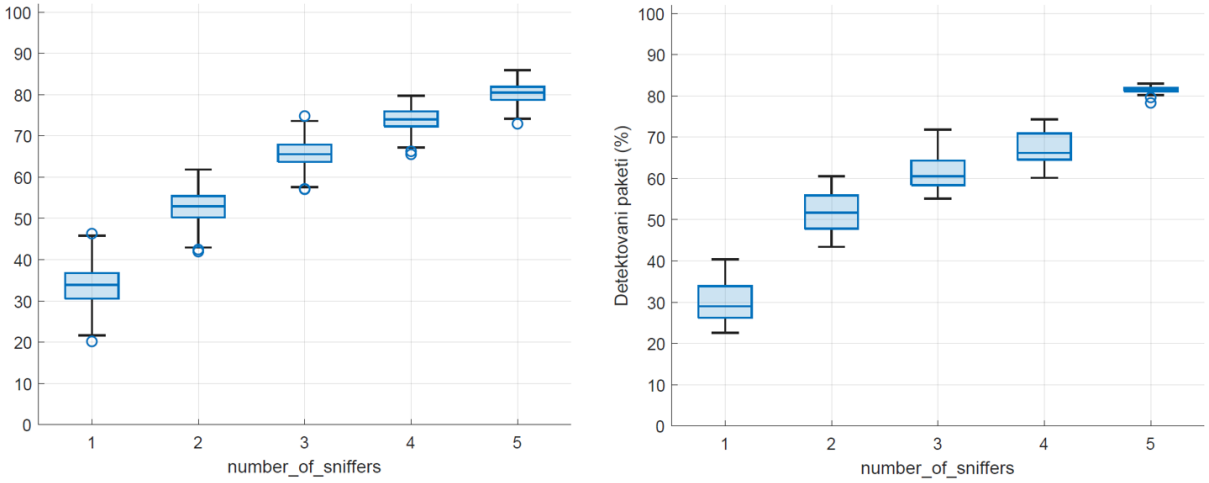
Simulacije su vršene za različite vrijednosti ulaznih parametara. *Target_pdr* je mijenjao vrijednosti od 0.1 do 1 sa korakom 0.05, dok je parametar *number_of_sniffers* išao od 1 do 5. Simulacije su vršene posebno za oba ulazna parametra, jer Metoda II radi u dva režima rada. Svaka tačka na prikazanim graficima je simulirana 100 puta i svaka od simulacija je trajala ukupno 5000 vremenskih slotova. Kao što je opisano u poglavlju 4.3, glavno ograničenje Metode II je veliki broj kombinacija koje je potrebno obraditi. Kako se povećava broj dostupnih snifera (parametar *number_of_sniffers*), tako raste broj kombinacija. Takođe, za veće vrijednosti parametra *target_pdr*, algoritam mora obraditi veliki broj kombinacija, dok ne dođe do vrijednosti navedenog parametra. Zbog toga je gornja granica za broj dostupnih snifera postavljena na 5, a za krajnje vrijednosti parametra *target_pdr*, tj. za vrijednost 1.0 za FiT IoT-lab Grenoble topologiju i vrijednosti 0.9, 0.95 i 1.0 za *Random* topologija, nije bilo moguće dobiti rezultate zbog velikog broja kombinacija. Kod *Random* topologije krajnje vrijednosti su niže, jer se za svaku od 100 simulacija generiše nova mrežna topologija za koju je potrebno određivati novu kombinaciju snifera. Kod FiT IoT-lab Grenoble topologije, najbolja kombinacija snifera se pronađe samo jednom, nakon čega se 100 puta simulira rad mreže.



a) *b)*

Slika 5.11 Procenat detektovanih paketa u odnosu na parametar target_pdr; a) Random topologije; b) FiT IoT-lab Grenoble topologija

Slika 5.11 prikazuje promjene procenta detektovanih paketa, u funkciji ulaznog parametra *target_pdr*, za *Random* topologije i FiT IoT-lab Grenoble topologiju. Sa porastom ovog parametra povećava se i procenat detektovanih paketa, koji je u nekim slučajevima manji od ciljane vrijednosti. Ovo se događa zbog interne interferencije, koja utiče na smanjenje procenta detektovanih paketa, o čemu je bilo riječi u poglavlju 3.1. Isprekidana crvena linija, na *Slikama 5.11 a) i b)*, prolazi kroz tačke na kojima se nalaze tražene vrijednosti procenta detektovanih paketa koje je potrebno dostići (10%, 15%, 20%, …, 95%). Interferencija onemogućava detekciju saobraćaja čak i kada se koriste idealni linkovi, pa je upravo na ovim visokim nivoima detekcije bolje vidljiv uticaj interne interferencije na smanjenje procenta detektovanih paketa. Oba tipa topologije pokazuju slične karakteristike pri detekciji paketa kada se primjenjuje parametar *target_pdr*. Kod slučajno generisanih topologija, procenat detektovanih paketa konstantno raste sa rastom parametra *target_pdr*, zbog toga što se za svaku od 100 simulacija generiše nova topologija i određuje se nova kombinacija snifera. Dok se kod FiT IoT-lab Grenoble topologije koristi samo jedna matrica konektivnosti, pa postoje nagle promjene procenta detektovanih paketa zbog neravnomjernog rasporeda kvaliteta linkova između snifera i senzora, slična karakteristika se može vidjeti i kod Metode I na *Slici 5.10*. *Za* visoke vrijednosti parametra *target_pdr*, varijacije procenta detektovanih paketa su manje, zbog stabilnih radio linkova koje grade sniferi.



a) *b)*

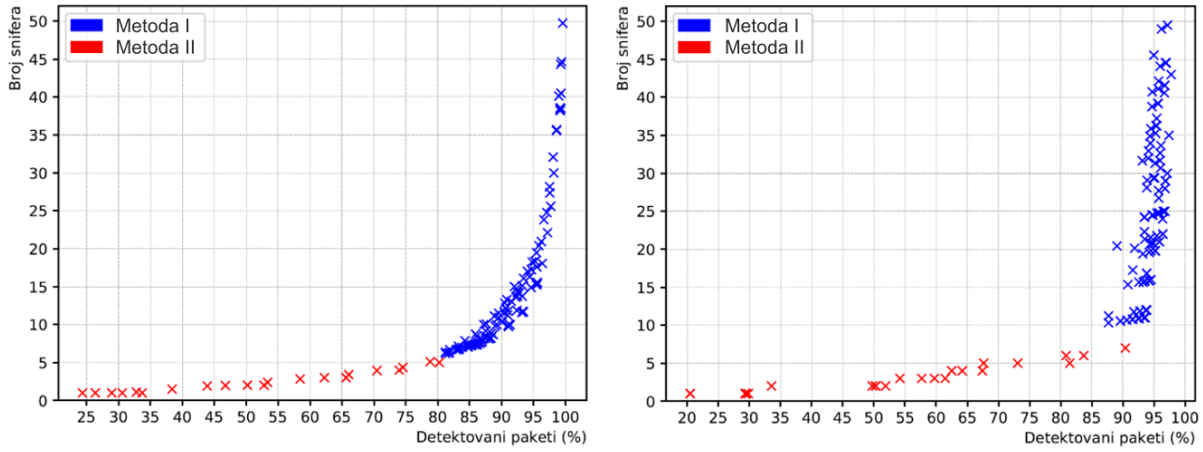
Slika 5.12 Procenat detektovanih paketa u odnosu na parametar number_of_sniffers; a) Random topologije; b) FiT IoT-lab Grenoble topologija

Slika 5.12 prikazuje promjene procenta detektovanih paketa, u funkciji ulaznog parametra *number_of_sniffers*, za *Random* topologije i FiT IoT-lab Grenoble topologiju. Metoda II pronalazi najbolju moguću kombinaciju sa zadatim brojem snifera. Veći broj snifera garantuje i veći procenat detektovanih paketa. Sa 2 snifera kod slučajnih topologija, moguće je detektovati oko 54% paketa, a sa 5 snifera oko 81% paketa. Kod FiT IoT-lab Grenoble topologije sa 2 snifera, detektovano je oko 51% paketa, a sa 5 oko 82% paketa.

U zavisnosti od mrežne topologije, potrebno je odabrati odgovarajući režim rada za Metodu II, kako bi se postigao željeni procenat detekcije paketa, ili na najbolji način iskoristili dostupni sniferi. Uz to treba voditi računa o broju kombinacija koje algoritam mora obraditi tokom rada, a on zavisi od broja snifera u mreži i ulaznih parametara. Takođe, napredniji procesori ili klaster računari mogu obraditi veći broj kombinacija, ako se rad podijeli na više jezgara, koji paralelno mogu vršiti obradu i pronaći najbolju kombinaciju lokacija za postavljanje snifera. Kada se koristi parametar *target_pdr* i nakon što algoritam dođe do tražene vrijednosti procenta detekcije paketa, efikasnije je nastaviti analizu i odrediti najbolju kombinaciju sa brojem snifera koji je u startu predložen. Na ovaj način može se postići bolji rezultat uz isti broj snifera, ako nastavak analize ne zahtijeva previše vremena u slučaju kada se koristi veliki broj snifera.

5.3 Poređenje Metode I i Metode II

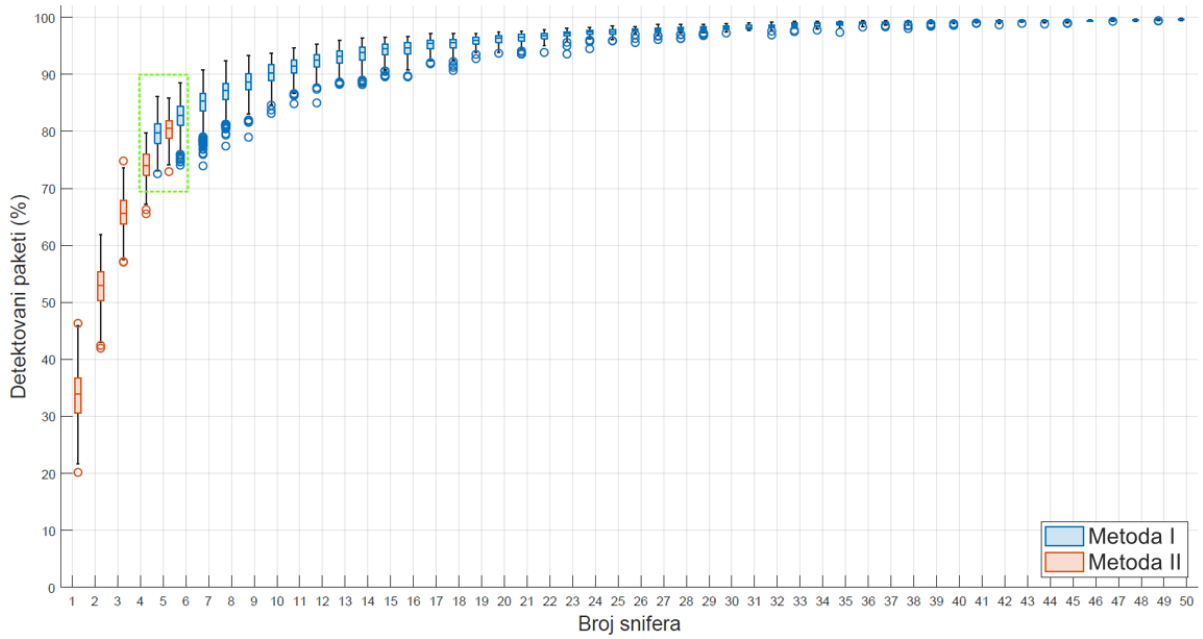
U ovom poglavlju je izvršena uporedna analiza obje metode sa svim dostupnim simulacionim podacima.



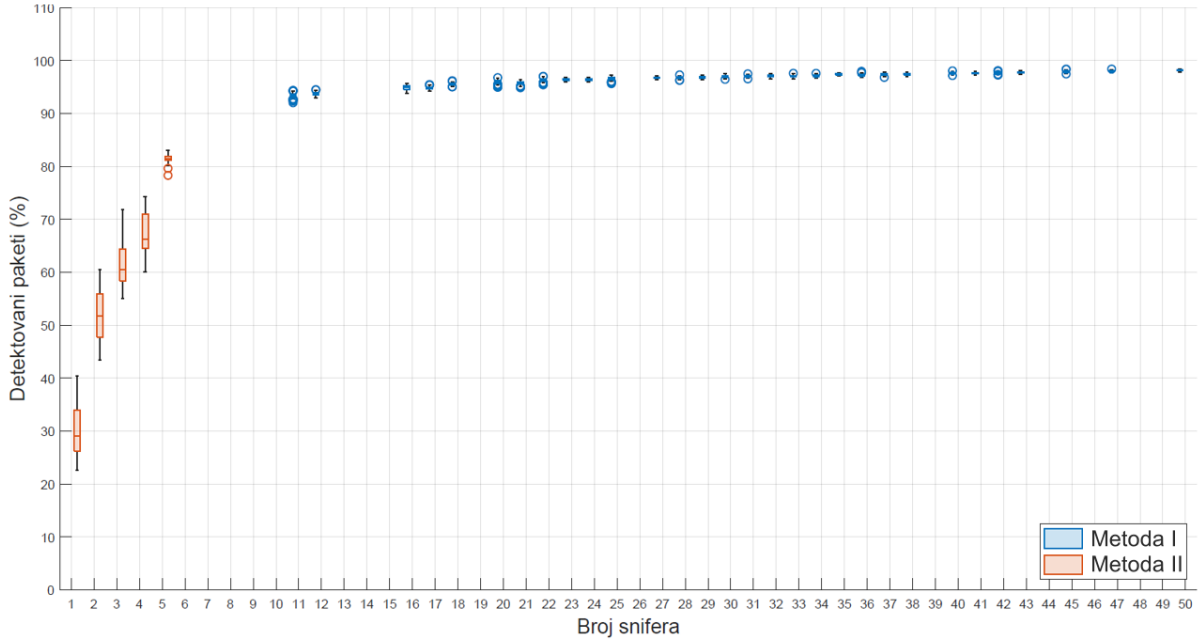
a) *b)*

Slika 5.13 Odnos prosječnog broja snifera i procenta detektovanih paketa za Metode I i II; a) za Random topologije; b) za FIT IoT-lab Grenoble topologiju

Slika 5.13 prikazuje odnos prosječnog broja snifera i prosječnog procenta detektovanih paketa, za *Random* i FIT IoT-lab Grenoble topologiju za Metode I i II. Kod slučajno generisanih topologija, moguće je pratiti krivu koja eksponencijalno raste i podaci iz Metode I se nastavljaju na podatke iz Metode II. Iako se na *Slici 5.13 a)*, rezultati dva algoritma ne preklapaju, na graničnoj vrijednosti Metoda II pokazuje bolje rezultate. Ovo se jasnije može vidjeti na *Slici 5.13 b)*, gdje je sa manjim brojem snifera, kod FIT IoT-lab Grenoble topologije moguće detektovati isti procenat saobraćaja. Sa 7 snifera je moguće detektovati oko 91% paketa sa Metodom II, dok je za detekciju istog procenta saobraćaja, pri korišćenju Metode I potrebno 11 snifera.



Slika 5.14 Procenat detektovanih paketa u odnosu na broj snifera, za obje metode za Random topologije



Slika 5.15 Procenat detektovanih paketa u odnosu na broj snifera, za obje metode za FIT IoT-lab Grenoble topologiju

Slike 5.14 i 5.15 prikazuju promjene procenta detektovanih paketa za različite vrijednosti broja snifera. Na *Slici 5.14*, za *Random* topologije, u označenoj zoni se vidi blaga prednost Metode II, koja sa istim brojem snifera ostvaruje bolji procenat detektovanih paketa.

Međutim, zbog pomenutog nedostatka, Metoda II je ograničena na određivanje lokacija za mali broj snifera. Dok Metoda I ne može određivati lokacije za mali broj snifera, jer za ove vrijednosti brija snifera nije moguće definisati MDS na svim kanalima. Na *Slici 5.15* prikazani su isti rezultati za FIT IoT-lab Grenoble topologiju, gdje nema jasnog preklapanja rezultata za dvije metode, ali se sa tendencijom rasta procenta detektovanih paketa kod Metode II može pretpostaviti njena prednost u odnosu na Metodu I.

Prednost Metode II po procentu detektovanih paketa u odnosu na Metodu I je očekivana, jer se kod druge metode pronalazi najbolja moguća kombinacija za dati broj snifera, ili za ciljani procenat detektovanog saobraćaja. Zato je Metodi II potrebno više vremena za određivanje lokacija za snifere, što predstavlja značajno ograničenje, a za veliki broj dostupnih snifera, WSNs sa velikim brojem senzora, ili visoke vrijednosti parametra *target_pdr,* dobijanje rezultata nije moguće. Metoda I predstavlja kompaktno rješenje kada je potrebno odrediti lokacije za veći broj snifera u mrežama sa velikim brojem senzora. Na ovaj način, Metode I i II pokrivaju sve vrijednosti broja snifera na graficima sa *Slike 5.14* i *5.15*.

Prilikom određivanja lokacija za snifere potrebno je odabrati odgovarajuću metodu i njene ulazne parametre. Kada je dostupan manji broj snifera (do 7) ili se koriste manje WSNs, Metoda II će predložiti rješenje koje će omogućiti detekciju većeg broja paketa nego Metoda I. U WSNs sa velikim brojem senzora i u slučajevima kada je dostupan veći broj snifera, Metoda II ne može obraditi veliku količinu podataka, zato je efikasnije koristiti Metodu I i podesiti njene ulazne parametre tako da se postigne željeni procenat detekcije paketa sa dostupnim brojem snifera.

Glava 6

Zaključak

Bežične senzorske mreže predstavljaju jednu od najaktuelnijih istraživačkih tema u oblasti telekomunikacija i tehnologije uopšte. Njihova primjena je moguća u različitim oblastima kao što su saobraćaj, zdravstvo, poljoprivreda, industrija i drugo. Aktivno se radi na unaprjeđenju i rješavanju različitih problema, kako bi se što prije omogućila primjena WSNs i iskoristili njihovi potencijali. Kreiranje protokola i standardizacija ove oblasti je od ključnog značaja, kako bi čitava naučnoistraživačka zajednica radila sinhronizovano i brže dolazila do rješenja.

WSNs se sastoje od jednostavnih i jeftinih čvorova koji međusobno komuniciraju, najčešće preko bežičnih radio linkova. Čvorovi mogu koristiti više vrsta senzora, kao što su biosenzori, termalni, mehanički, magnetni, optički i hemijski senzori, preko kojih mogu pratiti promjene različitih parametara iz okoline. Snimljene podatke mogu djelimično obrađivati, a zatim prosljeđivati ka korisnicima, direktno, putem Interneta, ili neke druge mreže. Kao izvor električne energije koriste se različite vrste baterija, koje imaju ograničen kapacitet. Zbog toga, senzorski čvorovi moraju biti energetski efikasni, kako bi njihov rad bio dugotrajan, bez potreba za čestim održavanjem. Cilj je da čvorovi mogu raditi i do 10 godina bez zamjene baterija.

WSNs se prije implementacije u realnim okruženjima, kao i tokom razvoja, moraju testirati. Testiranje se može vršiti simulacionim metodama, ili uz pomoć *testbed* platformi. Tokom testiranja, analize rada i praćenja performansi WSNs, kao i tokom razvoja novih standarda i protokola, neophodan je uvid u razmijenjeni paketski saobraćaj. Sniferi su uređaji koji mogu da vrše snimanje i analizu paketskog saobraćaja u višekanalnim WSNs. Međutim, da bi sniferi efikasno vršili monitoring u većim WSNs, u kojima jedan snifer ne može snimiti sav saobraćaj zbog prirode radio linkova, ograničene osjetljivosti prijemnika i interferencije, potrebno je definisati broj i pozicije snifera tako da hvataju što veći procenat saobraćaja. Tokom razmatranja potencijalnih lokacija za snifere u senzorskim mrežama, važno je da svi senzorski čvorovi imaju radio link većeg kvaliteta od definisane minimalne vrijednosti,

prema barem jednom sniferu. Na ovaj način, omogućava se uvid u saobraćaj koji se razmjenjuje između senzorskih čvorova.

U ovom radu su predstavljene dvije metode, koje omogućavaju određivanje pozicija, ili pozicija i broja snifera, u višekanalnim WSNs. Kao ulazni podatak za obje metode podrazumijevaju se matrice konektivnosti na svim frekvencijskim kanalima koji se koriste u mreži. Matrice konektivnosti pružaju uvid u stanje na svim radio linkovima koji povezuju senzorske čvorove, tj. dostupne su PDR vrijednosti linkova. Kao potencijalne lokacije za snifere, razmatraju se samo lokacije postojećih čvorova u mreži.

Prva metoda koristi teoriju grafova za analizu matrica konektivnosti, gdje čvorove u grafovima predstavljaju senzorski čvorovi iz mreže, a grane radio linkovi koji ih povezuju. Težinu svake grane određuju podaci iz matrice konektivnosti, tj. odgovarajuće PDR vrijednosti za svaki link. Pri određivanju pozicija za snifere, u ovoj metodi se koristi funkcija koja pronalazi minimalne dominantne skupove na svim kanalima, a kao rezultat daje se unija MDS na svim kanalima. Podešavanjem ulaznih parametara moguće je podešavati minimalni kvalitet linkova za MDS i prilagođavati broj snifera. Na ovaj način obezbjeđuje se uslov da svi senzori u mreži budu povezani sa bar jednim sniferom, sa linkom definisanog kvaliteta.

Druga metoda vrši analize matrica konektivnosti koristeći teoriju vjerovatnoće i kombinatoriku da bi se odredile lokacije na koje je potrebno postaviti snifere, tako da se može uhvatiti najveći procenat razmijenjenog saobraćaja. Ova metoda na osnovu ulaznih parametara, obrađuje sve moguće kombinacije za zadati broj snifera i odabira onu koja će omogućiti najveću vjerovatnoću detekcije paketa, ili traži kombinaciju koja će omogućiti traženu vjerovatnoću detekcije paketa.

Odgovarajući algoritmi za obje metode su realizovani u 6TiSCH Simulatoru kako bi se izvršila njihova analiza, pregled performansi i efikasnosti. Postojeće rješenje je prošireno, tako što je omogućena upotreba snifera u simulatoru i rad dva algoritma za određivanje pozicija na njih. Simulacije su vršene za različite vrijednosti ulaznih parametara i ponovljene su 100 puta da bi se dobili što kvalitetniji rezultati. Simulator može da generiše slučajne mrežne topologije sa matricama konektivnosti, ali postoji mogućnost korišćenja stvarnih matrica konektivnosti, koje su snimljene u realnim mrežnim okruženjima. Tokom testiranja korišćena su oba tipa matrica konektivnosti, u kojima se nalazi 50 senzorskih čvorova raspoređenih na prostoru od 750×750 metara.

Sa prvom metodom moguće je odrediti lokacije za snifere, koji omogućavaju detekciju oko 90% razmijenjenih paketa kod slučajnih topologija, kada se koristi od 10 do 15

snifera i oko 93.5% paketa kod topologije iz realnog mrežnog okruženja sa 13 snifera. Druga metoda omogućava detekciju oko 81% paketa sa 5 snifera za oba tipa mrežnih topologija. Druga metoda ostvaruje prednost u odnosu na prvu, kada se koristi manji broj snifera (do 7). Međutim, za određivanje lokacija kod druge metode potrebno je značajno više vremena, jer se obrađuje veliki broj kombinacija, pa ova metoda nije pogodna za velike mreže u kojima je potrebno koristiti veći broj snifera. Drugu metodu treba koristiti za manje mreže, ili mreže u kojima se koristi do 7 snifera. Prva metoda brže dolazi do predloga lokacija za snifere, ali sa njom nije moguće definisati lokacije za mali broj snifera. Pri izboru metode i ulaznih parametara, potrebno je razmotriti veličinu mreže, broj dostupnih snifera i procenat paketa koji je potrebno snimiti kako bi analiza mreže bila kvalitetna.

Literatura

[1] M. Ringwald, K. Romer, „Deployment of Sensor Networks: Problems and Passive Inspection," pp. 179-192, 2007.

[2] „IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)," *IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006),* pp. 1-314, 2011.

[3] X. Vilajosana, T. Watteyne, T. Chang, M. Vučinić, S. Duquennoy, P. Thubert, „IETF 6TiSCH: A Tutorial," *IEEE Communications Surveys & Tutorials,* t. 22, br. 1, pp. 595-615, 2020.

[4] J. Kovač, J. Crnogorac, E. Kočan, M. Vučinić, „Sniffing Multi-hop Multi-channel Wireless Sensor Networks," u *2020 28th Telecommunications Forum (TELFOR),* 2020.

[5] C. E. Nishimura, D. M. Conlon, „IUSS dual use: Monitoring whales and earthquakes using SOSUS," *Mar. Technol. Soc. J,* t. 27, br. 4, pp. 13-21, 1994.

[6] I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, E. Cayirci, „A survey on sensor networks," *IEEE Communications Magazine,* t. 40, br. 8, pp. 102-114, 2002.

[7] D. Jensen, „Aviation Today," 2002. [Na mreži]. Available: https://www.aviationtoday.com/2002/06/01/sivam-communication-navigation-and-surveillance-for-the-amazon/. [Poslednji pristup 2021].

[8] F. Group, „WirelessHART specification," 2007. [Na mreži]. Available: http://www.hartcomm2.org/.

[9] „ISA100: Wireless systems for automation," [Na mreži]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa100.

[10] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, M. Gidlund, „Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Transactions on Industrial Informatics,* t. 14, br. 11, pp. 4724-4734, 2018.

[11] A. Sharma, A. Banerjee, P. Sircar, „Performance analysis of energy-efficient modulation techniques for wireless sensor networks," u *2008 Annual IEEE India Conference*.

[12] „Wireless Sensor Network Market - Forecast(2021 - 2026)," [Na mreži]. Available: https://www.industryarc.com/Report/211/Wireless-Sensor-Network-Market-Research-Report.html. [Poslednji pristup 2021].

[13] I. Silicon Laboratories, „The Evolution of Wireless Sensor Networks," Silicon Laboratories, Inc, [Na mreži]. Available: https://www.silabs.com/documents/public/white-papers/evolution-of-wireless-sensor-networks.pdf. [Poslednji pristup 2021].

[14] N. R. Patel, S. Kumar, „Wireless Sensor Networks' Challenges and Future Prospects," u *International Conference on System Modeling & Advancement in Research Trends (SMART)*, Moradabad, India, 2018.

[15] 8. IEEE, „Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer," IEEE Standard, 2012.

[16] T. Watteyne, A. Mehta, K. Pister, „Reliability Through Frequency Diversity: Why Channel Hopping Makes Sense," u *Proceedings of the 6th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks*.

[17] T. Watteyne, C. Adjih, X. Vilajosana, „Lessons learned from large-scale dense IEEE802.15.4 connectivity traces," *CASE*, p. 145–150, 2015.

[18] J. Hui, P. Thubert, „Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks," RFC 6282, 2011.

[19] X. Vilajosana, T. Watteyne, T. Chang, M. Vučinić, S. Duquennoy, et al., „IETF 6TiSCH: A Tutorial," *Communications Surveys and Tutorials, IEEE Communications Society, Institute of Electrical and Electronics Engineers.*

[20] X. Vilajosana, K. Pister, T. Watteyne, „Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration," BCP 210, RFC 8180, 2017.

[21] Q. Wang, X. Vilajosana, T. Watteyne, „6TiSCH Operation Sublayer (6top) Protocol (6P)," RFC 8480, 2018.

[22] „Official Web site of the project OpenWSN," OpenWSN project, [Na mreži]. Available: https://openwsn.atlassian.net/wiki/spaces/OW/overview.

[23] Q. Wang, X. Vilajosana, T. Watteyne, „6TiSCH Operation Sublayer (6top) Protocol (6P)," 2018.

[24] X. Vilajosana, K. Pister, T. Watteyne, „Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration," BCP 210, rfc 8180, May, 2017.

[25] T. Chang, M. Vucinic, X. Vilajosana, S. Duquennoy, D. Dujovne, „Demo: Scheduling Function Zero on a 6TiSCH Network," u *International Conference on Embedded Wireless Systems and Networks (EWSN)*, Uppsala, Sweden, 20-22 February 2017.

[26] D. Fanucchi, B. Staehle, R. Knorr, „Network Formation for Industrial IoT: Evaluation, Limits and Recommendations," u *IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, September 2018.

[27] R. T. Hermeto, A. Gallais, F. Theoleyre, „On the (over)-Reactions and the Stability of a 6TiSCH Network in an Indoor Environment," u *Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, Montreal, QC, Canada, October 28 - November 02, 2018.

[28] G. Gardasevic, D. Vasiljevic, C. Buratti, R. Verdone, „Experimental Characterization of Joint Scheduling and Routing Algorithm Over 6TiSCH," u *2018 European Conference on Networks and Communications (EuCNC)*, 2018.

[29] R. T. Hermeto, A. Gallais, F. Theoleyre, „On the (over)-Reactions and the Stability of a 6TiSCH Network in an Indoor Environment," u *Proceedings of the 21st ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems*, Montreal, QC, Canada, 2018.

[30] D. Vasiljević, G. Gardašević, „Packet Aggregation-Based Scheduling in 6TiSCH Networks," u *IEEE EUROCON 2019 -18th International Conference on Smart Technologies*, 2019.

[31] M. Esteban, D. Glenn, M. Vucinic, S. Latré, J. Famaey, et al., „Simulating 6TiSCH Networks," u *Transactions on emerging telecommunications technologies*, 2018.

[32] K. Brun-Laguna, A.L. Diedrichs, D. Dujovne, R. Léone, X. Vilajosana, T. Watteyne, „(Not So) Intuitive Results from a Smart Agriculture Low-power Wireless Mesh Deployment," u *25–30ACM*, New York, NY, USA, 2016.

[33] X. Vilajosana, Q. Wang, F. Chraim, T. Watteyne, T. Chang, K. Pister, „A Realistic Energy Consumption Model for TSCH Networks," *IEEE Sensors Journal*, p. 482–489, 2014.

[34] T. Chang, M. Vučinić, X. Vilajosana, „6TiSCH Minimal Scheduling Function (MSF),“ draft-chang-6tisch-msf-00 [work-in-progress]: IETF, 2017.

[35] M. Vučinić, J. Simon, K. Pister, M. Richardson, „Minimal Security Framework for 6TiSCH,“ draft-ietf-6tisch-minimal-security-03 [work-in-progress]: IETF, 2017.

[36] Y. Tanaka, K. Brun-Laguna, T. Watteyne, „Trace-based simulation for 6TiSCH,“ *Internet Technology Letters Special Issue: Industrial Internet of Things,* t. 3, br. 4, 2020.

[37] „GitHub,“ OpenWSN, [Na mreži]. Available: https://github.com/openwsn-berkeley/opentestbed.

[38] „Industrial Shields,“ [Na mreži]. Available: https://www.industrialshields.com/shop/product/is-omb-001-openmote-b-721.

[39] „GitHub,“ Mercator: Dense Wireless Connectivity Datasets for the IoT, [Na mreži]. Available: https://github.com/openwsn-berkeley/mercator.

[40] „FIT IOT-LAB,“ [Na mreži]. Available: https://www.iot-lab.info/.

[41] K. Brun-Laguna, P. Minet, T. Watteyne, P. Henrique Gomes, „Moving Beyond Testbeds? Lessons (We) Learned About Connectivity,“ *IEEE Pervasive Computing,* t. 17, pp. 15-27, 2017.

[42] „BeamLogic,“ [Na mreži]. Available: http://www.beamlogic.com/802-15-4-siteanalyzer.

[43] M. Garey, D. Johnson, Computers and Intractability: A Guide to the Theory of NP-Completeness, New York, NY, United States: W. H. Freeman & Co., 1978.

[44] E. Municio, G. Daneels, M. Vučinić, S. Latré, J. Famaey, Y. Tanaka, K. Brun, K. Muraoka, X. Vilajosana, T. Watteyne, „Simulating 6TiSCH networks,“ u *Transactions on Emerging Telecommunications Technologies*, 2018.

[45] „FIT IOT-LAB,“ Inria, [Na mreži]. Available: https://www.iot-lab.info/legacy/deployment/grenoble/index.html.

[46] „CLEPS Cluster,“ Inria, [Na mreži]. Available: https://paris-cluster-2019.gitlabpages.inria.fr/cleps/cleps-userguide/index.html.

[47] A. Hagberg, D. Schult, P. Swart, „NetworkX, Network analysis in Python,“ [Na mreži]. Available: https://networkx.org/.

[48] J. Crnogorac, J. Kovač, E. Kočan, M. Vučinić, „d-Argus: a Distributed IEEE 802.15.4 Sniffer,“ u *27th Telecommunications Forum (TELFOR)*, Beograd, Srbija, 2019.

[49] „IEEE, 802.15.4-2015: IEEE Standard for Local and Metropolitan Area Networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer,“ IEEE Std., October, 2015.

[50] Y. Tanaka, K. Brun-Laguna, T. Watteyne, „Demo: Simulating a 6TiSCH Network using Connectivity Traces from Testbeds,“ u *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops*, Paris, France, 2019.

[51] M. R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. A. Grieco, G. Boggia, M. Dohler, „Standardized Protocol Stack for the Internet of (Important) Things,“ *IEEE Communications Surveys Tutorials,* t. 15, br. 3, pp. 1389-1406, December 2013.

Lista skraćenica

6LoWPAN – IPv6 over Low -Power Wireless Personal Area Networks

6TiSCH – IPv6 over the TSCH mode of IEEE 802.15.4e

6top – 6TiSCH Operation Sublayer Protocol

ACK – Acknowledgment

AI – Artificial Intelligence

ASN – Absolute Slot Number

ASN – Absolute Slot Number

AWACS – Airborne Warning and Control System

BDS – BeiDou Navigation Satellite System

CMOS – Complementary metal–oxide–semiconductor

CSMA/CA – Carrier Sense Multiple Access Collision Avoidance

CoAP – Constrained Application Protocol

CoJP – Constrained Join Protocol

DARPA – Defense Advanced Research Projects Agency

DES – Discrete Event Simulator

DIO – DODAG Information Objects

DS – Dominantan skup

DSN – Distributed Sensor Network

DSSS – Direct-sequence spread spectrum

EB – Enhanced Beacon

FES – Future Event Set

GLONASS – Global Navigation Satellite System

GPS – Global Positioning System

IEEE – Institute of Electrical and Electronics Engineers

IETF – Internet Engineering Task Force

IIOT – Industrial Internet of Things

IP – Internet protokol

IPv6 – Internet Protocol version 6

ISM – Industrial, Science and Medical

IoT – Internet of Things

LLN – Low-Power and Lossy

LR-WPANs – Low-Rate Wireless Personal Area Networks

MDS – Minimalan dominantan skup

MPF – Multipath Fading

MSF – Minimal Scheduling Function

NFC – Near Field Communication

OFDM – Orthogonal frequency-division multiplexing

PCE – Path Computation Element

PDR – Packet Delivery Ratio

RPL – IPv6 Routing Protocol for Low-Power and Lossy Networks

RSSI – Received Signal Strength Indicator

SAD – Sjedinjene Američke Države

SF – Scheduling Function

SF0 – Scheduling Function Zero

SINR – Signal-to-Interference-Plus-Noise Ratio

SIVAM – Amazon Surveillance System

SOSUS – Sound Surveillance System

TDMA – Time Division Multiple Access

TSCH – Time Slotted Channel Hopping

UWB – Ultra Wide Band

VPN – Virtual Private Network

V2V – Vehicle-to-vehicle

WLAN – Wireless Local Area Network

WSNs – Wireless Sensor Networks

Wi-Fi – Wireless-Fidelity

Ime i prezime autora: Jovan Crnogorac, Spec. Sci

E T I Č K A I Z J A V A

U skladu sa članom 22 Zakona o akademskom integritetu i članom 24 Pravila studiranja na postdiplomskim studijama, pod krivičnom i materijalnom odgovornošću, izjavljujem da je magistarski rad pod naslovom

"Predlog metoda za određivanje broja i pozicije snifera u višekanalnim bežičnim senzorskim mrežama"

moje originalno djelo.

Podnosilac izjave,

Jovan Crnogorac, Spec. Sci

U Podgorici, dana 12.01.2022. godine