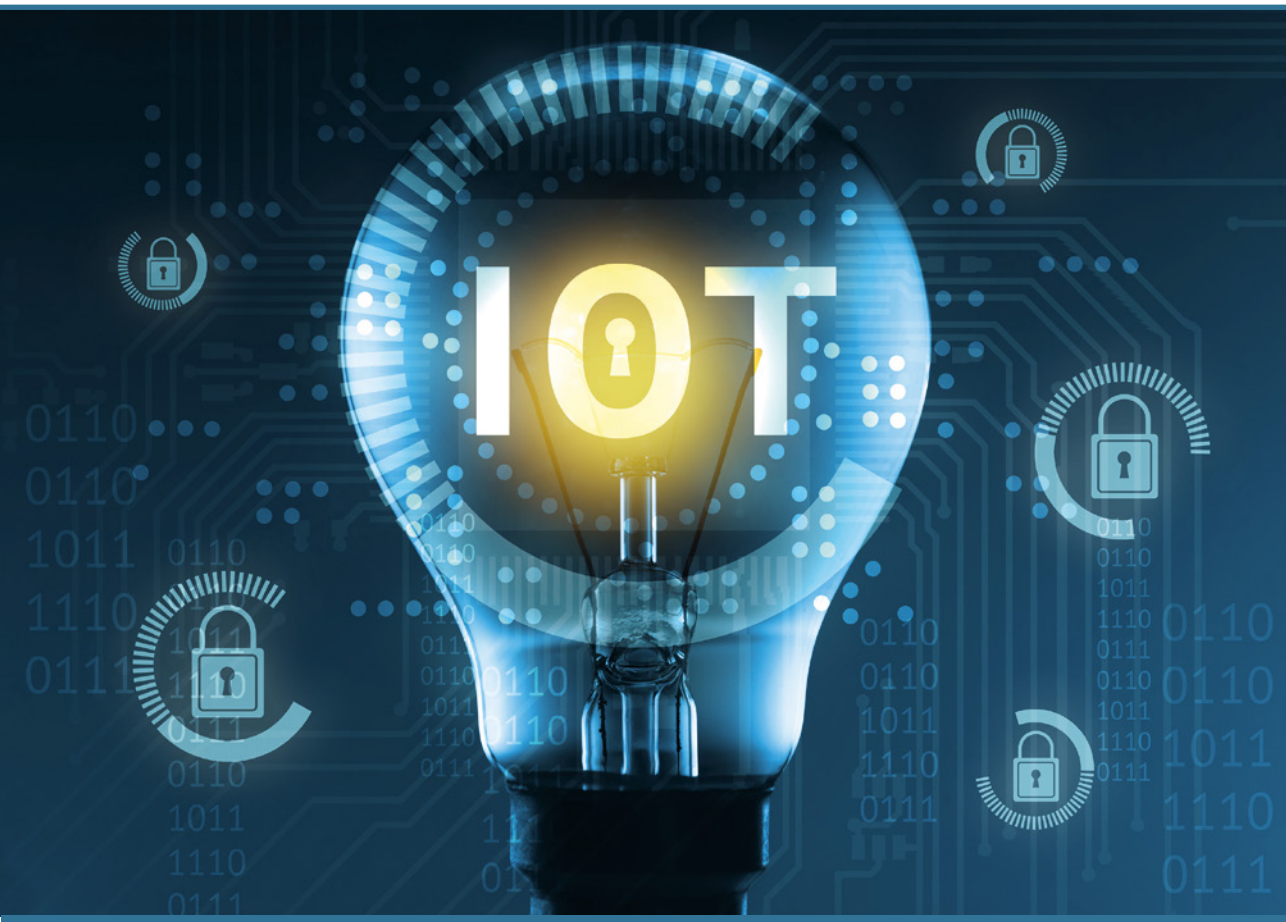
RĪGAS TEHNISKĀ UNIVERSITĀTE

Daniils Aleksandrovs-Moisejs

LIETU INTERNETA BEZVADU TĪKLU VEIKTSPĒJAS UN KIBERDROŠĪBAS NOVĒRTĒJUMS

Promocijas darba kopsavilkums



RTU Izdevniecība
Rīga 2025

RĪGAS TEHNISKĀ UNIVERSISTĀTE
Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultāte
Fotonikas, elektronikas un elektronisko sakaru institūts

Daniils Aleksandrovs-Moisejs
Doktora studiju programmas "Telekomunikācijas" doktorants

LIETU INTERNETA BEZVADU TĪKLU VEIKTSPĒJAS UN KIBERDROŠĪBAS NOVĒRTĒJUMS

Promocijas darbs kopsavilkums

Zinātniskais vadītājs
asociētais profesors *Dr. sc. ing.*
ALEKSANDRS IPATOVS

RTU Izdevniecība
Rīga 2025

Aleksandrovs-Moisejs, D. Lietu interneta bezvadu tīklu veiktspējas un kiberdrošības novērtējums. Promocijas darba kopsavilkums. – Rīga: RTU Izdevniecība, 2025. 49 lpp.

Publicēts saskaņā ar promocijas padomes "RTU P-08" 2025. gada 27. jūnija lēmumu, protokols Nr. 41.

Vāka attēls no *www.shutterstock.com*.

https://doi.org/10.7250/9789934372193
ISBN 978-9934-37-219-3 (pdf)

PROMOCIJAS DARBS IZVIRZĪTS ZINĀTNES DOKTORA GRĀDA IEGŪŠANAI RĪGAS TEHNISKAJĀ UNIVERSITĀTĒ

Promocijas darbs zinātnes doktora (*Ph. D.*) grāda iegūšanai tiek publiski aizstāvēts 2025. gada 21. novembrī plkst. 10.00 Rīgas Tehniskās universitātes Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultātē, Āzenes ielā 12, 201. auditorijā.

OFICIĀLIE RECENZENTI

Asociētais profesors *Dr. sc. ing.* Andis Supe,
Rīgas Tehniskā universitāte

Profesors *Dr. sc. ing. Rafael Asorey Cacheda*,
Kartahenas Politehniska universitāte, Spānija

Profesors *Dr.-Ing. habil. Mehmet Ercan Altinsoy*,
Drēzdenes Tehniskā universitāte, Vācija

APSTIPRINĀJUMS

Apstiprinu, ka esmu izstrādājis šo promocijas darbu, kas iesniegts izskatīšanai Rīgas Tehniskajā universitātē zinātnes doktora (*Ph. D.*) grāda iegūšanai. Promocijas darbs zinātniskā grāda iegūšanai nav iesniegts nevienā citā universitātē.

Daniils Aleksandrovs-Moisejs ……. (paraksts)
Datums: ……

Promocijas darbs ir uzrakstīts latviešu valodā, tajā ir ievads, piecas nodaļas, secinājumi, literatūras saraksts, 57 attēli, 22 tabulas, divi pielikumi, kopā 177 lappuses, ieskaitot pielikumus. Literatūras sarakstā ir 146 nosaukumi.

ANOTĀCIJA

Pēdējos gados *IEEE 802.11* un *IEEE 802.15.4* bezvadu jeb sensoru tīkla kombinācija ir plaši izplatīti dažādos lietojumos, tostarp lietu interneta (*IoT*), viedo māju sistēmās un kritiski svarīgās infrastruktūrās, piemēram, zinātnes, industrijas un medicīnas nozarēs. Šādi tīkli nodrošina ērtu un elastīgu datu pārraides vidi, taču to izmantošana ir saistīta ar vairākām drošības un veiktspējas problēmām. *IEEE 802.15.4* standarts, kas ir pamatā tādiem protokoliem kā *Zigbee*, ir strādāts darbībai zemas jaudas sensoru tīklos, nodrošinot datu pārraidi vidē ar ierobežotiem skaitļošanas resursiem. Tomēr zems enerģijas patēriņš un relatīvi zemā caurlaidspējas josla padara *IEEE 802.15.4* tīklus neaizsargātus pret fiziskā slāņa (*PHY*) un datu posma slāņa (*MAC*) uzbrukumiem, piemēram, pakešu injekciju un pakalpojuma atteikuma (*DoS*) uzbrukumiem.

Promocijas darbā aplūkoti kiberdrošības un caurlaidspējas aspekti *IEEE 802.15.4* tīklos, galveno uzmanību pievēršot standarta radīto uzbrukumu analīzei un neitralizēšanas metodēm. Pētījums ietver *Zigbee* tīkla caurlaidspējas eksperimentālu novērtēšanu, pamatojoties uz Šenona teorēmu, ņemot vērā tādus faktorus kā pieskaitāmās izmaksas, sekmīgas pakešu pārraides varbūtība un kanāla izmantošanas līmenis. Lai novērtētu traucējumu un uzbrukumu ietekmi uz tīklu, tika izmantota Nakagami sadalījumā balstīta statistiskā modelēšanas metode. Eksperimentos tika analizēti uzbrukumi tīklam, piemēram, pakešu injekcijas, *DoS* uzbrukumi un signāla traucēšana. Lai aizsargātu tīklu, tika izmantots pakešu monitorēšanas modulis *CC2531* un uzbrukumu bloķēšanas metodes, lietojot papildu uzraudzības ierīces un radiofrekvences (RF) traucējumu ģenerēšanu.

SATURS

IZMANTOTIE SAĪSINĀJUMI 6
PROMOCIJAS DARBA VISPĀRĒJS RAKSTUROJUMS 9
Tēmas aktualitāte 9
Darba mērķis un uzdevumi 10
Pētījumu metodika 11
Pētījumu rezultāti un zinātniskā novitāte 11
Promocijas darba aizstāvamās tēzes 13
Rezultātu aprobācija 14
Darba apjoms un struktūra 14
PROMOCIJAS DARBA SATURS 16
Pirmā nodaļa 16
Otrā nodaļa 21
Trešā nodaļa 23
Ceturtā nodaļa 30
Piektā nodaļa 32
PROMOCIJAS DARBA SECINĀJUMI 40
IZMANTOTĀS LITERATŪRAS SARAKSTS 44

IZMANTOTIE SAĪSINĀJUMI

A
AES (*Advanced Encryption Standard*) – uzlabots šifrēšanas standarts
AI (*Artificial Intelligence*) – mākslīgais intelekts
AMQP (*Advanced Message Queuing Protocol*) – uzlabots ziņojumu rindas protokols
AP (*Access Point*) – piekļuves punkts

B
BMS (*Building Management System*) – ēku pārvaldības sistēma
BPSK (*Binary Phase Shift Keying*) – binārā fāzes nobīdes modulācija

C
CoAP (*Constrained Application Protocol*) – ierobežoto lietojumprogrammu protokols
CRC (*Cyclic Redundancy Check*) – cikliskās redundances pārbaude
CRR (*Critical Response Rate*) – kritiskās reakcijas ātrums
CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance)* – nesēja jušanas un sadursmju nepieļaušanas daudzpieeja

D
DDoS (*Distributed Denial of Service*) – izkliedētais pakalpojumu atteices uzbrukums
DoS (*Denial of Service*) – pakalpojumu atteices uzbrukums
DSSS (*Direct Sequence Spread Spectrum*) – tiešās secības izkliedētais spektrs

F
FOTA (*Firmware Over-The-Air*) – programmatūras atjaunināšana pa gaisu
FHSS (*Frequency Hopping Spread Spectrum*) – frekvenču lēcienu izkliedētais spektrs

G
GPIO (*General Purpose Input/Output*) – universālais ieejas/izejas ports

H
HTTP (*Hypertext Transfer Protocol*) – hiperteksta pārsūtīšanas protokols

I
IaaS (*Infrastructure as a Service*) – infrastruktūra kā pakalpojums
IDS (*Intrusion Detection System*) – ielaušanās noteikšanas sistēma
IEEE (*Institute of Electrical and Electronics Engineers*) – Elektrotehnikas un elektronikas inženieru institūts
IoT (*Internet of Things*) – lietu internets
ISM (*Industrial, Science and Medical*) – rūpniecība, zinātne un medicīna
IT (*Information Technology*) – informācijas tehnoloģijas
IPS (*Intrusion Prevention System*) – ielaušanās novēršanas sistēma

L
LAN (*Local Area Network*) – lokālais datortīkls
LLC (*Logical Link Control*) – loģiskās saites vadība
LoRaWAN (*Long Range Wide Area Network*) – tālas darbības diapazona platjoslas tīkls
LQI (*Link Quality Indicator*) – savienojuma kvalitātes indikators

M
MAC (*Media Access Control*) – multivides piekļuves kontrole
MAE (*Mean Absolute Error*) – vidēja absolūtā kļūda
MIMO (*Multiple Input Multiple Output*) – vairāku ievadu un izvadu tehnoloģija
ML (*Machine Learning*) – mašīnmācīšanās
MQTT (*Message Queuing Telemetry Transport*) – viegls ziņojumu pārraides protokols

O
OAuth (*Open Authorization*) – atvērtās autorizācijas protokols
OFDM (*Orthogonal Frequency Division Multiplexing*) – ortogonālā frekvenču dalīšanas multiplēšana
OFDMA (*Orthogonal Frequency Division Multiple Access*) – ortogonālā frekvenčdales daudzpiekļuve
OLS (*Ordinary Least Squares*) – parastā mazāko kvadrātu metode
OSI (*Open Systems Interconnection*) – atvērtās sistēmas savienojuma modelis

P
PHY (*Physical Layer*) – fiziskais slānis

Q
QAM (*Quadrature Amplitude Modulation*) – kvadrātiskā amplitūdas modulācija
QoS (*Quality of Service*) – pakalpojuma kvalitāte

R
RADIUS (*Remote Authentication Dial-In User Service*) – attālinātās autentifikācijas pakalpojums
RBAC (*Role-Based Access Control*) – lomās balstīta piekļuves kontrole
RF (*Radio Frequency*) – radiofrekvence
RMSE (*Root Mean Square Deviation*) – vidējā kvadrātiskā novirze
RSA (*Rivest-Shamir-Adleman*) – publiskās atslēgas šifrēšanas algoritms
RSSI (*Received Signal Strength Indicator*) – uztvertā signāla stipruma indikators

S
SDR (*Software-Defined Radio*) – programmatūras definēts radio
SSH (*Secure Shell*) – droša čaula
SNR (*Signal-to-Noise Ratio*) – signāla un trokšņa attiecība
SSL (*Secure Sockets Layer*) – drošības ligzdu slānis

T
TCP / IP (*Transmission Control Protocol / Internet Protocol*) – pārsūtīšanas vadības protokols / interneta protokols
TLS (*Transport Layer Security*) – transporta slāņa drošība

U
URH (*Universal Radio Hacker*) – universālais radio uzlauzējs
USB (*Universal Serial Bus*) – universālā seriālā kopne

V
VLAN (*Virtual Local Area Network*) – virtuālais lokālais tīkls

W
WLAN (*Wireless Local Area Network*) – bezvadu lokālais tīkls
WI-FI (*Wireless Fidelity*) – bezvadu uzticamība
WPA2 (*Wi-Fi Protected Access 2*) – *Wi-Fi* aizsardzības 2. versija
WPA3 (*Wi-Fi Protected Access 3*) – *Wi-Fi* aizsardzības 3. versija

PROMOCIJAS DARBA VISPĀRĒJS RAKSTUROJUMS

Tēmas aktualitāte

Mūsdienās viedās mājas un ēku vadības sistēmas tiek plaši ieviestas gan privātmājās, gan rūpnieciskā vidē, nodrošinot centralizētu elektrības piegādes, apgaismojuma, apkures, ūdensapgādes, drošības un citu dzīves funkcijas pārvaldību. Tādas sistēmas kā lietu internets (angļu val. *Internet of Things – IoT*) un ēku vadības sistēmas (angļu val. *Building Management System – BMS*) sniedz plašas iespējas ēku/dzīvokļu automatizācijā un attālinātā pārvaldībā [1]–[3]. Tās ievērojami atvieglo dzīvi gan apsaimniekotajiem, gan galalietotājiem, pateicoties vadības paneļiem, mobilajām lietotnēm un tīkla risinājumiem.

Pārvaldības risinājumi mūsdienās strauji attīstās, taču drošības aspekti bieži tiek atstāti novārtā. Nereti lietotāji pieņem, ka pietiek ar sarežģītu paroli vai kanāla šifrēšanu, piemēram, transporta slāņa drošību (angļu val. *Transport Layer Security – TLS)*, lai nodrošinātu sistēmu. Sistēmas tiek uzlauztas ne tikai no ārpuses, bet arī no iekšpuses, piemēram, ja lietotājs, kuram nepatīk pārvaldnieks un kuram ir zināšanas informācijas tehnoloģijas (angļu val. *Information Technology – IT*) jomā, spēj iegūt piekļuvi tīklam un sistēmai. Tādos gadījumos labāk izmantot tīkla vārtus (angļu val. *bridge*), kur ir ieviesti segmentēti virtuāli lokālie tīkli (angļu val. *Virtual Local Area Network – VLAN*) vai ugunsmūri (angļu val. *firewall*) ar detalizētu piekļuves kontroli [4].

Īpaši satraucoša ir problēma ar "aizmugurējām durvīm" (angļu val. *backdoor*) – bieži tiek izmantotas lētākās, īpaši *IoT* ierīcēs. Tās var būt gan apzināti iebūvētas ražošanas laikā, gan pievienotas lietotāju neapzinātas konfigurācijas rezultātā, piemēram, atstājot aktīvu attālināto piekļuvi (angļu val. *Secure Shell – SSH*), novecojušu šifrēšanas protokolu vai nedrošus noklusējuma iestatījumus. Kiberdrošībā ar "aizmugurējām durvīm" saprot jebkuru ievainojamību, kas ļauj apiet autentifikāciju un iekļūt sistēmā bez īpašnieka ziņas [5]–[7].

Arī lietotāju neuzmanība ir biežs apdraudējumu avots – lietotāji pieslēdzas no nedrošām ierīcēm, izmanto vienkāršas paroles vai atver kaitīgas saites, tādējādi ielaižot vīrusus un spiegprogrammatūru tīklā. Ja organizācijas ugunsmūrī nav korekti konfigurētu piekļuves noteikumu, ir aptuveni 50–70 % iespēja, ka sistēmas tiks inficēta ar ļaunprogrammatūru.

Tādēļ informatīvā drošība jāskata ne tikai kā tehniskais izaicinājums, bet arī kā organizatoriska un lietotāju uzvedības problēma. Jāveicina izpratne par drošības pamatprincipiem – konfidencialitāti, integritāti un pieejamību (angļu val. *Confidentiality, Integrity, and Availability – CIA Triad*) – un jāievieš vairāku līmeņu aizsardzības mehānismi – gan loģiski (šifrēšana,

autentifikācija, ugunsmūri), gan fiziski (iekārtu kontrole, piekļuves ierobežojumi), gan administratīvi (drošības politikas, lietošanas noteikumi un apmācības) [8].

Promocijas darba pētījuma aktualitāti nosaka nepieciešamība izstrādāt un testēt praktiskus aizsardzības mehānismus *IoT* tīklos, īpaši *Zigbee* standarta vidē, kurā dominē lētas ierīces ar zemiem aizsardzības standartiem. Tīkliem jābūt ne tikai strādājošiem, bet arī izturīgiem pret dažāda veida kiberdraudiem, piemēram, pakešu injekciju (angļu val. *packet injection*) vai signāla traucēšanas (angļu val. *signal jamming*), kas spēj traucēt vai bloķēt sistēmas darbu [3], [9], [10].

Darba mērķis un uzdevumi

Pamatojoties uz *IoT* tīklu drošības un veiktspējas problēmu analīzi, tika definēts **promocijas darba mērķis** – teorētiski novērtēt lietu interneta (*IoT*) tīkla veiktspēju, kiberdrošības politiku un uzbrukumu veidus, eksperimentāli izveidot *IoT* tīklu ar noteiktu ierīču skaitu un analizēt tā vājās vietas, izmantojot ievainojamību testēšanas rīkus, *Python* programmēšanu un Nakagami sadalījumu.

Lai sasniegtu definēto mērķi, bija nepieciešams veikt vairākus **pamatuzdevumus**.

1. Izpētīt mūsdienu bezvadu *IoT* tīklu standarta veiktspēju un salīdzinoši analizēt *IEEE 802.15.4* standarta pamatprincipus, veiktspējas raksturlielumus un ar tiem saistītos kiberdrošības riskus.
2. Izstrādāt un ieviest eksperimentālu hibrīdā *IoT* tīkla darbības modeli ar noteiktu skaitu sensoru ierīču, lai testētu to savietojamību, darbības stabilitāti un caurlaidspēju.
3. Analizēt *IEEE 802.15.4* standarta datu pārraides veiktspēju eksperimentālā tīklā, izmantojot pakešu monitorēšanas ierīces un autora izstrādātu *Python* datu apstrādes rīku.
4. Veikt *IEEE 802.15.4* tīkla ievainojamību testēšanu, simulējot dažāda veida tīkla traucējumus, izmantojot *RZUSBSTICK* un pielāgotu *Python* palaišanas programmu signāla stipruma un caurlaidspējas novērtēšanai.
5. Veikt *IEEE 802.15.4* tīkla uzbrukumu modelēšanu un izstrādāt aizsardzības mehānismus, pamatojoties uz *CC2531* uztverto datu un *HackRF One* frekvences manipulācijas iespējām.
6. Izmantojot Nakagami sadalījumu un tā parametrus, matemātiski modelēt *IEEE 802.15.4* tīkla veiktspēju atbilstoši Šenonas teorēmai dažādos stāvokļos (normālā un uzbrukuma režīmā).

7. Balstoties eksperimentālajos rezultātos, veikt *IEEE 802.15.4* tīkla simulāciju *Python* vidē un salīdzināt ar teorētiskajiem modeļiem, fokusējoties uz kiberdrošības indikatoriem un datu pārraides caurlaidspēju.
8. Izvērtēt eksperimentālos un simulācijas rezultātus, formulēt galvenos secinājumus un sniegt rekomendācijas kiberdrošības paaugstināšanai *IEEE 802.15.4* tīklos.

Pētījumu metodika

Promocijas darba izstrādes gaitā, lai īstenotu definētos uzdevumus un analītiski izvērtētu konstatētās problēmas, tika veikti eksperimentāli mērījumi un izstrādātas programmēšanas pieejas, vienlaikus ņemot vērā kiberdrošības politikas aspektu. Testa vidē tika izmantoti tādi rīki un ierīces kā *RZUSBstick*, *CC2531* ar *KillerBee* bibliotēku, *HackRF One*, dažādi *ZigBee* mezgli, *Raspberry Pi* un *Kali Linux* vide, kā arī *Python* programmēšanas valoda. Datu pakešu analīzei tika izmantots *Wireshark*, savukārt, lai modelētu un testētu dažādus uzbrukuma un aizsardzības scenārijus, tika izveidoti gan vadu, gan bezvadu (*IEEE 802.15.4 ZigBee*) tīkli. Šāda pieeja ļauj sekmīgi novērtēt *IoT* ierīču savstarpējo mijiedarbību un identificēt iespējamās drošības ievainojamības, kā arī izstrādāt atbilstošus aizsardzības mehānismus.

Matemātiskie aprēķini veikti, izmantojot *Python* programmatūru ar matemātikas bibliotēkām (*matplotlib, scipy*), savukārt eksperimentālo mērījumu rezultātu statistiskā apstrāde veikta *Excel* vidē.

Eksperimentu veiksmīgai pabeigšanai izmantotās *Python* palaišanas programmas (*Zigbee* tīkla uzraudzībai, uzbrukumu veikšanai un to novēršanai) ir pieejamas publiskajā *Github* repozitorijā: *https://github.com/DannyAlmois/PhD_IoT_Zigbee_Cybersecurity*.

Pētījumu rezultāti un zinātniskā novitāte

Promocijas darba praktiskā vērtība un jaunieguvumi

1. Polinomu un hibrīdmodeļa tendences izmantošana, lai apskatītu tīkla darbspējas atjaunošanas procesus pretpasākuma ierīces uzbrukuma laikā. Eksperimenti liecina, ka klasiskās lineāras tendences nevar aprakstīt atjaunošanas dinamiku, jo uzbrukuma process un paketes sūtīšana nav vienmērīgi. Tika izmantoti kvadrātiski un kubiski polinomi, lai modelētu svārstības atjaunošanas procesos un hibrīdmodelī, kas padziļināti apraksta tīkla atjaunošanas posmu, ņemot vērā ārējos parametros.

2. Tika veikta visaptveroša analīze modificētam *DoS* uzbrukumiem, traucēšanas un pakešu injekcija *IEEE 802.15.4* tīklā, izmantojot pielāgotu programmatūru un jaunas palaišanas programmas *Python* vidē. Tika izstrādāta aizsardzības metode, kas balstīta dinamiskā uzraudzībā un adaptīvā traucēšanā, izmantojot *CC2531* un *SDR* moduli pēc konkrētu pakešu kadru vai anomālu uzbrukumu darbībām, kas palielināja izturību pret uzbrukumiem līdz 60–95 % atkarībā no uzbrukuma veida un līdz 30 % samazināja caurlaidspējas atjaunošanas laiku.
3. Izstrādātais uzbrukuma simulācijas modelis ļauj testēt traucēšanas, pakešu injekcijas un *DoS* uzbrukumus bez fiziskas aparatūras, emulējot līdz 30 ierīcēm simulācijas tīklā. Salīdzinot ar reālajiem eksperimentiem, pretpasākumu precizitāte sasniedza 95 %, padarot modeli par efektīvu rīku aizsardzības mehānismu testēšanai un turpmākajiem pētījumiem.
4. Pētījumā tika izmantots Nakagami sadalījuma modelis ar fiksētiem parametriem (m = 0,8, Ω = 0,3), kas bija izvēlēti, jo tie atbilst reāliem iekštelpu apstākļiem, kur *IEEE 802.15.4* tīkli darbojas ar daudzceļu izplatīšanos un signāla traucējumiem, kas raksturīgi viedajām mājām un *IoT* vidēm, lai analizētu uzbrukumu ietekmi uz tīkla signāla stiprumu un caurlaidspēju. Neskatoties uz parametriem, modelēšana spēja atspoguļot signāla stabilitātes vājinājumu un paaugstinātu pakešu zudumu varbūtību uzbrukumu laikā, parādot tīkla jutīgumu pret dažādiem uzbrukumu veidiem.

Promocijas darba galvenie secinājumi

1. Integrēta *WLAN* un *IoT* sakaru tīkla izveide, izmantojot *Raspberry Pi* un *IoT* maršrutētājus *RaspBee II*, ir tehniski un ekonomiski pamatota. Šī pieeja ļauj vienkārši pieslēgties *Raspberry Pi* mikrokontrolierim, izmantojot *SSH* savienojumu, kas atvieglo attālināto piekļuvi un nodrošina iespēju attālināti pārvaldīt tīklu.
2. Tika izstrādāti aizsardzības mehānismi, tostarp ļaunprātīgu pakešu dinamikas traucēšana, adaptīvas datu plūsmas filtrēšana un tīkla kanāla darbības uzraudzība. Tādi pasākumi spēja daļēji atjaunot tīkla caurlaidspēju pēc uzbrukumiem un nodrošināt stabilu datu pārraidi pat pastāvīgu draudu gadījumā.
3. Īstenotie aizsardzības mehānismi demonstrēja augstu efektivitāti pret dažāda vieda uzbrukumiem. *IoT* tīkls uzrādīja visaugstāko noturību pret pakešu injekcijas uzbrukumiem, reālajā vidē sasniedzot 94,83 %, savukārt simulācijā – tikai 85,14 %.
4. Traucēšanas uzbrukumu veida gadījumā izturība bija 60,11 % tīklā un 78,05 % simulācijā, kas apstiprina ierosināto ļaunprātīgo signālu filtrēšanas un traucēšanas metožu panākumus.

5. Visgrūtāk bija novērst *DoS* uzbrukumus, jo aizsardzības efektivitāte bija tikai 47,75 %, savukārt simulācijā *DoS* uzbrukumu pretpasākuma rādītājs sasniedza 93,33 %, uzsverot to, ka testa rezultātus ietekmēja gan aparatūras ierobežojumi, gan ārējie traucējumi.
6. Salīdzinošā simulācijas un reālās vides analīze parādīja aizsardzības mehānismu efektivitātes atšķirības. Simulācijas vidē efektivitāte bija augstāka, jo nebija ārējo faktoru un aparatūras ierobežojumu, savukārt reālos apstākļos bija iespējams novērtēt *DoS* un signāla traucēšanas uzbrukumu atklāšanas un bloķēšanas sarežģītību.
7. Nakagami sadalījuma lietošana, lai analizētu uzbrukumu ietekmi uz tīkla caurlaidspēju un *RSSI*, ļāva simulēt trafika signāla uzvedību dažādos uzbrukumu scenārijos. Fiksētu parametru izmantošana ļāva novērtēt signāla stabilitātes samazināšanos un pakešu zudumu varbūtības palielināšanos, kas bija īpaši redzama traucēšanas uzbrukumu apstākļos.
8. Tika izveidota *Python* simulācijas vide, lai modelētu uzbrukumus un novērtētu aizsardzības mehānismu efektivitāti. Simulācijā tika atveidoti uzbrukumu veidu scenāriji ar 95 % precizitāti, salīdzinot ar reāla tīkla rezultātiem. Tas ļāva veikt detalizētu tīkla uzvedības analīzi pārslodzes apstākļos, neizmantojot fiziskas iekārtas.
9. Analizējot uzbrukumu ietekmi uz tīklu, tika konstatēts, ka *DoS* uzbrukumu un traucēšanas uzbrukumu rezultātā caurlaidspēja samazinājās par 40–60 % un tīkla atjaunošana pēc uzbrukumiem bez aizsardzības mehānismiem bija par 30 % ilgāka. Polinomu un hibrīdmodeļu tendenču izmantošana ļāva ar augstu precizitāti $R^2 = 0,96$ prognozēt tīkla atjaunošanas procesu un optimizēt stratēģijas uzbrukumu seku novēršanai.

Promocijas darba aizstāvamās tēzes

1. Viens no uzbrukuma scenārijiem lietu interneta (*IoT*) hibrīdtīklam ir mākslīgi samazināt signāla stiprumu (*RSSI*) līdz aptuveni –90 dBm, kas var izraisīt būtiskus tīkla darbības traucējumus. Šādu uzbrukumu ir iespējams identificēt un novērst ar efektivitāti līdz pat 90 %, izmantojot aizsardzības moduli, kas bāzēts *HackRF One*.
2. Izmantojot *CC2531* monitorēšanas moduli *Zigbee* 15. kanālā (2,425 GHz), iespējams identificēt *RSSI* līmeņa izmaiņas un pakešu plūsmas traucējumus, kas izraisa daļēju tīkla darbības paralīzi un pārraides kārtības traucējumus definētu uzbrukumu rezultātā.
3. Pamatojoties uz pieņēmumu, ka signāla vājinājumu slēgtās telpās iespējams ticami modelēt ar Nakagami sadalījumu, var prognozēt līdz pat 20 % lielāku signāla stiprumu (*RSSI*), salīdzinot ar faktiskajiem, eksperimentāli mērītajiem signāla stipruma (*RSSI*) rādītājiem.

Rezultātu aprobācija

Promocijas darba pētījumi un rezultāti prezentēti trīs starptautiskās zinātniskās konferencēs un divos RTU SZTK pasākumos, kā arī atspoguļoti vienā publikācijā zinātniskajā žurnālā un divās publikācijās konferenču materiālos.

Publikācijas zinātniskajos žurnālos

Aleksandrovs-Moisejs, D., Ipatovs, A., Grabs, E., Rjazanovs, D. Evaluationof a Long-Distance IEEE 802.11ah Wireless Technology in Linux Using Docker Containers. Elektronika ir elektrotechnika = Electronics and Electrical Engineering, 2022, Vol. 28, No. 3, 71.–77. lpp.

Publikācijas pilna teksta konferenču rakstu krājumos

1. **Aleksandrovs-Moisejs, D**., Ipatovs, A., Grabs, E., Rjazanovs, D., Siņuks, I.Arduino-Based Temperature Sensor Organization and Design. No: 2023 Photonics & Electromagnetics Research Symposium (PIERS 2023):Proceedings, Čehija, Prāga, 3.–6. jūlijs, 2023.
2. **Aleksandrovs-Moisejs, D.,** Grabs, E., Chen, T., Beļinskis, R., Bogdanovs, N., Kārkliņš, T., Klūga, J., Stetjuha, M., Ipatovs, A. Arduino-based Implementation and Design of Modern Temperature Measurements Sensor Environments. In: 2024 Photonics & Electromagnetics Research Symposium (PIERS 2024): Proceedings, Ķina, Čendu, 21.–25. aprīlis, 2024.

Darba apjoms un struktūra

Promocijas darbā ir 177 lappuses. Darbā ir piecas nodaļas, nobeigums, literatūras saraksts un divi pielikumi.

Darba pirmajā nodaļā analizēti mūsdienu bezvadu tīkli un arhitektūra, standarta darbības principi un īpašības, īpašu uzmanību pievēršot *IEEE 802.11* un *IEEE 802.15.4* tīkliem, funkcijām un topoloģijām, protokoliem un integrācijas iespējām *IoT* ekosistēmā. Nodaļā aplūkotas arī šo tīklu galvenās ievainojamības fiziskajā (*PHY*) un datu kanāla (*MAC* un *LLC*) slānī, kā arī kopīgās drošības problēmas.

Darba otrajā nodaļā veiktas *IEEE 802.11/802.15.4* tīklu uzbrukuma veidu analīzes, tostarp *DoS* uzbrukumi, pakešu injekcijas un signāla traucēšanas uzbrukumi. Detalizēti aprakstīti katra uzbrukuma darbības principi, īstenošanas metodes un sekas uz tīkla darbību atbilstoši *RSSI* un tīkla caurlaidspējas mērījumiem. Nodaļā analizētas arī esošās metodes uzbrukumu atklāšanai un novēršanai, kā arī pretpasākuma efektivitāte.

Trešajā nodaļā aprakstīta pētījuma eksperimentālā metodoloģija, tostarp testa tīkla arhitektūra, izmantotā aparatūra un programmatūra. Nodaļā aprakstīti arī uzbrukuma rīki (*RZUSBSTICK*, *CC2531*, *HackRF One*), uzraudzības rīki *Wireshark* un izstādātie *DoS*, traucēšanai un pakešu injekcijai paredzētās palaišanas programmas. Nodaļā sniegti arī modelēšanas parametri *Python* simulācijas vidē un eksperimentu metodoloģija – *RSSI* un caurlaidspējas mērīšana (izmantojot empīrisko Šenona teorēmu).

Ceturtajā nodaļā sniegta detalizēta iegūto datu analīze, tostarp uzbrukumu ietekme uz savienojuma kvalitāti, caurlaidspēju un tīkla stabilitāti, kā arī eksperimentu rezultāti gan reālā, gan simulētā vidē. Nodaļā aprakstīta arī dažādu uzbrukumu veidu un to ietekmes uz tīklu salīdzinošā analīze, īpašu uzmanību pievēršot Nakagami sadalījuma izmantošanai tīkla signāla degradācijas modelēšanai un tīkla uzticamības novērtēšanai pārslodzes apstākļos.

Piektajā nodaļā aprakstītas izstrādātās metodes tīkla aizsardzībai pret *DoS*, traucēšanas un pakešu injekcijas uzbrukumiem. Aprakstītas pieejas ļaunprātīgu pakešu atklāšanai, tostarp *MAC* adresēs balstīta filtrēšana, dinamiskā kanālu traucēšana un adaptīvā bloķēšana. Nodaļā izklāstīti arī polinomu tendences algoritmi tīkla atjaunošanas prognozēšanai pēc uzbrukumiem un ierosināti pasākumi tīkla noturības uzlabošanai, kā arī aplūkota ierosināto mehānismu efektivitāte reālos un simulētos apstākļos.

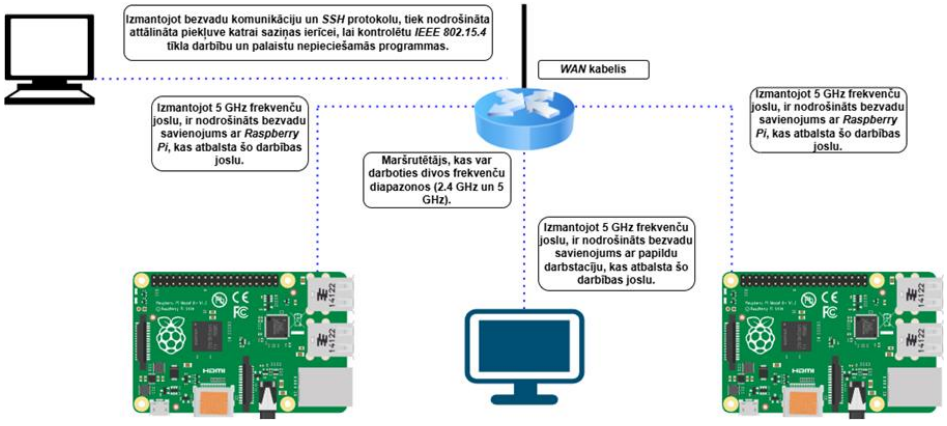
Promocijas darba nobeigumā sniegti galvenie secinājumi, kas izriet no pētījuma rezultātiem, kā arī priekšlikumi turpmākajiem darba virzieniem bezvadu *IoT* kiberdrošības jomā, uzsverot piedāvāto risinājumu praktisko nozīmi un to izmantošanas iespējas *IoT* sistēmās un *Zigbee* tīklos. Noslēgumā pievienots literatūras saraksts, izmantotie avoti un promocijas darba izstrādei noderīgo publikāciju saraksti.

PROMOCIJAS DARBA SATURS

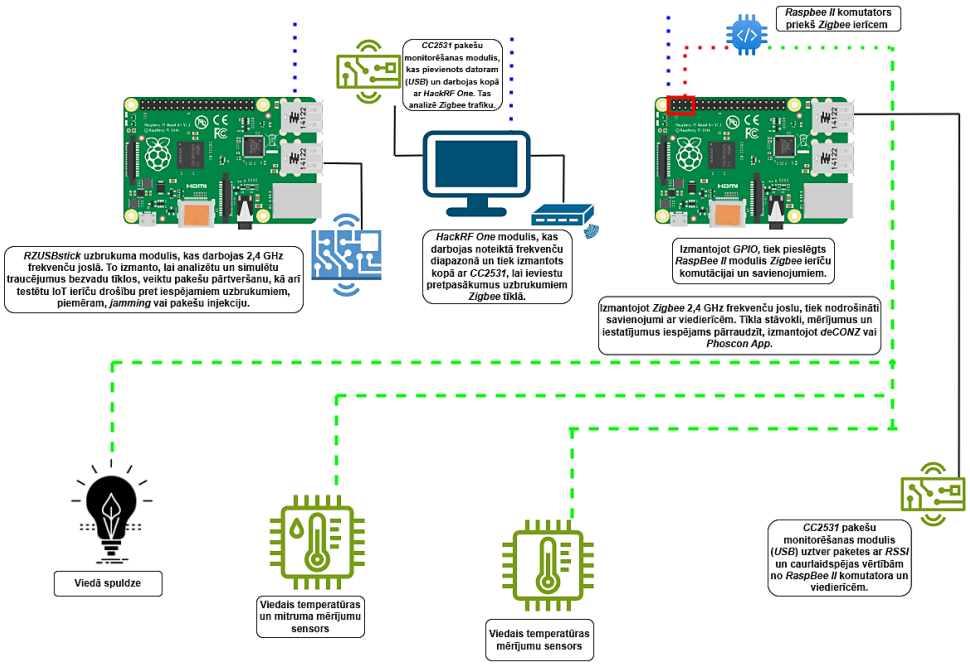
Pirmā nodaļa

Promocijas darba pirmajā nodaļā sniegts *IEEE 802.11* un *802.15.4* hibrīdtīkla novērtējums, apskatot galvenos mehānismus un protokolus.

Pirmās nodaļas sākumā aprakstīta *IEEE 802.11* un *802.15.4* hibrīdtīkla izveide. Apvienojot šīs datu pārraides tehnoloģijas, ir izveidota hibrīda darbības shēma, kas vienlaikus atbalsta abus standartus. *IEEE 802.11* standarts tiek izmantots *IEEE 802.11ax* versijā, darbojoties 5 GHz frekvenču joslas diapazonā. Šāda izvēle palīdz samazināt tīkla traucējumu risku (interferenci), kad tas darbojas paralēli ar *IEEE 802.15.4*. *IEEE 802.11* ir pamats tradicionālajām interneta komunikācijām, kā arī attālinātai piekļuvei, piemēram, izmantojot *SSH* protokolu. Savukārt *IEEE 802.15.4* tiek lietots kā veido māju risinājumu bāze, izmantojot *Zigbee* protokolu un darbojoties 2,4 GHz frekvenču joslā. Tieši šajā tīklā veikti dažādu uzbrukumu ieviešanas testi, tīkla uzvedības analīze un aizsardzības mehānismu novērtēšana pret kiberuzbrukumiem.



1.1. att. Eksperimentālās bezvadu *IEEE 802.11* tīkla arhitektūras shēma *IEEE 802.15.4* komunikācijas kontrolei.

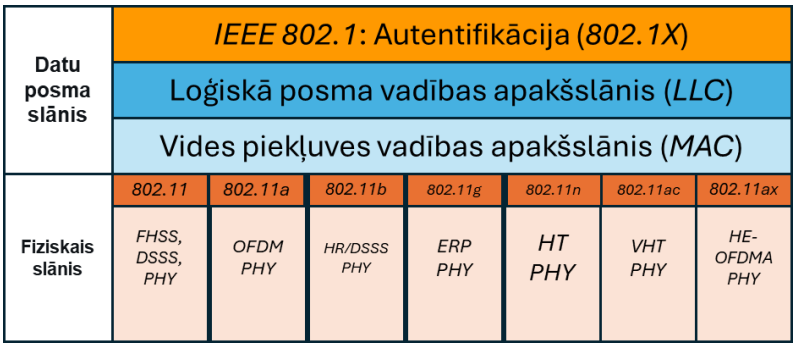


1.2. att. Eksperimentālā *Zigbee* tīkla arhitektūra ar uzbrukumu, aizsardzības mehānismiem un viedierīcēm.

1.1. apakšnodaļā apskatīts *IEEE* 802.11 (*Wi-Fi*) standarts, ko var izmantot tīklu izveidē mājās un birojos. Tas nodrošina datu pārraidi dažādās frekvenču joslas – 2,4 GHz, 5 GHz, 6 GHz un 60 GHz – un ir piemērots gan mobilitātei, gan augstai caurlaidspējai. Kopš standarta ieviešanas 1997. gadā tā attīstībā ir bijuši vairāki varianti (no *802.11a* līdz *802.11ax* jeb *Wi-Fi 6*), piedāvājot uzlabotu veiktspēju un mērogojamību [11], [12].

Galvenie veiktspējas rādītāji ir tīkla caurlaidspēja, latentuma aizture un traucējumu noturība. 2,4 GHz josla nodrošina plašu pārklājumu, bet ir jutīga pret traucējumiem. 5 GHz un 6 GHz joslas piedāvā lielāku ātrumu un mazāku traucējumu risku, taču tai ir mazāks pārklājums [11].

IEEE 802.11 standarts ietver fizisko slāni (*PHY*), datu posma slāni (*MAC* un *LLC*) un drošības mehānismus, kas nodrošina efektīvu un drošu pārraidi bezvadu tīklos.



1.3. att. *IEEE 802.11* standarta darbības steks [13].

Fiziskais slānis nodrošina datu pārraidi, izmantojot radioviļņus 2,4 GHz, 5 GHz un 6 GHz joslās. Tiek izmantotas dažādas modulācijas metodes – agrākās versijās *DSSS* un *FHSS*, jaunākajos standartos – *OFDM*, *QAM*, *MIMO* un *OFDMA*, kas ievērojami uzlabo caurlaidspēju un traucējumu noturību [14]–[16].

***MAC* apakšslānis** pārvalda piekļuvi koplietojamai pārraides videi, izmantojot *CSMA/CA* algoritmu. Tas kontrolē pakešu plūsmu, nodrošina sadursmju novēršanu, pakalpojuma kvalitāti (angļu val. *Quality of Service – QoS*) un uzticamu datu piegādi [17].

***LLC* apakšslānis** nodrošina loģiskās saites vadību starp datu posmu un tīkla slāni. Tas pārvalda datu plūsmas virzienu, adresāciju, kļūdu labošanas mehānismiem (*CRC*) un nodrošina saskarni starp *MAC* un augstākiem tīkla protokoliem *OSI* modelī [17].

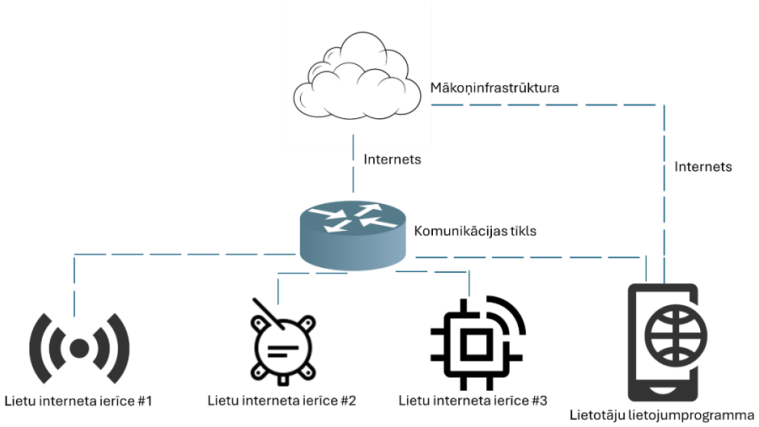
Drošības mehānismi ietver vairākus aizsardzības līmeņus – no autentifikācijas līdz datu šifrēšanai. *IEEE 802.11* standartā agrāk izmantoja *WEP*, kas mūsdienās tiek uzskatīts par nedrošu.

Mūsdienu standarti izmanto *WPA2* un *WPA3* protokolus:

- ***WPA2*** izmanto uzlabotu datu šifrēšanas algoritmu (angļu val. *Advanced Encryption Standard – AES*) ar 128 bitu atslēgu un četru pakāpju apstiprinājuma mehānismus (angļu val. *4-Way Handshake*);
- ***WPA3*** ievieš uzlabotu autentifikāciju ar *SAE* (angļu val. *Simultaneous Authentication of Equals – SAE*), kas aizsargā pret vājo paroļu uzbrukumiem (angļu val. *brute force*) un piedāvā arī uzlabotu datu aizsardzību publiskajos tīklos (angļu val. *Forward Secrecy*) [18]–[20].

Abos protokolos ir iekļauti arī mehānismi pret atkārtotu pakešu sūtīšanās uzbrukumu (angļu val. *replay attacks*) un *DoS* uzbrukumiem. Turklāt autentifikāciju var papildināt ar *802.1X* protokolu un *RADIUS* serveriem, kas nodrošina centralizētu lietotāju pārvaldību, kā arī daudzfaktoru autentifikācijas iespējas (angļu val. *Multi-Factor Authentification*).

1.2. apakšnodaļā apskatīta bezvadu *IoT* tīklu arhitektūra un lietojums. *IoT* ierīcēm ir saziņas shēma, kas izskatās diezgan vienkārša. Mākoņinfrastruktūra ir centralizēta infrastruktūra, kurā tiek glabāti, analizēti un apstrādāti no *IoT* ierīcēm savāktie dati. Sakaru tīkls jeb komunikācijas tīkls ir tīkls, kas nodrošina saziņu starp *IoT* ierīcēm un mākoņinfrastruktūru, izmantojot internetu. Tas var būt vadu vai bezvadu tīkls. Savukārt saziņas funkciju starp ierīcēm un internetu pilda lietu interneta centrmezgls jeb komutators. Tālāk ir pašas ierīces, kas ir fiziskas ierīces, piemēram, viedie sensori, sensori u. c., kas ir savienotas ar sakaru tīklu un vāc datus no vides. Vide var būt dažāda, tas var būt gan dzīvoklis, gan dzīvojamā ēka, gan iela, gan pilsēta, gan valsts. Lietotāja lietojumprogrammas ir programmatūra vai saskarne, kas ļauj lietotājiem mijiedarboties ar *IoT* ierīcēm, skatīt, vizualizēt un pārvaldīt datus. Katra *IoT* ierīce vāc datus no savas darbības vides un, izmantojot ārējo tīklu, pārsūta tos uz mākoni tālākai apstrādei un glabāšanai. Lietotāji paši var mijiedarboties ar ierīcēm un datiem, izmantojot lietotnes [2], [21], [23].



1.4. att. Lietu interneta (*IoT*) tīkla arhitektūra.

1.3. apakšnodaļā apkopoti būtiskākie *IoT* protokoli un izmantošanas jomas. Protokoli iedalīti pēc funkcijas – datu pārraides un tīkla organizācijas. Ziņojumu pārsūtīšanas protokoli, piemēram, *MQTT*, *CoAP* un *AMQP*, kalpo datu nodošanai starp *IoT* ierīcēm un serveriem. *MQTT* ir īpaši piemērots zema joslas platuma tīkliem, *CoAP* kā vienkārša *HTTP* alternatīva ierobežotu resursu vidēm, savukārt *AMQP* piedāvā plašāku funkcionalitāti sarežģītāku ziņojumu apmaiņai. Bezvadu tīkla protokoli, kā *Zigbee*, *LoRaWAN*, nosaka datu pārraides tehnoloģiju un topoloģiju. Protokolu izvēle atkarīga no lietojuma specifikas – datu apjoma, nepieciešamā pārklājuma, latentuma un energoefektivitātes [2], [22], [25].

1.4. apakšnodaļā aplūkoti *IEEE 802.15.4* standarta fiziskā (*PHY*) un datu posma (*MAC*) slāņu darbības principi, uzsverot to nozīmi *IoT* tīklu izveidē. *IEEE 802.15.4* ir pamatstandarts daudziem zemas jaudas bezvadu protokoliem, tostarp *Zigbee* un *Thread*. Fiziskais slānis izmanto *DSSS* modulāciju un darbojas galvenokārt 2,4 GHz *ISM* joslā, kā arī 868/915 MHz frekvenču joslās atkarībā no reģiona. Tas nodrošina pietiekamu pārklājumu un labu noturību pret traucējumiem [24], [26]–[28].

Datu posma slānis nodrošina datu kadru piekļuvi, izmantojot *CSMA/CA* mehānismu, *Beacon* signālus sinhronizācijai un atbalstu dažādām tīkla topoloģijām, tostarp hierarhiskām un *mesh* struktūrām [27].

Drošība ir būtisks aspekts *IEEE 802.15.4* tīklos. Standarts ietver *AES-128* šifrēšanu, lai nodrošinātu datu konfidencialitāti, integritāti un autentifikāciju. Šie drošības mehānismi aizsargā tīklu no nesankcionētas piekļuves un pārtveršanas uzbrukumiem. Papildus tam dažas implementācijas izmanto reputācijas sistēmas un tīkla monitoringa risinājumus, lai uzlabotu drošības līmeni [29].

Tiek uzsvērts, ka *IEEE* 802.15.4 ir īpaši piemērots ierīcēm ar ierobežotiem resursiem, jo tas nodrošina zemu enerģijas patēriņu, zemu datu pārraides ātrumu un augstu uzticamību, kas ir būtiski viedajiem sensoriem, monitoringa iekārtām un citām *IoT* ierīcēm.

1.5. apakšnodaļā teorētiski analizētas *IEEE 802.11* un *IEEE 802.15.4* tīklu veiktspējas atšķirības, balstoties zinātniskajā literatūrā un standartu tehniskajos rādītājos. *IEEE 802.11* (*Wi-Fi*) tīkli nodrošina augstu datu caurlaidspēju (līdz 9,6 Gbit/s), un tie ir piemēroti lietojumiem ar lielu datu plūsmu, piemēram, video straumēšanai. Tomēr šiem tīkliem raksturīgs augstāks enerģijas patēriņš, lielāka traucējumu iespējamība un zemāka piemērotība energoierobežotām ierīcēm. *RSSI* līmenis parasti ir no –30 dBm līdz –50 dBm, bet *LQI* parametrs šajā standartā netiek izmantots [30], [33].

Savukārt *IEEE* 802.15.4 tīkli, kas paredzēti sensoriem un zemas caurlaidspējas ierīcēm, piedāvā pārraides ātrumu līdz 250 kbit/s, zemāku enerģijas patēriņu un labāku noturību pret traucējumiem. *RSSI* līmenis ir līdzīgs – ap –30 dBm līdz –50 dBm, un *LQI* rādītāji robežojas no 0 līdz 255, kur lielākas vērtības liecina par augstāku signāla kvalitāti [31].

Salīdzinājums parāda, ka *IEEE 802.11* standarts ir piemērots datu intensīvām un ātras reakcijas lietotnēm, savukārt *IEEE 802.15.4* labāk piemērots ilgtspējīgām, energoefektīvām sistēmām, piemēram, vides monitoringa vai automatizācijas risinājumiem. Protokolu izvēle atkarīga no konkrētā lietojuma prasībām pēc ātruma, enerģijas patēriņa un pārklājuma apjoma.

1.6. apakšnodaļā aprakstīts eksperimentālais hibrīdtīkls, kurā apvienotas *IEEE 802.11* un *IEEE 802.15.4* standarta ierīces, lai novērtētu to sadarbību un tīkla veiktspēju reālos lietošanas apstākļos. Detalizēti aplūkotas visas izmantotās komponentes un lietojumi šajā tīklā.

Tīkla struktūrā tika izmantotas divas *Raspberry Pi* ierīces. Viena no tām darbojas kā *Zigbee* komutators ar *RaspBee II* moduli uz *GPIO* pieslēgvietām un papildu *CC2531* adapteri ar *Killerbee* programmaparatūru datu monitorēšanai. Tāda konfigurācija ļauj analizēt *RSSI*, caurlaidspēju un datu paketes darbības laikā, izmantojot autora izstrādātās *Python* palaišanas programmas [34], [35].

Otra *Raspberry Pi* ierīce kalpo kā uzbrucējs, izmantojot *RZUSBStick* ar uzprogrammētu *KillerBee* bibliotēku, kas spēj veikt *DoS* uzbrukumus, pakešu injekciju un signāla iestrēgšanu. Tika izmantoti arī papildu aizsardzības mehānismi – stacija ar *Kali Linux*, *HackRF One* – un vēl viens *CC2531* modulis uzbrukumu novēršanai un neitralizācijai [34], [36].

Eksperimentos tika analizēta datu plūsma, sinhronizācijas problēmas, traucējumu ietekme un savienojamības uzticamība starp protokoliem. Tika konstatēts, ka *IEEE 802.11* nodrošina augstu pārraides ātrumu, savukārt *IEEE 802.15.4* – stabilitāti un energoefektivitāti, padarot šādu hibrīdtīklu piemērotu elastīgām un drošām *IoT* sistēmām.

Otrā nodaļa

2.1. apakšnodaļā sniegts vispārīgs ieskats kiberdrošības jēdziena un vēstures attīstībā un aprakstīta kiberdrošības aktualitāte mūsdienu informācijas tehnoloģiju vidē. Apskatīti ne tikai kiberdrošības inženieru pienākumi, bet dots arī kiberdrošības daudzveidības pārskats (angļu val. *Cyber Resilience Review, CRR*), kas ietver gan preventīvus, gan reaģējošus pasākumus kiberdraudu gadījumā. Kā papildinājums – tiek izcelts cilvēciskais faktors kā nozīmīgs aspekts drošības uzturēšanā, kā arī norādīta dažādu drošības dalībnieku sadarbības nozīme [37], [38].

2.2. apakšnodaļā aplūkoti dažādi kiberdrošības pārkāpumu veidi un to piemēri, kā arī analizēta iespējamā ietekme uz *IT* infrastruktūru un pakalpojumu pieejamību. Skarti arī jautājumi par draudu avotiem – gan ārējiem, gan iekšējiem, mērķiem un tipiskām ievainojamībām, kā arī aprakstīts, kā mainās uzbrukumu motivācija laikā gaitā.

Kā piemēri aprakstīti vairāki ievērojami ļaunprogrammatūras uzbrukumi.

- **Šifrētāji jeb izspiedējprogrammatūra** – šāda veida hakeru būtība ir šifrēt datus vai bloķēt piekļuvi tiem. Lietotājs zaudē iespēju atvērt dokumentus vai palaist nepieciešamās programmas. Šāda veida ļaunprogrammatūra sniedz norādījumus, ka, lai atšifrētu datus, ir jāmaksā. Tādējādi diezgan daudzu uzņēmumu datorsistēmas ir uzlauztas, izmantojot tādas

programmas kā *WannaCry* vai *Petya*, kad lietotājs, atverot programmu, zaudē pilnu piekļuvi datoram tā lietošanas vai ieslēgšanas posmā.

- **Vīrusi**, kas var inficēt failus, inficēt pašu infrastruktūru un kopēt tās izpildāmo kodu citos failos un programmās.
- **Trojas zirgi** (angļu val. *Trojan horse*) – kiberuzbrukuma metode, kur ļaunprātīgās izpildes kods tiek maskēts kā likumīga programmatūra vai fails.
- **Botnets** (angļu val. *botnet*) ir ļaunprātīgi kontrolēts tīkls, kas ietver ļaunprogrammatūru inficētas ierīces (botus), tostarp datorus, maršrutētājus, *IP* kameras, *IoT* ierīces un citus tīkla mezglus [39].

2.3. un **2.4. apakšnodaļā** autors koncentrējas uz lietu interneta tīklu drošības izaicinājumiem, īpaši pievēršot uzmanību *IEEE 802.15.4* standarta ievainojamībām. Izklāstīti *IEEE 802.15.4* standarta drošības aspekti, īpaši tādi kā datu šifrēšana, izmantojot *TLS/SSL* un *AES* vai *RSA* algoritmu. Autentifikācija (*OAuth*, *OpenID*) un divfaktoru autentifikācija (angļu val. *Two-Factor Authentication*), piekļuves kontrole (angļu val. *Role-Based Access Control – RBAC*) un atjauninājumu politikas. Detalizēti aprakstīti riski – bezvadu savienojumu ievainojamības, piemēram, "cilvēks-pa-vidu" (angļu val. *Man-in-the-Middle*), traucēšanas uzbrukumi (angļu val. *Jamming Attack*) u. c., kā arī noklusējuma akreditācijas dati un nepietiekamas ierīču aizsardzības faktori. Sniegta sistemātiska pieeja tīkla drošības nodrošināšanai, izmantojot ierīces fiziskās aizsardzības un *IDS/IPS* uzbrukumu atklāšanas sistēmas [9], [10], [39]–[42].

2.5. apakšnodaļā aprakstīta praktiska pieeja drošības analīzei un uzbrukumu testēšanai *IEEE 802.15.4* standartā, *Zigbee* protokolā. Tiek uzsvērta praktiskā nozīme ievainojamību identificēšanā un tas, kā konkrētas aparatūras ierīces un atvērtā koda programmatūra ļauj izveidot dažādus uzbrukumu scenārijus. Aprakstīti izmantotie rīki – *CC2531* modulis, *Killerbee* bibliotēka, arī *Python* koda elements *RSSI* datu ieguvei [34], [35].

```
start_time = time.time()
while time.time() - start_time < duration:
    try:
        packet = kb.pnext()
        if packet:
            rssi = packet.get("rssi", None)
            if rssi is None:
                logging.warning("Nav RSSI vērtības, izlaist.")
                continue
```

2.1. att. *RSSI* vērtības apstrādes paketes piemērs no *Killerbee*.

Promocijas darba izstrādes gaitā pētīti dažāda veida uzbrukumi.

- **Pakešu injekcijas** – promocijas darba izstrādes gaitā izveidotas papildu uzbrukumu paketes, kas inicializētas kā parastās un likumīgās darbības paketes ar zemākām *RSSI* vērtībām, kas raksturīgas vājākiem vai attālāk esošiem avotiem, lai tās vizuāli un funkcionāli atbilstu tīkla darbības normām, vienlaikus pārbaudot tīkla spēju atpazīt un apstrādāt šādu trafiku. Šāda metode ļauj identificēt, vai tīkls spēj efektīvi noteikt novirzes, piemēram, anomālijas *RSSI* vērtībās, kas spēj piesārņot trafiku vai padarīt to par darbnespējīgu.
- ***DoS* uzbrukums** – promocijas darba izstrādes gaitā ģenerētas papildu uzbrukuma paketes, kuru mērķis ir radīt tīkla pārslodzi, izmantojot augstu pakešu nosūtīšanas biežumu, kas pārsniedz *IEEE 802.15.4* tīkla normālās darbības kapacitāti. Šīs paketes inicializētas ar specifiskām paketes galvenēm (angļu val. *header*) un noteiktiem parametriem, lai vizuāli un funkcionāli atbilstu tīkla likumīgajam darbības raksturam, vienlaikus pārbaudot tīkla spēju atpazīt un apstrādāt šādu uzbrukuma trafiku.
- **Sakaru signāla traucēšana (angļu val. *Jamming*) uzbrukums –** promocijas darba izstrādes gaitā veikti uzbrukumi, ieviešot tīklā apzinātus signāla traucējumus, kas bloķē *IEEE 802.15.4* savstarpējo komunikāciju. Traucējumi simulēti, analizējot tīkla reakciju uz ilgstošiem periodiem bez uztvertiem datiem, kā arī signāla stipruma līmeņa (*RSSI*) pēkšņām izmaiņām, kas liecina par iespējamu uzbrukumu.

Papildus aprakstīta *HackRF One* un *CC2531* izmantošana uzbrukuma noteikšanai un aizsardzības scenāriju realizācijai ar adaptīvu traucēšanas mehānismu. Sniegts detalizēts ieskats, kā tiek mērīts signāla stiprums, un analizēta datu plūsma dažādos scenārijos.

Trešā nodaļa

3.1. apakšnodaļā apskatīti bezvadu sakaru ierīču tehniskie parametri, savukārt **3.1.1. apakšnodaļā** teorētiski un praktiski izvērtēta *Zigbee* tīkla caurlaidspēja, balstoties Šenona teorēmā un empīriski pielāgotā caurlaidspējas modelī. Tika ņemti vērā tādi ietekmējošie faktori kā ierobežots kanāla joslas platums (2 MHz), traucējumu klātbūtne (signāla interference), protokola pieskaitāmās izmaksas (angļu val. *overhead*) un *CSMA/CA* mehānisma darbība [35], [43]–[46].

Lai arī *Zigbee* standarta teorētiskā maksimālā pārraides caurlaidspēja var sasniegt 250 kbit/s, reālos apstākļos, ņemot vērā trokšņa līmeni (angļu val. *Noise Floor – SNR*), paketes pārraides veiksmes varbūtības koeficientu, kanāla izmantošanas koeficientu un citus parametrus, faktiski

pieejamā caurlaidspēja pārsniedz 120 kbit/s. Tika definētas un izmantotas 3.1.–3.4. formulas, kurās integrēti faktori, piemēram, paketes pārraides veiksmes varbūtības koeficients (P_{success}) un kanāla izmantošanas koeficients (*Duty_Cycle*). *SNR* tika aprēķināts kā starpība starp *RSSI* un trokšņa līmeni (pieņemts –95 dBm), savukārt pārraides efektivitātes kritēriji balstīti praktiski izmērāmos parametros [46]–[56].

$$C = C_{\text{THEORETICAL}} \times (1 - OVERHEAD) \times P_{\text{success}} \times Duty\ Cycle\,, \tag{3.1.}$$

kur C – maksimāla reāla caurlaidspēja (kbit/s); $C_{\text{THEORETICAL}}$ – teorētiskā *Zigbee* tīkla caurlaidspēja (250 kbit/s); *OVERHEAD* – pieskaitāmās izmaksas (0,4 = 40 %); P_{success} – paketes pārraides veiksmes varbūtības koeficients; *Duty_Cycle* – kanāla izmantošanas koeficients [46], [56].

$$SNR = RSSI - NOISE\_FLOOR, \tag{3.2.}$$

kur *SNR* – signāla/trokšņa attiecība (dB); *RSSI* – signāla stipruma identifikators (dBm); *NOISE_FLOOR* – trokšņa līmenis (dBm).

$$P_{\text{success}} = \left(0{,}1, \left(1{,}0, \frac{SNR}{MAX\_SNR}\right)\right), \tag{3.3.}$$

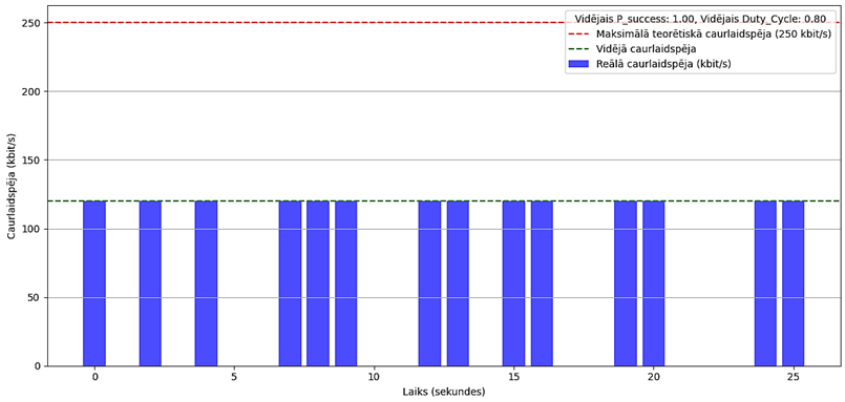
kur P_{success} – paketes pārraides veiksmes varbūtības koeficients; *SNR* – signāla/trokšņa attiecība; *MAX_SNR* – maksimālā signāla/trokšņa attiecība.

$$Duty\_Cycle = \left(0{,}1, \left(0{,}8, \frac{SNR}{MAX\_SNR}\right)\right), \tag{3.4.}$$

kur *Duty_Cycle* – kanāla izmantošanas koeficients; *SNR* – signāla/trokšņa attiecība; *MAX_SNR* – maksimālā signāla/trokšņa attiecība.

MAX_SNR vērtību promocijas darba autors izvēlējās 40 dB, jo tā balstīta praktiskos mērījumos un ņem vērā bezvadu *Zigbee* tīklu ierobežojumus. Šis parametrs ietekmē pakešu pārraides veiksmes varbūtības koeficienta un kanāla izmantošanas koeficientu aprēķinus. Reālā praksē *Zigbee* strādā 2,4 GHz frekvences joslā, kur ir daudz traucējumu, ko rada *Wi-Fi* un *Bluetooth* sakari. Tomēr 40 dB ir labs empīriskais skaitlis nākotnes mērījumiem [47]–[51].

Tika konstatēts, ka veiksmīgas pārraides varbūtības koeficients pie zema *SNR* ir tikai 10 %, bet pie sasniegta maksimālā līmeņa – 100 %. Savukārt kanāla izmantošanas koeficients pat pie ļoti augsta *SNR* nepārsniedz 80 %, jo *CSMA/CA* mehānisms un tīkla slodze ierobežo pārraides laiku. Šie secinājumi apstiprina nepieciešamību optimizēt tīkla darbību specifiskos lietojuma apstākļos, kur svarīgākais ir energoefektivitāte, un vienlaikus piedāvā pieeju precīzākai sistēmu projektēšanai, ņemot vērā konkrētās *IoT* infrastruktūras vajadzības.



3.1. att. *Zigbee* tīkla reālās caurlaidspējas analīzes grafiks.

3.1.2. apakšnodaļā izvērtēta bezvadu *Zigbee* tīkla signāla stipruma (*RSSI*) izplatība, izmantojot Nakagami sadalījumu, kas labāk raksturo sarežģītos daudzceļu izplatības apstākļus nekā tradicionālie Reilija un Raisa modeļi [52], [53].

Lai modelētu bezvadu tīklu signāla izplatīšanos un novērtētu tā ietekmi uz tīkla veiktspēju, promocijas darbā tika izmantots Nakagami sadalījums. Lai modelētu *RSSI* vērtības, tika izmantota funkcija.

$$F \sim Gamma\left(m, \frac{m}{\omega}\right), \tag{3.5.}$$

kur m – formas (angļu val. *shape*) parametrs; ω – vidējais enerģijas līmenis.

3.5. izteiksme tiek izmantota, lai ģenerētu datus no Nakagami sadalījuma, pielāgotu *RSSI* vērtības un simulētu signāla izmaiņas reālās bezvadu tīkla vidēs. Nejauši ģenerētie dati tiek aprakstīti ar varbūtību blīvuma funkciju (*PDF*), 3.6. izteiksme norāda, kā vērtības tiek sadalītas [52]–[54].

$$f(x) = \frac{2m^m}{\Gamma(m)\omega} m_{x^{2m-1}e^{-\frac{m}{\omega}x^2}, \quad x>0}, \tag{3.6.}$$

kur m – formas (angļu val. *shape*) parametrs; ω = E[R^2] – vidējā signāla jauda; Γ(m) – gamma funkcija.

Izmantojot 3.5. un 3.6. izteiksmi, tika veikti signāla modelēšanas aprēķini, izmantojot parametrus m = 0,8 un ω = 0,3, kas balstīti eksperimentāli iegūtās *RSSI* vērtībās (–85 dBm), liecinot par vāju, nestabilu savienojumu bez tiešās redzamības līnijas (angļu val. *Non-Line-of-Sight* –

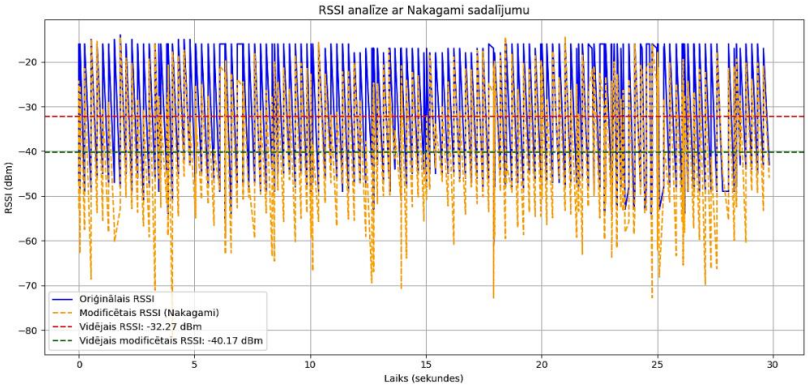
NLOS). Eksperimentālo datu analīze rāda, ka *RSSI* vērtības *Zigbee* tīklā ievērojami mainās atkarībā no vides šķēršļiem un daudzceļu atstarošanas efektiem. Tika aprēķinātas modificētās *RSSI* vērtības un caurlaidspēja, ņemot vērā Nakagami sadalījuma ietekmi. Rezultāti liecina, ka šī metode ļauj precīzāk modelēt reālas vides ietekmi uz tīkla darbību, kas ir būtiski *IoT* sistēmu projektēšanā [52]–[54].

Tas ir īpaši noderīgi, lai novērtētu *Zigbee* tīkla signāla stiprumu un tīkla caurlaidspēju pēc Nakagami sadalījumam. 3.7. izteiksme nosaka modificēto *RSSI* signāla stiprumu pēc reāli nomērītā *RSSI*, izmantojot *Killerbee* programmatūru, un aprēķina modificēto caurlaidspēju pēc iegūtām modificētām *RSSI* vērtībām, izmantojot 3.1.–3.4. izteiksmi [47]–[56].

$$RSSImod = RSSIorig + 10 \times \log10(F), \tag{3.7.}$$

kur $RSSI_{orig}$ – nomērītā *RSSI* vērtība; F – gamma starojums.

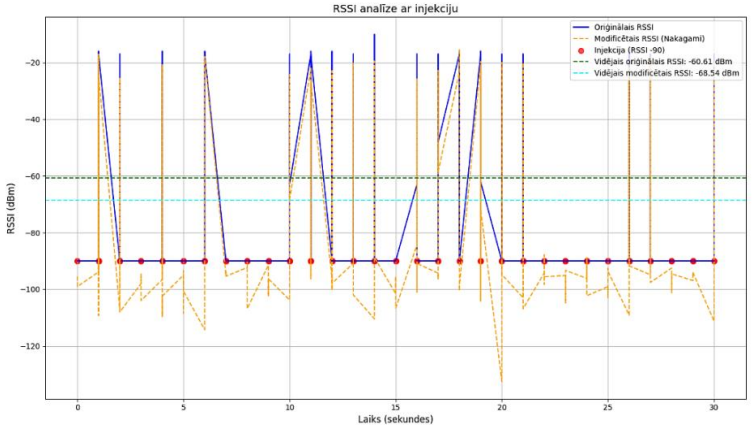
Izmantojot logaritmisko korekciju no 3.7. izteiksmes, tai pievieno nejaušas signāla jaudas svārstības, ko rada daudzceļu izplatīšanas efekti (piemēram, atstarojumi, difrakcijas un izkliedēšana). Iegūtajā *RSSI* vērtībā tiek ņemtas vērā nejaušās svārstības, tādējādi tā ir tuvāka reālajiem apstākļiem sarežģītā vidē (piemēram, ēkā vai pilsētvidē).



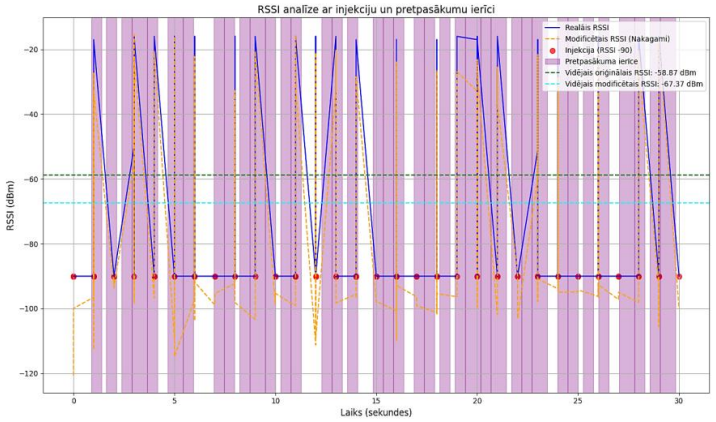
3.2. att. Signāla stipruma identifikators Nakagami sadalījuma ietekmē.

3.2. apakšnodaļā analizēta *Zigbee* tīkla veiktspēja, izmantojot *Python* palaišanas programmas un *Killerbee* rīkus. Papildus apskatīta modificēta signāla stipruma vērtība, kas tiek iegūta, piemērojot Nakagami sadalījumu, kas precīzāk atspoguļo reālos signāla izplatīšanās apstākļus. Veiktas gan reālās, gan modificētās caurlaidspējas un signāla stipruma analīzes, ņemot vērā uzbrukuma un pretpasākumu ieviešanas scenārijus [55].

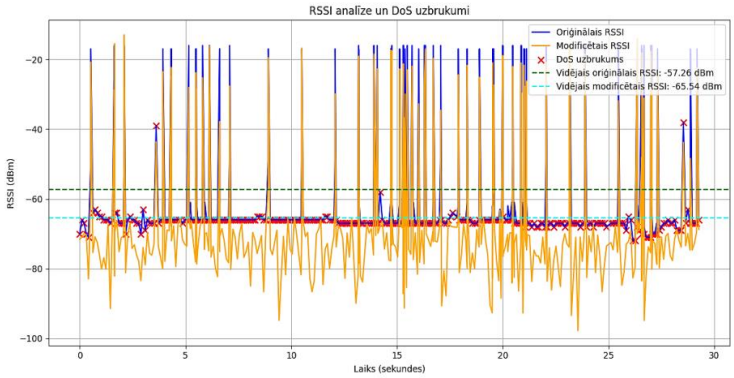
Eksperimenti ietver trīs veidu uzbrukumus – pakešu injekciju, *DoS* uzbrukums un signāla iestrēgšanu. Tika izmantoti dažādi injekcijas biežumi (0,25 sekundes un 0,5 sekundes), un analizēta gan *RSSI* (reālā un modificētā) vērtību dinamika, gan reālā un modificētā tīkla caurlaidspēja.



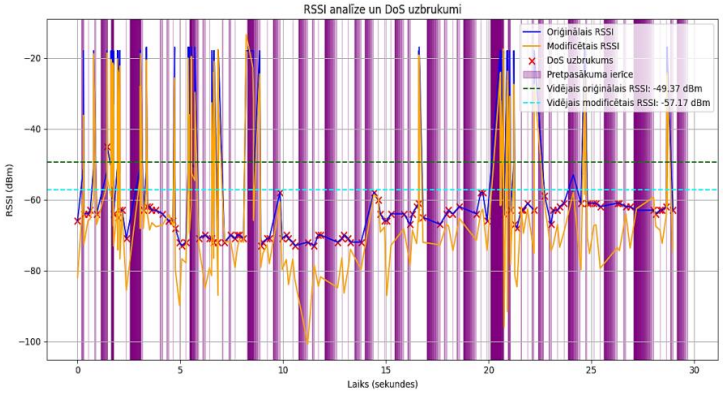
3.3. att. Signāla stipruma identifikatora analīze pakešu injekcijas uzbrukuma laikā ar sūtīšanas biežumu 0,25 sekundes.



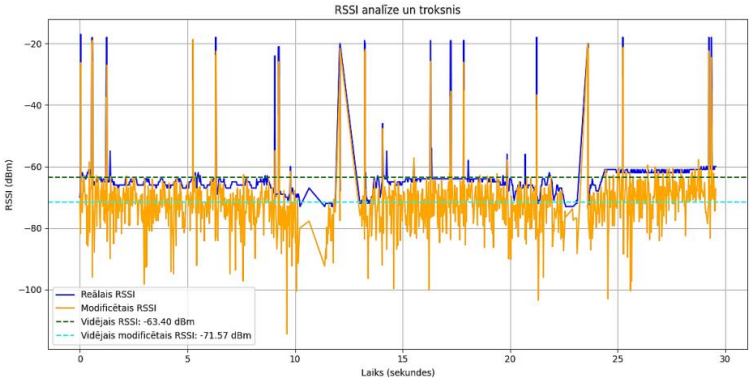
3.4. att. Signāla stipruma identifikatora analīze pakešu injekcijas uzbrukuma laikā ar pretpasākumu ierīci ar sūtīšanas biežumu 0,25 sekundes.



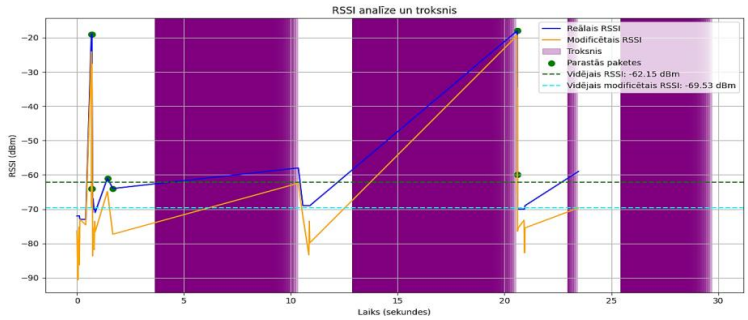
3.5. att. Signāla stipruma identifikatora analīze *DoS* uzbrukuma laikā.



3.6. att. Signāla stipruma identifikatora analīze *DoS* uzbrukuma un pretpasākuma laikā.



3.7. att. Signāla stipruma identifikatora analīze signāla traucēšanas laikā.



3.8. att. Signāla stipruma identifikatora analīze signāla traucēšanas un pretpasākuma laikā.

Eksperimentu rezultāti liecina, ka pakešu injekcijas uzbrukumi ar *RSSI* vājinājumu (–90 dBm) būtiski ietekmē *Zigbee RSSI* un tīkla caurlaidspēju, taču tie nav pietiekami spēcīgi, lai pilnībā paralizētu tīklu. Ilgāki mērījumi (60–120 sekundes) atklāj būtiskas svārstības gan *RSSI*, gan caurlaidspējas vērtībās, īpaši pie intensīvām pakešu injekcijām. *DoS* uzbrukumi, kas balstīti augsta biežuma trafika ģenerēšanā (ik pēc 0,1 sekundes), ievērojami samazina tīkla caurlaidspēju, tomēr tīkla spēja pielāgoties ir redzama – *RSSI* saglabājas salīdzinoši stabils, un ierīces joprojām spēj savstarpēji sazināties, bet ar nelielu aizturi. Savukārt sakaru signāla traucēšanas uzbrukums ar 0,02 sekundes biežumu izraisa straujas *RSSI* vērtību svārstības un samazina tīkla caurlaidspēju (gan reālo, gan modificēto), uzskatāmi demonstrējot kanāla pārslogotību un nestabilitāti.

Lai cīnītos pret šiem uzbrukumiem, tika lietoti *CC2531* monitorēšanas un *HackRF One* pretpasākuma moduļi, kas spēj identificēt specifiskas ļaunprātīgas paketes un bloķēt to tālāku izplatīšanos. Novērots, ka injekcijas pakešu bloķēšana nodrošina līdz pat 99 % efektivitāti, saglabājot stabilu caurlaidspēju un būtiski ierobežojot *RSSI* svārstības. *DoS* uzbrukumu gadījumā selektīva traucējumu ģenerēšana ļauj uzturēt caurlaidspēju aptuveni 85 % apmērā no normālās, kas ir ievērojams rezultāts tīkla noturības ziņā. Savukārt signāla traucēšanas laikā *Zigbee* tīkla pašadaptācijas mehānismi, tostarp *RSSI* analīze, dinamiska signāla pielāgošana un datu filtrēšana, palīdz samazināt traucējumus un uzlabot signāla komunikācijas kvalitāti, īpaši ilgstošos mērījumos.

Analizētie grafiki, kas parāda gan reālās, gan modificētās *RSSI* un caurlaidspējas vērtības, vizuāli ilustrē tīkla uzvedību dažādu uzbrukumu un pretpasākumu laikā. Tie uzskatāmi demonstrē tīkla adaptīvo spēju nozīmi, kas ļauj saglabāt augstu efektivitāti arī sarežģītos darbības apstākļos. Turklāt modificētās caurlaidspējas aprēķini, kas balstīti empīriskos modeļos, sniedz iespēju objektīvi izvērtēt traucējumu ietekmi un prognozēt tīkla darbību nākotnē, padarot šo pieeju par noderīgu rīku *IoT* infrastruktūras drošības analīzē [46], [49]–[50], [52], [60].

Ceturtā nodaļa

4.1. apakšnodaļā aprakstīta ieviestā papildu darbība – simulācija, kas balstās ideālā *Zigbee* tīkla modelī, lai konstatētu un salīdzinātu caurlaidspējas un *RSSI* mērījumus ar iepriekšējā nodaļā aprakstītajiem promocijas darba izstrādes gaitā iegūtajiem mērījumiem reālajā vidē pēc dažādiem uzbrukumiem. Galvenais simulācijas mērķis ir izpētīt, kā tīkls turpina darboties optimālos apstākļos, kad tiek novērsti ārējie uzbrukumi, piemēram, pakešu injekcijas, *DoS* uzbrukums un arī sakaru signāla traucēšana, kā arī analizētas iegūto rezultātu atšķirības, salīdzinot ar reālo vidi [56], [57].

Papildus tam **4.1. apakšnodaļā** ieviests jauns rādītājs – atjaunošanās vērtība, kas palīdzēja kvantitatīvi novērtēt tīkla spēju atgriezties darbības stāvoklī pēc uzbrukuma. Izmantojot matemātiskās izteiksmes *RSSI* un caurlaidspējas līmeņu salīdzināšanai pirms un pēc aizsardzības, veikts detalizēts efektivitātes novērtējums [47], [48], [56].

4.2. apakšnodaļā veikta salīdzinoša analīze starp *Zigbee* tīkla uzvedību reālajā vidē un *Python* balstītā simulācijas vidē, īpašu uzmanību pievēršot uzbrukumu un pretpasākumu efektivitātei. Šāda veida analīze palīdzēja izprast reālās vides traucējumu ietekmi, kā arī precīzāk novērtēt simulācijas rezultātu atbilstību praksē novērotajam.

Simulācijas vide sniedza kontrolētus apstākļus, kuros iespējams reproducēt identiskus parametrus vairākiem testiem, taču tā nevar pilnībā atspoguļot dinamisko un daudzfaktoru raksturu, kas ir raksturīgs *IoT* videi. Reālā tīklā būtiska nozīme ir ierīču fiziskajam izvietojumam, apkārtējai elektromagnētiskajai videi un neparedzētiem traucējumiem. Tāpēc *RSSI* un caurlaidspējas svārstības reālā tīklā bieži vien atšķiras no simulācijas rezultātiem.

1. tabula

Vidējā *RSSI* salīdzinājums reālā tīklā un simulācijā. Dažu uzbrukumu veidi un aizsardzības ietekme

	Reālā tīkla darbība				**Simulācijas tīkla darbība**			
Uzbrukumu veids	**Δ Oriģinālā *RSSI* vērtība [dBm]**	**Δ Modificētā *RSSI* vērtība [dBm]**	**Δ Atjaunotā oriģinālā *RSSI* vērtība [dBm]**	**Δ Atjaunotā modificētā *RSSI* vērtība [dBm]**	**Δ Oriģinālā RSSI vērtība [dBm]**	**Δ Modificētā *RSSI* vērtība [dBm]**	**Δ Atjaunotā oriģinālā *RSSI* vērtība [dBm]**	**Δ Atjaunotā modificētā *RSSI* vērtība [dBm]**
Pakešu injekcija	–56,63	–65,46	–49,93	–58,75	–51,90	–58,77	–42,21	–49,15
DoS uzbrukums	–49,37	–57,17	–44,87	–51,77	–59,30	–67,84	–59,95	–69,70
Sakaru signāla traucēšana	–62,15	–69,53	–57,85	–63,46	–53,88	–59,93	–47,18	–52,94

2. tabula

Vidējās caurlaidspējas salīdzinājums reālā tīklā un simulācijā. Dažu uzbrukumu veidi un aizsardzības ietekme

	Reālā tīkla darbība				Simulācijas tīkla darbība			
Uzbrukumu veids	**Δ Oriģinālā caurlaid-spēja [kbit/s]**	**Δ Modificē-ta caurlaid-spēja [kbit/s]**	**Δ Atjaunotā Oriģinālā caurlaid-spēja [kbit/s]**	**Δ Atjaunotā Modificētā caurlaid-spēja [kbit/s]**	**Δ Oriģinālā caurlaid-spēja [kbit/s]**	**Δ Modificētā caurlaid-spēja [kbit/s]**	**Δ Atjaunotā Oriģinālā caurlaidspēja [kbit/s]**	**Δ Atjaunotā Modificētā caurlaidspēja [kbit/s]**
Pakešu injekcija	73,42	63,55	80,86	70,45	91,25	89,37	114,57	113,31
DoS uzbrukums	96,02	73,38	105,04	85,48	94,40	68,05	94,42	64,76
Sakaru signāla traucēšana	74,51	50,08	82,25	60,16	87,83	83,75	104,33	101,97

Piemēram, reālajā tīklā injekcijas uzbrukumu laikā vidējais atjaunotais bija augstāks nekā simulācijā (1. tab.), sasniedzot –49,93 dBm, salīdzinot ar –42,21 dBm simulācijas laikā. Arī caurlaidspējas rādītāji parādīja, ka reālā vidē tīkls spēj veiksmīgāk pielāgoties slodzei. Signāla traucēšanas uzbrukumu gadījumā caurlaidspējas rādītāji reālajā tīklā pieauga no 74,51 kbit/s līdz 82,25 kbit/s pēc aizsardzības aktivizācijas, demonstrējot reālās vides adaptīvās spējas.

3. tabula

Uzbrukumu veiksmīgu pretpasākumu procentuālā vērtība reālā un simulācijas vidē

	Reālā tīkla darbība	**Simulācijas tīkla darbība**
Injekcijas uzbrukumu veiksmīgu pretpasākumu vērtība [%]	94,83 %	85,14 %
***DoS* uzbrukumu veiksmīgu pretpasākumu vērtība [%]**	47,75 %	93,33 %
Traucēšanas uzbrukumu veiksmīgu pretpasākumu vērtība [%]	60,11 %	78,05 %

No otras puses, *DoS* uzbrukumu gadījumā simulācija uzradīja augstāku pretpasākumu efektivitāti (3. tab.) – 93,33 %, salīdzinot ar tikai 47,75 % reālajā tīklā, kas skaidrojams ar reālā vidē esošajiem latentumu faktoriem un nepilnīgu *DoS* pakešu identificēšanu.

4. tabula

RSSI kļūdu analīze eksperimentālajiem un simulācijas datiem (oriģinālās *RSSI* vērtības)

Uzbrukumu veids	*MAE* orig. *RSSI*, *dBm*	*RMSE* orig. *RSSI*, *dBm*
Pakešu injekcija	33,33	40,01
DoS uzbrukums	19,99	25,74
Sakaru signāla traucēšana	21,87	23,85

5. tabula

RSSI kļūdu analīze eksperimentālajiem un simulācijas datiem (modificētās *RSSI* vērtības)

Uzbrukumu veids	*MAE* mod. *RSSI, dBm*	*RMSE* mod. *RSSI, dBm*
Pakešu injekcija	34,31	40,9
DoS uzbrukums	21,97	28,51
Sakaru signāla traucēšana	23,69	28,10

RSSI kļūdu analīze starp simulāciju un eksperimentu parādīja, ka lielākās atšķirības novērojamas injekcijas uzbrukumu laikā (*MAE* ≈ 33,33 dBm, *RMSE* ≈ 40,01 dBm), savukārt *DoS* uzbrukumiem kļūdas bija mazākas (*MAE* ≈ 19,99 dBm), kas liecina par stabilāku simulācijas precizitāti šajos gadījumos [58], [59].

Kopsavilkumā šī nodaļa pierāda, ka gan reālai, gan simulācijas videi ir savas priekšrocības. Reālais tīkls demonstrē augstu pielāgošanās spēju, īpaši attiecībā uz injekcijām, savukārt simulācijas palīdz identificēt optimālos parametrus un testēt aizsardzības stratēģijas kontrolētā veidā. Apvienojot abas pieejas, iespējams izveidot uzticamākus un drošākus *IoT* risinājumus nākotnē.

Piektā nodaļa

Piektajā nodaļā aprakstīta veiktā padziļinātā analīze par *IoT* tīklu pārvaldības, drošības un veiktspējas optimizācijas aspektiem. Apskatītie temati ietver *IoT* tīklu aktuālās problēmas, risinājumus un inovatīvas pieejas, kas palīdz uzlabot gan tīklu drošību, gan to darbības efektivitāti reālos apstākļos. *IoT* tīklu attīstība ir saistīta ar strauju ierīču skaita pieaugumu un datu apjoma palielināšanos, kas rada jaunas izaicinājumu jomas. Svarīgās no tām ir uzraudzības un atjauninājumu pārvaldība, standartu un likumdošanas nozīme, tīkla plūsmas un caurlaidspējas optimizācija, kā arī mašīnmācīšanās (angļu val. *Machine Learning*) un mākslīgā intelekta (angļu val. *Artificial Intelligence*) izmantošana drošības risinājumu kontekstā.

5.1. apakšnodaļā aplūkota problēmas, kas saistītas ar ierīču heterogenitāti, atšķirīgu protokolu izmantošanu un ierobežotiem resursiem. Svarīga nozīme ir *FOTA* tehnoloģijai, kas ļauj attālināti veikt atjauninājumus, nodrošinot drošu autentifikāciju un datu integritāti.

5.2. apakšnodaļā veikta analīze par standartiem un likumdošanu, savukārt **5.3. apakšnodaļā** analizēta tīkla optimizācija saistībā ar malu skaitļošanu (angļu val. *Edge Computing*), kas ļauj samazināt latentumu un uzlabot datu apstrādes efektivitāti, veicot datu filtrēšanu jau pie ierīces avota, piemēram, *IoT* komutatora.

5.4. apakšnodaļā analizēta mašīnmācīšanās un mākslīgā intelekta nozīme drošības nodrošināšanā. Konkrēti, anomāliju noteikšana, neironu tīklu izmantošana un automatizētās reaģēšanas sistēmas (angļu val. *Security Orchestration, Automation and Response – SOAR*) kalpo kā pamats proaktīvām aizsardzības stratēģijām [60].

5.5. apakšnodaļā analizēta tīkla segmentācija un mikrosegmentācija kā stratēģija, kas ļauj ierobežot uzbrukumu izplatību, kā arī kontrolēt piekļuvi lietojumprogrammu līmenī. Tādas metodes ir īpaši noderīgas *IoT* tīklos ar lielu savienoto ierīču skaitu [61], [62].

5.6. apakšnodaļā aplūkota integrētās veiktspējas un drošības pārvaldības pieejas nepieciešamība. Uzsvērta pakalpojumu kvalitātes (*QoS*) loma prioritizēt datu plūsmu un saglabāt tīkla stabilitāti, it īpaši kritisku datu gadījumā. *QoS* tehnoloģijas ļauj ierobežot nekritisko procesu ietekmi un atbrīvot resursu svarīgākajiem uzdevumiem [63].

5.7. apakšnodaļā padziļināti analizēta *IoT* tīklu uzvedība kiberdraudu klātbūtnē, lietojot matemātiskas modelēšanas pieejas, lai raksturotu *RSSI* un tīkla caurlaidspējas izmaiņas dažādu uzbrukumu laikā. Būtisks uzsvars likts uz nelineāru regresijas un hibrīdmodeļu izmantošanu, kas ļauj precīzi prognozēt un interpretēt tīkla dinamiku. Eksperimentālie rezultāti parāda, ka tradicionālie regresijas modeļi bieži vien nespēj uztvert haotiskās svārstības uzbrukumu laikā [64].

Polinomu regresija tika izmantota, lai aprakstītu signāla stipruma un caurlaidspējas vispārējās izmaiņas, pieņemot, ka šīs izmaiņas var izteikt kā n-tās pakāpes polinomus:

$$y(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n, \qquad (5.1)$$

kur a_n, a_{n-1},…,a_0 – polinoma koeficienti, kas nosaka funkcijas formu, izmantojot vismazāko kvadrātu metodi *OLS* (angļu val. *Ordinary Least Squares*); x – normalizētais laiks ($x \in [0,1]$); $y(x)$ – prognozētā vērtība (*RSSI* vai caurlaidspēja) [64], [65].

Koeficienti a_i tiek atrasti, izmantojot vismazāko kvadrātu metodi *OLS*, un tās mērķis ir minimizēt kļūdu funkciju E, kas aprēķina atšķirību starp faktiskajiem datiem y_i un polinomu $y(x_i)$

$$E = \sum_{i=1}^{N} \big(y_i - y(x_i)\big)^2, \qquad (5.2)$$

kur N – datu punktu skaits.

Lai atrastu koeficientus, tiek izmantota matricu forma:

$$Y = XA + \epsilon, \tag{5.3}$$

kur Y – vērtību vektors (mērījumi); X – dizaina matrica (katra x pakāpes vērtības); A – nezināmo koeficientu vektors; ϵ – trokšņa un mērījumu kļūdas.

Koeficienti tiek atrasti, izmantojot normālo vienādojumu:

$$A = (X^T X)^{-1} X^T Y. \tag{5.4}$$

Tas nozīme, ka katrs a_i tiek aprēķināts, minimizējot kļūdu starp faktiskajiem un prognozētajiem datiem.

Hibrīdmodelis tiek veidots kā vidējā vērtība starp polinoma regresiju un kubisko splainu. Tādējādi dati tiek izlīdzināti, saglabājot caurlaidspējas pamattendences, bet samazinot trokšņu ietekmi tīklā un *RSSI*. Lietotais polinoms ir atkarīgs no polinoma pakāpes, kas var būt kvadrātiskā, kubiskā un 5. pakāpes, un aproksimācijas precizitātes [64]–[66].

Kubiskais splains tiek aprakstīts kā

$$S(x) = \sum_{i=1}^{m} b_i B_i(x), \tag{5.5}$$

kur $B_i(x)$ – bāzes splainu funkcijas; b_i – koeficienti, kas tiek aprēķināti, lai nodrošinātu gludu grafika interpolāciju; m – mezglu skaits.

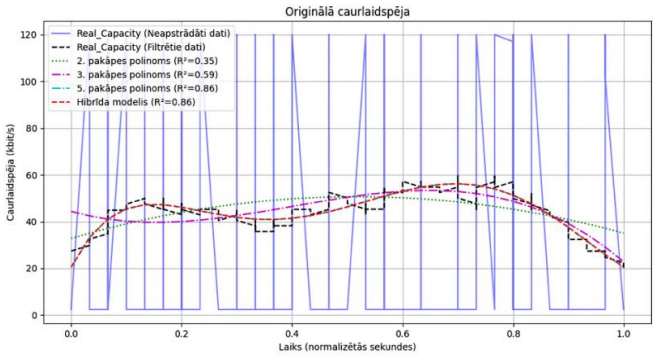
Splaina koeficienti tiek iegūti, minimizējot šādu kļūdu funkciju:

$$E = \sum_{i=1}^{N} \big(y_i - S(x_i)\big)^2 + \lambda \int \big(S''(x)\big)^2 dx, \tag{5.6}$$

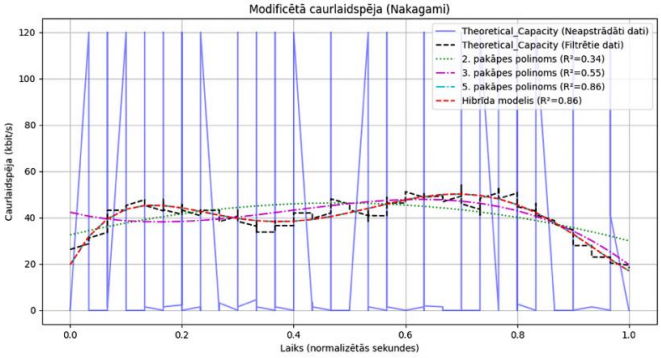
kur λ – regulējošais parametrs, kas nosaka, cik gluds būs splains [64].

Augstākas pakāpes polinoma pieejas un kubiskie splaini, kā arī to hibrīdmodeļi nodrošina optimālu līdzsvaru starp precizitāti un gludumu. Tie veiksmīgi filtrē trokšņus un akcentē būtiskās tendences, piemēram, strauju caurlaidspējas kritumu *DoS* un signāla traucēšanas uzbrukumu laikā vai atkopšanās procesu pēc aizsardzību aktivācijas.

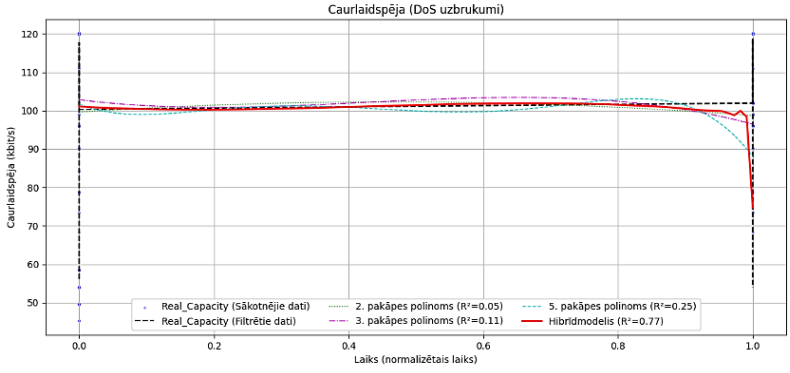
Polinomu un splaina integrācija ļauj identificēt uzbrukuma brīžus un modelēt tīkla adaptācijas spēju, kas atspoguļojas kā atjaunošanās fāze pēc traucējumiem. Īpaši svarīgi ir tas, ka modeļi tika validēti ar determinācijas koeficientu R^2, kur augstākas pakāpes modeļi demonstrēja ievērojami augstāku korelāciju ar reālajiem datiem, salīdzinot ar klasiskajām pieejām.



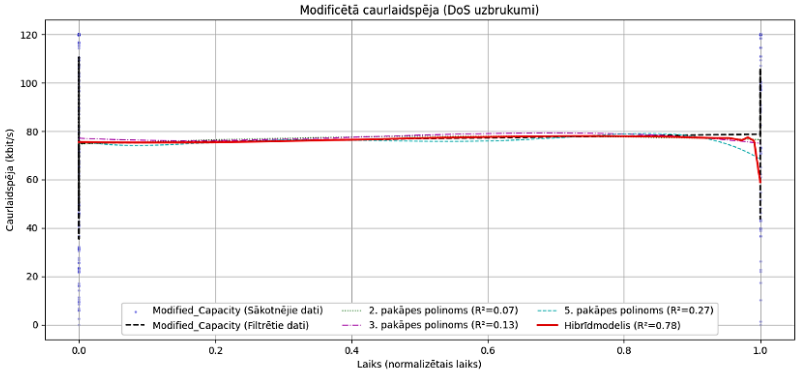
5.1. att. Tīkla caurlaidspējas izmaiņu analīze. Oriģinālie dati, pakešu sūtīšanas biežums – 0,25 sekundes ar polinomu un hibrīdmodeļiem pakešu injekcijas laikā.



5.2. att. Tīkla caurlaidspējas izmaiņu analīze. Modificētie dati, pakešu sūtīšanas biežums – 0,25 sekundes ar polinomu un hibrīdmodeļiem pakešu injekcijas laikā.

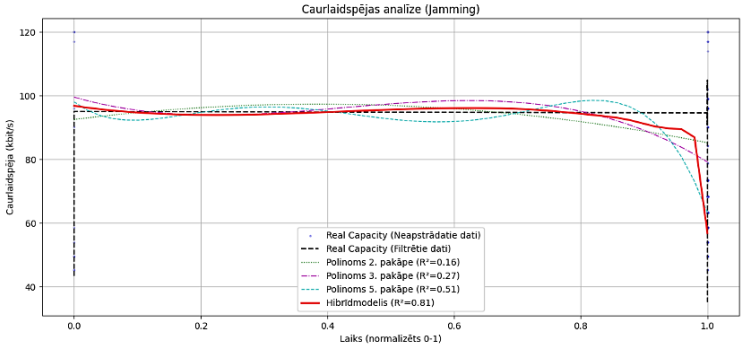


a)

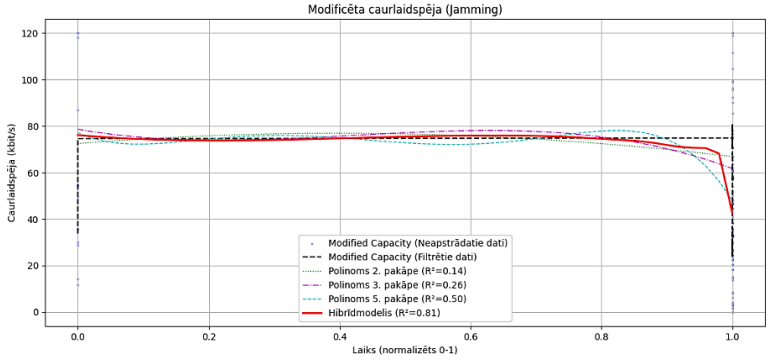


b)

5.3. att. Tīkla caurlaidspējas izmaiņu analīze: a) oriģinālie dati; b) modificētie dati ar polinomu un hibrīdmodeļiem *DoS* uzbrukuma laikā.

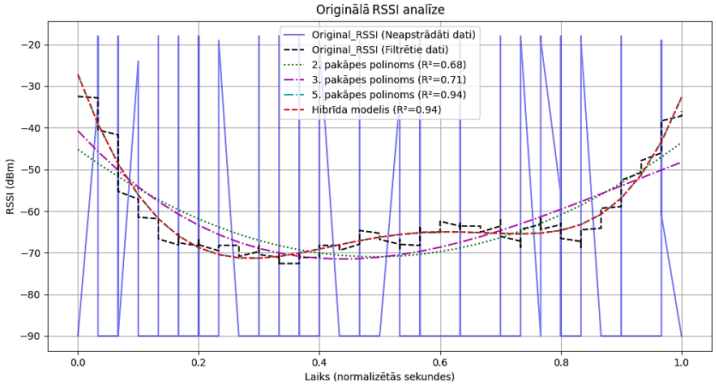


a)

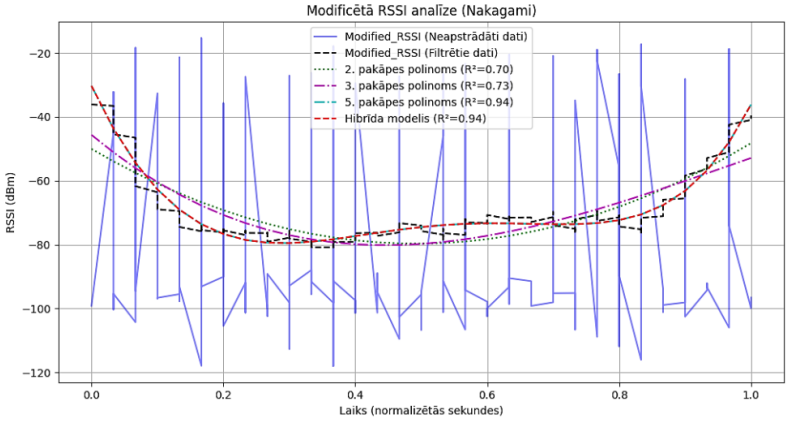


b)

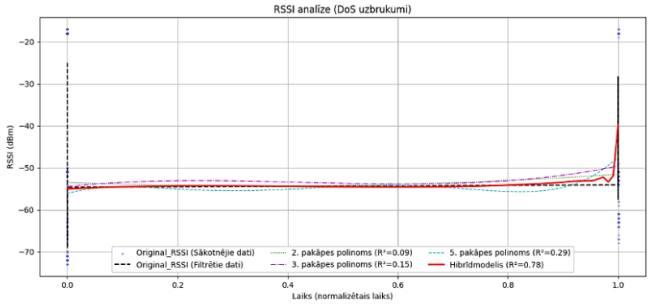
5.4. att. Tīkla caurlaidspējas izmaiņu analīze: a) oriģinālie dati; b) modificētie dati ar polinomu un hibrīdmodeļiem signāla traucēšanas uzbrukuma laikā.



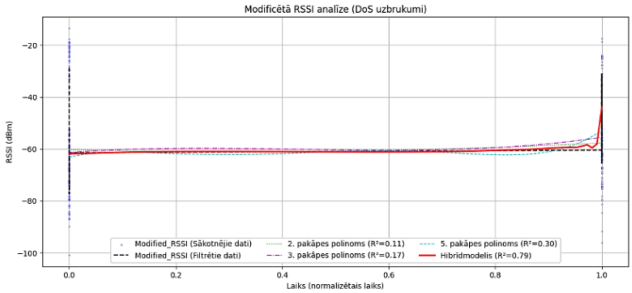
5.5. att. Signāla stipruma identifikatora analīze. Oriģinālie dati, pakešu sūtīšanas biežums – 0,25 sekundes ar polinomu un hibrīdmodeļiem pakešu injekcijas uzbrukuma laikā.



5.6. att. Signāla stipruma identifikatora analīze. Modificētie dati, pakešu sūtīšanas biežums – 0,25 sekundes ar polinomu un hibrīdmodeļiem pakešu injekcijas uzbrukuma laikā.

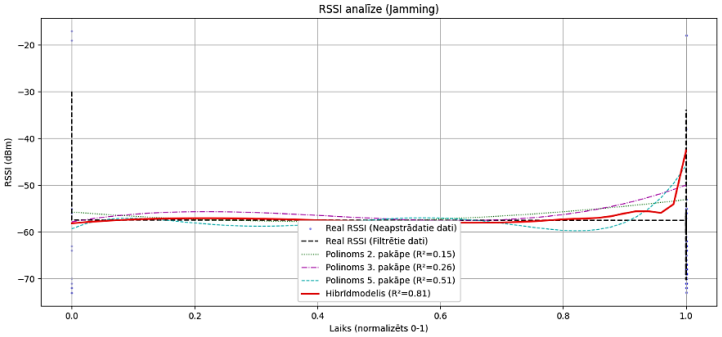


a)

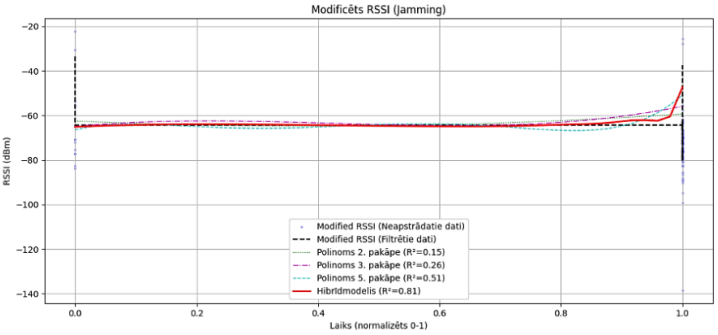


b)

5.7. att. Signāla stipruma identifikatora analīze: a) oriģinālie dati; b) modificētie dati ar polinomu un hibrīdmodeļiem *DoS* uzbrukuma laikā.



a)



b)

5.8. att. Signāla stipruma identifikatora analīze: a) oriģinālie dati; b) modificētie dati ar polinomu un hibrīdmodeļiem signāla traucēšanas uzbrukuma laikā.

Analīze rāda, ka gan *RSSI*, gan caurlaidspējas indikatoru izmaiņas var kalpot kā uzticami parametri automatizētām uzbrukumu detektēšanas sistēmām. Šāda pieeja ļauj izstrādāt dinamiskas aizsardzības mehānismus, kas pielāgojas tīkla slodzei un traucējumu veidam. Tika secināts, ka hibrīdmodeļi nodrošina vislabāko līdzsvaru starp datu pielāgošanu un trokšņu filtrēšanu, padarot tos īpaši piemērotus *IoT* uzbrukumu detektēšanai un tīkla atjaunošanas spēju novērtēšanai. Tiek secināts, ka piektajā nodaļā aprakstītais ierosina inovatīvu un matemātiski pamatotu pieeju *IoT* tīklu drošības novērtēšanai, kas var kļūt par pamatu turpmākai automatizētas aizsardzības stratēģiju attīstībai dažādos lietojuma scenārijos.

PROMOCIJAS DARBA SECINĀJUMI

Promocijas darba izstrādes gaitā veikts visaptverošs pētījums par bezvadu sakaru tīklu drošību, koncentrējoties uz izveidotu hibrīdtīklu *IEEE 802.11* un *IEEE 802.15.4* standartu un ievainojamībām ar iespējamo aizsardzības mehānismu ieviešanu, kas spētu nodrošināt tīkla stabilitāti un drošību dažādu kiberdraudu apstākļos. Darba mērķis bija izstrādāt un novērtēt efektīvus aizsardzības risinājumus pret uzbrukumiem *IEEE 802.15.4* bezvadu tīklā, tostarp *DoS*, signāla traucēšanas un pakešu injekcijām, kā arī izvērtēt tīkla caurlaidspēju, signāla stipruma identifikatora un tīkla atjaunošanas spējas pēc uzbrukumiem.

Pirmajā nodaļā analizēti *IEEE 802.11* un *IEEE 802.15.4* standarti, īpaši uzsverot to lietojumu *IoT* tīklos. *IEEE 802.15.4* standarts, kas tiek plaši lietots *Zigbee* tīklos, izstrādāts zemas caurlaidspējas komunikācijām un mazas joslas platuma sakariem, padarot to par populāru izvēli *IoT* ierīcēm. Energoefektīvā arhitektūra ļauj nodrošināt ilgu ierīču darbības laiku, taču šim ieguvumam ir arī otra puse – zemas drošības iespējas un lielāka ievainojamība pret uzbrukumiem, piemēram, *DoS* un signāla traucēšanas uzbrukumiem. Nodaļā apskatītas arī *IEEE 802.11* standarta drošības ievainojamības, piemēram, *WPA2* un *WPA3* šifrēšanas uzbrukumi, kas vēl aizvien rada būtiskus draudus *Wi-Fi* tīkliem. Galvenie secinājumi – *IEEE 802.15.4* tīkli ir īpaši jutīgi pret dažāda uzbrukuma veidiem ierobežotā resursu patēriņa un 2,4 GHz diapazona frekvenču joslas izmantošanas dēļ, savukārt IEEE 802.11 standarti, lai arī nodrošina augstāku datu pārraides ātrumu, nav pasargāti no drošības ievainojamībām.

Otrajā nodaļā padziļināti analizēti dažādi tīkla uzbrukumu veidi un to ietekme uz *IEEE 802.11* un *IEEE 802.15.4* tīklu veiktspēju. Nodaļā apskatīti galvenie uzbrukumu veidi, kas ietekmē bezvadu tīklu darbību, tostarp *DoS* uzbrukumi un pakešu injekcijas, kā arī analizēts, kā šie uzbrukumi ietekmē tīkla caurlaidspēju un kopējo tīkla stabilitāti. Nodaļā apskatīti arī aizsardzības mehānismi, kas spēj lietot *IEEE 802.11* un *IEEE 802.15.4* tīklus, lai spētu aizsargāt tīklu no dažādiem uzbrukumiem. Secinājumos definēts, kādi uzbrukuma veidi tiks lietoti eksperimentālajā tīklā un to pamatdarbības un ietekme.

Trešajā nodaļā detalizēti aprakstīta izstrādātā eksperimentālā vide un izmantotās tehnoloģijas, kas tika lietotas tīkla signāla stipruma identifikatora (*RSSI*), tīkla caurlaidspējas un drošības analīzei. Eksperimentos tika izmantotas vairākas ierīces, tostarp *RZUSBstick* uzbrukuma veikšanas ierīce un *CC2531* pakešu uzrauga modulis *IEEE 802.15.4* tīklā, kā arī *HackRF One* universālais *SDR* rīks pretpasākuma realizācijai. Nodaļā īpaša uzmanība pievērsta tīkla caurlaidspējas aprēķināšanai, izmantojot empīrisku modeli, kas balstīts Šenona teorēmā. Šī pieeja ļāva novērtēt

maksimālo teorētisko caurlaidspēju, ņemot vērā ideālus apstākļus pakešu pārraidei. Aprēķini parādīja, ka teorētiskā caurlaidspēja sasniedz līdz 250 kbit/s, taču, ņemot vērā reālos ierobežojumus, praktiski sasniegtā caurlaidspēja bija aptuveni 120 kbit/s. Eksperimentu laikā tika izmantots arī Nakagami sadalījums, lai modelētu signāla kvalitātes izmaiņas tīklā dažādos slodzes apstākļos. Fiksētie parametri ($M = 0{,}8$, $\Omega = 0{,}3$) nodrošināja precīzu signāla stipruma analīzi un tā ietekmi uz caurlaidspēju, ļaujot labāk izprast tīkla uzvedību traucējumu apstākļos. Eksperimentālie rezultāti parādīja, ka *DoS* uzbrukumi ievērojami pazemina tīkla caurlaidspēju, radot pārslogojumu un padarot tīklu nepieejamu legālām aktivitātēm, un aizsardzības efektivitāte *IEEE 802.15.4* tīklā sasniedza tikai 47,75 %, atklājot reālās vides sarežģītību un ārējo spēcīgu faktoru ietekmi, kas padara spēcīgāku *DoS* uzbrukuma darbību, bet nevar apgalvot, ka uzbrukums pilnībā ietekmē tīklu. Sakaru traucēšanas uzbrukums radīja signāla traucējumus, kas būtiski ietekmēja signāla kvalitāti un tīkla caurlaidspēju, samazinot to no sākotnējam vērtībām līdz 50,08 kbit/s. Aizsardzības mehānismu efektivitāte šajā gadījumā sasniedza 60,11 %, kas ir būtiski labāk nekā *DoS* uzbrukumos. Savukārt pakešu injekcijas uzbrukumi tika identificēti un bloķēti ar vislielāko precizitāti – 94,83 % reālajā vidē, izmantojot uzlabotas pakešu filtrēšanas un pakešu autentifikācijas metodes.

Ceturtajā nodaļā aprakstīta veikto eksperimentu rezultātu analīze, salīdzinot reālajā vidē un *Python* simulācijas vidē iegūtos rezultātus. Analīze parādīja, ka simulācijas vidē aizsardzības mehānismi darbojas ievērojami efektīvāk nekā reālajā vidē, kur tos ietekmē ārējie traucējumi, aparatūras ierobežojumi un citi vides faktori. Tika konstatēts, ka reālajā vidē *DoS* un traucēšanas uzbrukumi ievērojami ietekmē tīkla caurlaidspēju, bet efektīvi pretpasākumi, piemēram, dinamiskā frekvenču maiņa un pakešu filtrēšana, spēj samazināt uzbrukumu ietekmi par 40–60 %. Simulācijā *DoS* uzbrukumu aizsardzības efektivitāte sasniedza 93,33 %, sakaru signāla traucēšanas uzbrukuma aizsardzības efektivitāte – 78,05 %, savukārt pakešu injekcija simulācijas vidē ir sliktāka nekā reālajā tīklā (85,14 %).

Piektajā nodaļā novērtēti *IEEE 802.15.4* papildu veiktspējas un aizsardzības pasākumi izcilai tīkla darbībai, piemēram, mikrosegmentācija, *QoS* un arī *VLAN* izmantošana *IEEE 802.11* tīklos, kas netieši pārklājas, strādājot ar *IoT* tīkliem. Nodaļā veiksmīgi izmantoti polinomu regresijas modeļi tīkla darbības atjaunošanas prognozēšanai pēc uzbrukumiem. Piemēram, pēc *DoS* uzbrukuma tīkla darbspēja tika atjaunota līdz 85 % no sākotnējās caurlaidspējas 30 sekunžu laikā, izmantojot regresijas prognozēšanu. Tas apliecināja polinomu regresijas modeļu efektivitāti tīkla atjaunošanas prognozēšanā un uzlabošanā. Polinomu regresijas prognozes palīdzēja konstatēt ātrāku dinamikas atjaunināšanu tīkla darbību pēc uzbrukumiem, precīzi prognozējot atkopšanās

laiku (ar 96 % precizitāti). Šie mehānismi ievērojami uzlaboja tīkla drošību un veiktspēju, ļaujot efektīvi reaģēt uz dažādiem uzbrukuma scenārijiem.

Veiktie pētījumi skaidri parādīja, ka *IEEE 802.15.4* tīkli ir pakļauti uzbrukumiem, tomēr efektīvu aizsardzības mehānismu ieviešana spēj ievērojami uzlabot tīkla drošību un stabilitāti. Pētījuma laikā noskaidrots, ka *DoS* un traucēšanas uzbrukumi ir visgrūtāk novērojami, jo tie ietekmē tīkla darbību jau fiziskā slānī, radot būtiskus traucējumus signāla pārraidē un tīkla darbspējā. Savukārt pakešu injekcijas uzbrukumi tika identificēti kā visefektīvāk bloķējamie, pateicoties uzlabotām pakešu filtrēšanas mehānismiem, kas ļāva novērst nelikumīgu datu plūsmu.

Lai modelētu *RSSI* izmaiņas dažādos apstākļos, nodrošinot precīzu signāla kvalitātes analīzi un palīdzot novērtēt tīkla darbību uzbrukumu laikā, veiksmīgi tika izmantots Nakagami sadalījums. Turklāt izstrādātā simulāciju vide sniedza drošu platformu dažādu uzbrukumu scenāriju un aizsardzības mehānismu testēšanai pirms to ieviešanas reālajā vidē, kas ļāva optimizēt aizsardzības stratēģijas un novērtēt to efektivitāti.

Praktiskā nozīme šim pētījumam ir ievērojama, jo izstrādātos aizsardzības mehānismus var lietot dažādos *IoT* un *Zigbee* tīklos, uzlabojot drošību un stabilitāti. Tādi risinājumi ir piemērojami gan viedajām mājām, gan industriālajiem tīkliem, kur nepieciešama augsta drošības pakāpe, lai aizsargātu datus un nodrošinātu stabilu tīkla darbību.

Nākotnē pētījumus būtu lietderīgi turpināt, paplašinot izpēti vairākos virzienos. Viens no tiem ir mašīnmācīšanās algoritmu integrācija, lai uzlabotu uzbrukumu prognozēšanas un noteikšanas spējas, kas ļautu proaktīvi novērst potenciālos draudus, pirms tie ietekmē tīkla darbību. Būtu vērtīgi arī paplašināt eksperimentus lielāka mēroga tīklos, kuros darbojas vairāk nekā 100 *IoT* ierīces, lai novērtētu izstrādāto aizsardzības mehānismu efektivitāti lielākos un sarežģītākos tīklos. Turklāt ir svarīgi testēt aizsardzības mehānismus hibrīdtīklos, kur vienlaikus darbojas *IEEE 802.11* un *IEEE 802.15.4* standarti, jo šādi tīkli kļūst arvien izplatītāki mūsdienu *IoT* infrastruktūrā.

Salīdzinošā analīze ar tradicionālajiem tīkla drošības risinājumiem

Salīdzinot promocijas darba rezultātus ar populāriem tīkla drošības avotiem, var secināt, ka autors piedāvā jaunu pieeju *Zigbee* tīklu drošībai. Atšķirībā no literatūras avotiem kurā galvenā uzmanība tiek pievērsta vispārējai tīkla drošībai, autentifikācijas, piekļuves kontrolei un kriptogrāfisko algoritmu drošībai, promocijas darba pētījums ir orientēts uz specifisku *IEEE 802.15.4* un *IEEE 802.11* hibrīdtīklu drošības analīzi, analizējot reālus uzbrukumus un pretpasākumu veidus *Zigbee* tīklos [67], [68].

Promocijas darba galvenais jaunieguvums ir eksperimentāli pārbaudīta pieeja pakešu injekcijas, *DoS* un signāla traucēšanas uzbrukumiem *Zigbee* tīklā, kas līdz šim nav detalizēti

analizēti. Pētījuma laikā praktiski testētas dažādas uzbrukumu metodes un aizsardzības stratēģijas, piemēram, selektīva pakešu bloķēšana, adaptīvā traucēšana pēc pakešu galvenēm vai citiem parametriem un tīkla atjaunošanas modelēšana. Turklāt tika veikta eksperimentālā analīze, kas ietver reālas ierīces un programmatūru, kā arī matemātiskā modelēšana, kas ļauj precīzāk prognozēt tīkla darbību pēc uzbrukumiem.

IZMANTOTĀS LITERATŪRAS SARAKSTS

[1] Neuron Team. “KNX Protocol: The Basics and Its Possibilities with IoT”. Emqx.com. https://www.emqx.com/en/blog/knx-protocol (pieejams Nov. 10, 2023).

[2] V. Shashkina. “IoT solution architecture: an overview of components & design tips.” Itrexgroup.com. https://itrexgroup.com/blog/iot-architecture-components-design-tips/ (pieejams Aug. 31, 2022).

[3] AVSystem. “IoT Protocols & Standards Guide – Protocols of the Internet of Things.” Avsystem.com. https://avsystem.com/blog/iot/iot-protocols-and-standards (pieejams Jul. 6, 2024).

[4] TDT BMS. “How a battery management system (BMS) works and its role in different sectors.” https://www.tdtbms.com/ru/news/-how-a-battery-management-system-bms-works-and-its-importance-across-industries.html (pieejams Aug. 8, 2024).

[5] B. Toulas. “Bleeping Computer Chinese cyberspies use new SSH backdoor in network device hacks.” Bleepingcomputer.com. https://www.bleepingcomputer.com/news/security/chinese-cyberspies-use-new-ssh-backdoor-in-network-device-hacks/ (pieejams Feb. 4, 2025).

[6] R. A. Shaikh. “Backdoor uncovered in China-made patient monitors – Contec CMS8000 raises questions about healthcare device security.” Tomhardware.com. https://www.tomshardware.com/tech-industry/cyber-security/backdoor-uncovered-in-china-made-patient-monitors-contec-cms8000-raises-questions-about-healthcare-device-security (pieejams Feb. 1, 2025).

[7] Yiming Li, Yong Jiang, Zhifeng Li, Shu-Tao Xia, “Backdoor Learning: A Survey”, 2020, p. 17.

[8] PIRIT. “Information Security.” Pirit.biz. https://pirit.biz/reshenija/informacionnaja-bezopasnost (pieejams Apr. 12, 2019).

[9] Payatu Security. “Zigbee Security 101: Architecture and Security Issues.” Payatu.com. https://payatu.com/blog/zigbee-security-101-architecture-and-security-issues/ (pieejams Feb. 11, 2023).

[10] Kudelski Security. “Zigbee Security Basics: Part 3. ” Research.kudelskisecurity.com. https://research.kudelskisecurity.com/2017/11/21/zigbee-security-basics-part-3/ (pieejams Nov. 21, 2017).

[11] Ancāns A., “Research And Improvement Of The Performance Of Road Transport Wireless Communication Networks”, RTU Press, 2021, 175 p.

[12] Saliga S. V., “An introduction to IEEE 802.11 wireless LANs”, IEEE Xplore, 2000, 10 p.

[13] Tektronix. “Wi-Fi Overview: 802.11 Physical Layer and Transmitter Measurements // Tektronix.” Tek.com. https://www.tek.com/en/documents/primer/wi-fi-overview-80211-physical-layer-and-transmitter-measurements (pieejams 2017).

[14] Sharma, P., Singh G., “Comparison of Wi-Fi IEEE 802.11 Standards Relating to Media Access Control Protocols”, International Journal of Computer Science and Information Security, 2016, 7 pp.

[15] Kurnaz C., Engiz B. K., Kose U., “Investigating the effect of number of users on signal strength level and throughput for Wi-Fi system”, IEEE, 2017, 4 pp.

[16] Song, X., Wu, M., Jermaine, C., Ranka, S. “Using support vector machines for anomalous change detection”, Proceedings of the 3rd IEEE International Conference on Data Mining (ICDM 2003), 2003, pp. 626–629.

[17] Banerjee, S., Sharan, A. “WiFi-LSTMs: A deep learning approach for WiFi based human activity recognition”, IEEE Access, 2021, Vol. 9.

[18] NetSpot. “Wireless Security Protocols : WEP, WPA, WPA2, and WPA3.” Netspotapp.com. https://www.netspotapp.com/blog/wifi-security/wifi-encryption-and-security.html.

[19] HFCL. “WPA2 vs WPA3: Key Difference in Wi-Fi Security Protocols.” HFCL.com. https://io.hfcl.com/blog/wpa2-vs-wpa3/ (pieejams May. 7, 2024).

[20] Cisco Meraki. “WPA3 Encryption and Configuration Guide.” Meraki.com. https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/WPA3_Encryption_and_Configuration_Guide (pieejams Apr. 15, 2025).

[21] Telecommunication Standardization Sector of ITU, “Series Y: Global Information Infrastracture, Internet Protocol Aspects and Next-Generation Networks, Next Generation Network – Frameworks and Functional Architecture Models, Overview of the Internet of Things”, 2012.

[22] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M. “Internet of Things: A General Overview between Architectures, Protocols and Applications,” IEEE Communications Surveys & Tutorials, Vol. 17, No. 4, pp. 2347–2376, Oct. 2015, DOI: 10.1109/COMST.2015.2444095.

[23] **Aleksandrovs-Moisejs, D.,** Ipatovs, A., Grabs, E., Rjazanovs, D., Sinuks, I. “Arduino-based temperature sensor organization and design,” 2023 Photonics & Electromagnetics Research Symposium (PIERS), Aug. 2023, DOI: 10.1109/PIERS59004.2023.10221361.

[24] B. K.Sethi, “Your complete guide to IoT protocols and standards in 2022 for support secure data exchange.” Kellton.com. https://www.kellton.com/kellton-tech-blog/your-complete-guide-to-iot-protocols-and-Standards-2022 (pieejams Mar. 15, 2022).

[25] NetworkLessons. “IoT Standards and Protocols.” NetworkLessons.com. https://networklessons.com/cisco/evolving-technologies/iot-standards-and-protocols.

[26] Allerin. “Six Types of IoT Network Protocols” Allerin.com https://www.allerin.com/blog/six-types-of-iot-network-protocols.

[27] L. Frenzel. “What’s the Difference Between IEEE 802.15.4 and Zigbee Wireless?” Electronicdesign.com. https://www.electronicdesign.com/technologies/communications/wireless/article/21796046/whats-the-difference-between-ieee-802154-and-zigbee-wireless (pieejams Mar. 22, 2013).

[28] GeeksforGeeks. “Introduction of IEEE 802.15.4 Technology” GeeksforGeeks.org https://www.geeksforgeeks.org/introduction-of-ieee-802-15-4-technology/ (pieejams Feb. 22, 2023).

[29] Saleem S., Ullah S., Kwak K. S., “A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks”,Graduate School of Information & Communication Engineering, Jan. 2011, pp. 13.

[30] Goldoni E., Savioli A., Risi M., Gamba P., “Experimental analysis of RSSI-based indoor localization with 802.15.4”, IEEE Xplore, May 2010, pp. 8.

[31] Delsing J., Eliasson J., Leijon V., “Latency and Packet Loss of an Interferred 802.15.4 Channel in an Industrial Environment”, SensorComm 2010, July 2010, pp. 9.

[32] Latre B., De Mil P., Moerman I., Dierdonck N. V., Dhoedt B., Demeester P., “Maximum Throughput and Minimum Delay in IEEE 802.15.4”, Mobile Ad-hoc and Sensor Networks, First International Conference, MSN 2005, Dec. 2005, pp. 12.

[33] Shu F., Sakurai T., Zukerman M., Vu H., “Packet loss analysis of the IEEE 802.15.4 MAC without acknowledgments”, IEEE Communications Letters, Jan. 2007, pp. 4.

[34] Hacking Land. “KillerBee - IEEE 802.15.4/ZigBee Security Research Toolkit” Hacking.land. https://www.hacking.land/2018/07/killerbee-ieee-802154zigbee-security.html?m=1 (pieejams Jul. 2018).

[35] River Loop Security. “KillerBee Project Overview” RiverLoopSecurity.com. https://riverloopsecurity.com/projects/killerbee/.

[36] “AVR2016: RZRaven Hardware User’s Guide”, Microchip Documentation, https://manualzz.com/doc/19793759/avr2016--rzraven-hardware-user-s-guide-8-bit-microcontrol.

[37] Microsoft. “What is Information Security (InfoSec)?”, Microsoft Security, 2024.

[38] Sousa de Araujo M., Souza Machado B.A., Passos F.U., “Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance”, Progress and Research in Cybersecurity and Data Privacy, Mar. 2024, pp. 16.

[39] Kolias, C., Kambourakis, G., Stavrou, A., Voas, J., “DDoS in the IoT: Mirai and Other Botnets” ResearchGate, Jan 2017, pp. 6, DOI: 10.1109/MC.2017.201.

[40] Mazhar T., Talpur D.B., Al Shloul T., Ghadi Y.Y., Haq I., Ullah I., Ouahada K., Hamam H., “Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence”, MDPI Intelligent Neural Systems for Solving Real Problems, Apr. 2023, pp. 30.

[41] Singh J., Rani S., Kumar V., “Role-Based Access Control (RBAC) enabled secure and efficient data processing framework for IoT networks,” International Journal of Communication Networks and Information Security (IJCNIS), Vol. 16, No. 2, Aug. 2024. pp. 19–32.

[42] Security Scorecard. “Cybersecurity for the Internet of Things (IoT)” SecurityScorecard.com. https://securityscorecard.com/blog/cybersecurity-for-the-internet-of-things-iot/ (pieejams Feb. 8, 2024).

[43] Texas Instruments: CC2531 Datasheet, Texas Instruments. – https://www.ti.com/lit/ds/symlink/cc2531.pdf.

[44] Adafruit. Great Scott Gadgets HackRF One – Software Defined Radio. – https://www.adafruit.com/product/3583.

[45] MetaGeek. “Zigbee and Wi-Fi Coexistence” MetaGeek.com. 2024. https://www.metageek.com/training/resources/zigbee-wifi-coexistence/ (pieejams 2024).

[46] NS2Project. “How to Calculate Network Channel Capacity in NS2” NS2Project.com. https://www.ns2project.com/how-to-calculate-network-channel-capacity-in-ns2/ (pieejams 2024).

[47] Haque K. F., Abdelgawad A., Yelamarthi K.., “Comprehensive Performance Analysis of Zigbee Communication: An Experimental Approach with XBee S2C Module”, MDPI Reliability Analysis of Wireless Sensor Network, Apr. 2022, pp. 23.

[48] Lanzisera S., Mehta A. M., Pister K. S. J., “Reducing Average Power in Wireless Sensor Networks Through Data Rate Adaptation”, Communications, 2009. ICC '09. IEEE International Conference, Jul. 2009, p. 6.

[49] Rupareliya K., “Top 6 Factors To Consider When Designing the IoT Infrastructure”, Spiceworks.com. https://www.spiceworks.com/tech/iot/guest-article/factors-to-consider-when-designing-the-iot-infrastructure/ (pieejams Sept. 20, 2021).

[50] Burchfield T. R., Venkatesan S., Weiner D., “Maximizing Throughput in ZigBee Wireless Networks through Analysis, Simulations and Implementations.”, MobiusConsulting.com., 2007, pp. 13.

[51] Goyal M., Prakash S., Xie W., Bashir Y., Hosseini S. H., Durresi A., “Evaluating the Impact of Signal to Noise Ratio on IEEE 802.15.4 PHY-level Packet Loss Rate”, The 13th International Conference on Network-Based Information Systems, NBiS 2010, 2010, pp. 279-284.

[52] Di Marco P., Fischione C., Santucci F., Johansson K.H., “Modeling IEEE 802.15.4 Networks over Fading Channels”, IEEE Transactions on Wireless Communications, Sept. 2012, pp. 30.

[53] Bandur D., Jaksic B., Raicevic A., Popovic B., Bandur M., “Performance Analysis of an IEEE 802.15.4 Network Operating Under κ–μ Fading, Interference and AWGN”, Iranian Journal of Science and Technology, Transactions of Electrical Engineering, Vol. 44, Mar. 2020, pp. 1549–1557.

[54] Molisch A.F., Balakrishnan K., Cassioli D., Chong C-C., Emami S., Fort A., Karedal J., Kunisch J., Schantz H., Schuster U., Siwiak K., “Channel Model Final Report for IEEE 802.15.4a”, IEEE Communications, Jan 2004., pp. 40.

[55] Carnegie Mellon University. Zigator: Security Analysis of Zigbee Networks. – https://mews.sv.cmu.edu/research/zigator.

[56] Lopez-Vilos N., Valencia-Cordero C., Azurdia-Meza C., Montejo-Sanchez S., Mafra S.B., “Performance Analysis of the IEEE 802.15.4 Protocol for Smart Environments under Jamming Attacks”, MDPI Cyber Security in IoT Era, Jun. 2021, pp. 26.

[57] Khanji S., Iqbal F., Hung P.C.K., “ZigBee Security Vulnerabilities: Exploration and Evaluating”, The 10th International Conference on Information and Communication Systems 2019, Jul. 2019, pp. 6.

[58] Rajawat A.S., Mohammed O., Shaw R.N, Ghosh A., “Applications of AI and IoT in Renewable Energy,” Chapter 6 – Renewable energy system for industrial internet of things model using fusion-AI, 2022, pp. 107–128.

[59] StatisticsHowTo. “Root Mean Square Error (RMSE) Calculation.” Statisticshowto.com. https://www.statisticshowto.com/probability-and-statistics/regression-analysis/rmse-root-mean-square-error/.

[60] Rapid7. “What is Security Orchestration, Automation, and Response (SOAR)?” Rapid7.com. https://www.rapid7.com/fundamentals/what-is-soar/

[61] Varga P., Plosz S., Soos G., Hegedus C., “Security threats and issues in automation IoT”, 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), Jul. 2017.

[62] Al-Ofeishat H.A., Alshorman R., “Build a Secure Network Using Segmentation and Micro-segmentation Techniques”, International Journal of Computing and Digital Systems, Jul. 2024, pp. 1499–1508.

[63] UC Berkeley. Quality of Service in Wireless Networks. UC Berkeley Lecture Notes – https://people.eecs.berkeley.edu/~istoica/classes/cs268/06/notes/13-QoSx2.pdf.

[64] Scikit-learn. “Polynomial Regression for Signal Analysis.”Scikit-learn Documentation.

[65] Fletcher S.J., “Data Assimilation for the Geosciences”, Chapter 10 – Introduction to Semi-Lagrangian Advection Methods, 2017, pp. 361–441.

[66] Hodges L., “Methods in Experimental Physics”, Vol. 28, Common Univariate Distributions, 1994, pp. 35–61.

[67] Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson Education, 2011.

[68] Ferguson, N., Schneier, B., Kohno, T. Cryptography Engineering: Design Principles and Practical Applications. Wiley, 2010.

Daniils Aleksandrovs-Moisejs dzimis 1997. gadā. Rīgas Tehniskajā universitātē (RTU) ieguvis akadēmisko inženierzinātņu bakalaura grādu elektrozinātnē (2019) un akadēmisko inženierzinātņu maģistra grādu telekomunikācijās (2021). Kopš 2020. gada strādā VSIA "Traumatoloģijas un ortopēdijas slimnīca", ieņemot Informācijas tehnoloģiju un datortehnikas apkopes nodaļas IT speciālista amatu. Patlaban ir RTU Datorzinātnes, informācijas tehnoloģijas un enerģētikas fakultātes Fotonikas, elektronikas un elektronisko sakaru institūta pētnieks un lektors. Zinātniskās intereses saistītas ar tīkla drošumu, bezvadu sakaru tīkliem un vadu/bezvadu sensoru tīkliem.