KAUNO TECHNOLOGIJOS UNIVERSITETAS
ELEKTROS IR ELEKTRONIKOS FAKULTETAS

Modestas Kasnauskas

MOBILIOJO RYŠIO TINKLO BLOKAVIMO GALIMYBIŲ TYRIMAS

Baigiamasis magistro projektas

Vadovas
Doc. dr. Vitas Grimaila

KAUNAS, 2017

KAUNO TECHNOLOGIJOS UNIVERSITETAS
ELEKTROS IR ELEKTRONIKOS FAKULTETAS
TELEKOMUNIKACIJŲ KATEDRA

MOBILIOJO RYŠIO TINKLO BLOKAVIMO GALIMYBIŲ TYRIMAS

Baigiamasis magistro projektas
Išmaniosios telekomunikacijų technologijos (621H64001)

Vadovas
(parašas) Doc. dr. Vitas Grimaila
(data)

Recenzentas
(parašas) Doc. dr. Saulius Japertas
(data)

Projektą atliko
(parašas) Modestas Kasnauskas
(data)

KAUNAS, 2017

KAUNO TECHNOLOGIJOS UNIVERSITETAS

Elektros ir elektronikos fakultetas

(Fakultetas)

Modestas Kasnauskas

(Studento vardas, pavardė)

Išmaniosios telekomunikacijų technologijos (kodas 621H64001)

(Studijų programos pavadinimas, kodas)

Baigiamojo projekto „Mobiliojo ryšio tinklo blokavimo galimybių tyrimas“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 17 m. gegužės 26 d.

Kaunas

Patvirtinu, kad mano **Modesto Kasnausko** baigiamasis projektas tema „Mobiliojo ryšio tinklo blokavimo galimybių tyrimas“ yra parašytas visiškai savarankiškai, o visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

(vardą ir pavardę įrašyti ranka) *(parašas)*

Kasnauskas, Modestas. Mobiliojo ryšio tinklo blokavimo galimybių tyrimas. Telekomunikacijų inžinerijos magistro baigiamasis projektas / vadovas doc. dr. Vitas Grimaila; Kauno technologijos universitetas, Elektros ir elektronikos fakultetas, Telekomunikacijų katedra.

Mokslo kryptis ir sritis: Elektros ir elektronikos inžinerija, Technologiniai mokslai

Reikšminiai žodžiai: *GSM, UMTS, LTE, signalo blokavimas, IMSI gaudyklė, padengimas*.

Kaunas, 2017. 88 p.

SANTRAUKA

Šiame magistro baigiamajame darbe tiriamos mobiliojo ryšio tinklo blokavimo galimybės. Išskiriami du būdai blokavimui atlikti: mobiliojo signalo tarp vartotojo įrenginio ir tinklo bazinės stoties blokavimas bei signalo tarp vartotojo įrenginio ir tinklo bazinės stoties pagavimas bei manipuliavimas juo. Analizuojami abu minėti būdai, detalizuojami jų veikimo principai, nagrinėjami visi blokavimo procese dalyvaujantys elementai. Taip pat analizuojami šia tematika atlikti moksliniai darbai.

Darbe apžvelgiami populiariausi radijo bangų sklidimo lauke, į pastatus bei pastatų viduje modeliai, detalizuojami svarbiausi blokuojantį signalą siunčiančių įrenginių siųstuvų antenų parametrai. Taip pat aprašoma mobiliojo ryšio tinklo struktūra ir GSM, UMTS bei LTE technologijų saugumo mechanizmai, kurie naudojami komunikavime tarp vartotojo įrenginio ir tinklo bazinės stoties.

Tiriamojoje darbo dalyje nustatomi pagrindiniai aprašytų blokavimo metodų trūkumai ir pateikiami sprendimai mobiliojo ryšio signalų pagavimo bei blokavimo efektyvinimui. Projektuojamas Pravieniškių pataisos namų-atvirosios kolonijos teritoriją padengiantis GSM, UMTS bei LTE technologijų mobiliojo ryšio signalų pagavimo įrangos tinklas.

Kasnauskas, Modestas. Study Of Blocking Feasibility Of Mobile Network: Master's thesis in Telecommunications engineering master degree / supervisor doc. dr. Vitas Grimaila; Kaunas University of Technology, Faculty of Electrical and Electronics Engineering, department of Telecommunications.

Research area and field: Electrical and Electronics Engineering, Technological Sciences

Key words: *GSM, UMTS, LTE, jammer, IMSI catcher, coverage*

Kaunas, 2017. 88 p.

SUMMARY

In this master's thesis blocking feasibility of mobile network is studied. There are two ways to accomplish blocking: jam the mobile signal or use IMSI catcher. This paper analyzes both of them, looks into their operating principles and details all elements involved in the blocking process. It also analyzes scientific work performed in this topic.

This paper gives an overview of the most popular outdoor, outdoor to indoor and indoor radio wave propagation models. Moreover, it details key parameters of radio wave transmitting antennas. It also describes the structure of the mobile network and GSM, UMTS, LTE network security procedures that are used in communication between mobile station and the base station.

In the last part of this paper major limitations of jammers and IMSI catchers are described. Moreover, solutions that makes blocking of mobile signal more efficient are proposed. In the end GSM, UMTS and LTE technology network of IMSI catchers, which covers territory of open prison colony of Pravieniškės is designed.

TURINYS

SANTRUMPŲ IR ŽENKLŲ AIŠKINIMO ŽODYNAS

- GSM (angl. *Global System for Mobile Communications*, originalo kalba *Groupe Spécial Mobile*) - globalus mobilių telefonų ryšio standartas;
- UMTS (angl. *Universal Mobile Telecommunications System*) – trečios kartos mobiliojo ryšio sistema;
- LTE (angl. *Long-Term Evolution*) – didelės spartos duomenų perdavimo standartas skirtas mobiliesiems įrenginiams;
- eNodeB (angl. *E-UTRAN Node B*) – LTE tinklo bazinė stotis;
- UE (angl. U*ser Equipment*) – vartotojo galinė įranga LTE tinkle;
- IMSI (angl. *International Mobile Subscriber Identity*) – unikalus mobiliojo ryšio tinklo vartotojo tapatumo kodas;
- DoS (angl. *Denial-of-Service*) – atkirtimo nuo paslaugos ataka;
- VPN (angl. *Virtual Private Network*) – virtualus privatus tinklas;
- HLR (angl. *Home Location Register*) – buvimo registras;
- VLR (angl. *Visitor Location Register*) – lankytojo registras;
- MS (angl. *Mobile Station*) – judrioji stotis;
- SIM (angl. *Subscriber identification module*) – abonento identifikavimo modulis;
- MCC (angl. *Mobile Country Code*) – mobilus šalies kodas;
- MNC (angl. *Mobile Network Code*) – mobilus operatoriaus tinklo kodas;
- MSIN (angl. *Mobile Subscription Identification Number*) – mobilus abonento identifikacijos numeris;
- IMEI (angl. *International mobile station equipment identity*) - tarptautinis mobiliojo telefono tapatumo kodas;
- BS (angl. *Base Station*) – bazinė stotis;
- BSC (angl. *Base Station Controller*) – bazinės stoties valdiklis;
- AuC (angl. *Authentication Center*) – autentifikavimo centras;
- EIR (angl. *Equipment Identity Register*) – įrangos identifikavimo registras;
- FDD (angl. *Frequency Division Duplex*) – dažninis dvipusis atskyrimas;
- TDD (angl. *Time Division Duplex*) – laikinis dvipusis atskyrimas;
- MBMS (angl. *Multimedia Broadcast Multicast Services* – multimedijos transliavimo paslauga;
- RRC (angl. *Radio Resource Control*) – radijo resursų kontrolės protokolas;

- RAND (angl. *Random Number*) – atsitiktinis numeris;
- SRES (angl. *Signed Response*) – patvirtintas atsakymas;
- TMSI (angl. *Temporary mobile subscriber identity*) – laikinas mobiliojo ryšio tinklo vartotojo tapatumo kodas;
- USIM (angl. *Universal subscriber identification module*) – universalus abonento identifikavimo modulis;
- XRES (angl. *Expected Response*) – tikėtinas atsakymas;
- CK (angl. *Cipher Key*) – šifro raktas;
- IK (angl. *Integrity Key*) – vientisumo raktas;
- AUTN (angl. *Authentication Token*) – autentifikavimo raktas;
- SQN (angl. *Sequence Number*) – eilės numeris;
- AMF (angl. *Authentication Management Field*) – autentifikavimo valdymo sritis;
- SN ID (angl. *Serving Network Identity*) – paslaugas teikiančio tinklo tapatybės kodas;
- FTB (angl. *Federal Bureau of Investigation*) – federalinis tyrimų biuras;
- CID (angl. *Cell ID*) – celės identifikacinis numeris;
- LAC (angl. *Location Area Code*) – buvimo vietovės kodas;
- SS7 (angl. *Signaling System 7*) – septintos kartos signalizavimo sistema;

ĮVADAS

Mobiliojo ryšio skvarba vis labiau didėja. Mobiliosios technologijos suteikia didžiulę naudą vartotojui, tačiau jos taip pat gali tarnauti ir nusikalstamai veikai. Teroristai gali naudoti mobiliojo ryšio įrenginius nuotoliniam sprogstamųjų įtaisų detonavimui ar bendravimui organizuojant teroro aktus. Panaudojant mobilųjį telefoną gali būti nutekinama informacija iš konfidencialių susitikimų ar pokalbių. Sudėtinga kontroliuoti mobiliųjų telefonų naudojimą ten kur jis yra draudžiamas, pavyzdžiui įkalinimo įstaigose nuteistiesiems draudžiama turėti ir naudotis mobiliaisiais telefonais, tačiau jie sugeba įvairiais būdais jų gauti ir moka, nepastebėti įkalinimo įstaigų darbuotojų, jais naudotis. Siekiant apsisaugoti nuo nesankcionuoto mobiliojo ryšio telefonų ar kitų mobiliojo ryšio įrenginių naudojimo, ryšys gali būti blokuojamas. Blokavimui atlikti dažniausiai naudojami du būdai: mobiliojo ryšio signalo tarp vartotojo ir tinklo bazinės stoties blokavimas skleidžiant blokuojantįjį signalą (triukšmą) ir mobiliojo ryšio signalo tarp vartotojo ir tinklo bazinės stoties pagavimas bei manipuliavimas juo. Blokuojantis signalas gali paveikti didesnę teritoriją nei norima blokuoti ir sutrikdyti paslaugų teikimą įprastiems vartotojams, o signalo pagavimo metodą galima apeiti. Net yra sukurtų specialių aplikacijų išmaniesiems įrenginiams, kurie gali identifikuoti tokio, signalą gaudančio prietaiso, veikimą vartotojo buvimo vietoje ir jį apie tai įspėti [1], [2].

Darbo tikslas ir uždaviniai

Darbo tikslas:

Išanalizuoti mobiliojo ryšio tinklo blokavimo galimybes ir pasiūlyti patobulinimų, kurie mobiliojo ryšio blokavimą padarytų efektyvesnį bei pasirinktoje teritorijoje sumodeliuoti mobilųjį ryšį blokuojančios įrangos tinklą.

Darbo uždaviniai:

1. Atlikti radijo bangų sklidimo modelių apžvalgą;
2. Atlikti šiuo metu naudojamų signalų pagavimo ir blokavimo metodų analizę;
3. Pateikti sprendimą mobiliojo ryšio signalų perėmimo ir blokavimo proceso patobulinimui, kuris padarytų jį efektyvesnį;
4. Atlikti mobiliojo ryšį blokuojančios įrangos tinklo signalo padengimo modeliavimą pasirinktoje teritorijoje.

1. DARBŲ, SUSIJUSIŲ SU RYŠIO BLOKAVIMU, APŽVALGA

Teorinis GSM technologijos 900 MHz ir 1800 MHz dažnių diapazone veikiančių telefonų detektoriaus ir mobiliojo ryšio blokavimo prietaiso projekto aprašymą savo moksliniame straipsnyje kartu su kolegomis publikavo Rehna V J [3]. Šiame darbe pateikiamas pasyvaus mobiliojo ryšio blokavimo įrenginio, kuris pasirinktoje vietovėje skanuoja minėtų dažnių spektrą ir aptikęs radijo bangų aktyvumą pradeda skleisti blokuojantįjį signalą, teorinis modelis.

Ahmad Jisrawi savo darbe pateikia GSM 900 MHz dažnių ruožą blokuojančio įrenginio kūrimo namų sąlygomis procesą. Darbe taip pat pateikiami galutinio produkto praktinio bandymo rezultatai, kurie, įvertinus įrenginio pagaminimo kaštus, yra pakankamai geri – stipraus GSM signalo zonoje blokavimas sėkmingas 10 m. spinduliu, o silpno signalo zonoje 20 m. [4]. Aktyvaus GSM ir UMTS mobiliojo ryšio blokavimo įrenginio projektavimas ir realizavimą savo straipsnyje aprašo Shantanu Krishna Mahato [5].

Roger Piqueras Jover savo darbe nagrinėja teorines galimybes blokuoti mobilųjį ryšį LTE tinkle naudojant išmanaus aukštynkrypčio signalo blokavimo techniką, kuri nereikalauja didelės galios siųstuvo. Siekiant užblokuoti ryšį visoje LTE bazinės stoties (eNodeB) ar celės aprėpties teritorijoje, pakaktų įprasto galinio įrenginio (UE) skleidžiamo signalo galios – 23 dBm. Blokavimo efektyvumui pagerinti blokuojančio signalo siuntimui autorius rekomenduojama naudoti kryptinę anteną nukreipiant ją į eNodeB [6].

Chris Paget 2010 metais vykusioje „DEF CON 18“ konferencijoje realiai pademonstravo namų sąlygomis sukurtos IMSI gaudyklės, kuri veikia GSM technologijoje, veikimą. [7]. Adam Kostrzewa savo darbe nagrinėja GSM A5/2 šifro režimo pažeidžiamumą, kuriuo pasinaudojant galima atlikti tarpinio įsilaužimo (angl. *man-in-the-middle*) ataką. Jis taip pat aprašo tokios IMSI gaudyklės projektavimo ir kūrimo procesą bei pateikia realaus bandymo rezultatus [8]. Ulrike Meyer ir Susanne Wetzel savo straipsnyje nagrinėja teorines galimybes IMSI gaudykle pagauti UMTS tinkle veikiančios judriosios stoties siunčiamą signalą panaudojant hibridinio UMTS ir GSM tinklo saugumo spragas [9]. Stig F. Mjolsnes ir Ruxandra F. Olimid 2017 m. pradžioje publikavo mokslinį straipsnį, kuriame aprašo, kaip pasinaudojus LTE saugumo spragomis, galima surinkti netoliese esančių įrenginių IMSI numerius ir atlikti DoS ataką [10]. Roger Piqueras Jover savo straipsnyje apie LTE saugumo protokolų spragas nagrinėja galimybes išnaudoti nešifruotų paketų apsikeitimą tarp judriosios stoties ir eNodeB [11]. Savo įžvalgų pagrindimui Roger atliko ir praktinius bandymus panaudodamas openLTE programinę įrangą ir programiškai valdomą radijo įrangą.

Nico Golde su kolegomis praktiškai patvirtino, kad išnaudojant femtocelių, kaip saugių įrenginių, pozicionavimą bendroje tinklo struktūroje bei galimybę joms tarpusavyje bendrauti per

VPN, galima ne tik perimti vartotojų informaciją bet ir apsimesti jais tinkle ar sutrikdyti paslaugų teikimą femtocelių tinkle [12].

Mokslininkai susirūpinę vartotojų saugumu atlieka tyrimus ir ieško būdų, kaip apsisaugoti nuo mobiliojo ryšio blokavimo ar IMSI gaudyklių atakų. Adrian Dabrowski ir jo kolegos išskyrė pagrindinius IMSI gaudyklių aptikimo požymius ir pateikė pasiūlymus, pagal kuriuos galima sukurti prietaisą gebantį aptikti IMSI gaudykles esančias jo veikimo zonoje – IMSI gaudyklės gaudyklę [13]. Bryan Harmat su kolegomis atliko tyrimą ir pateikė pasiūlymų, kaip būtų galima patobulinti GSM saugumo procedūras, papildant jas naujais saugumą užtikrinančiais algoritmais bei funkcijomis. Vienas iš siūlymų yra naudoti laikiną raktą, kurį buvimo vietos registras (HLR) išduotų lankytojo registrui (VLR) judriosios stoties autentikavimui atlikti [14]. Kita mokslininkų komanda siūlo tinklo procedūrose nebenaudoti IMSI kodų, o juos pakeisti kintančiais pseudonimais, kuriuos žinotų tik abonento mobiliojo ryšio tiekėjas ir SIM modulis [15].

2. RADIJO BANGŲ SKLIDIMO MODELIŲ APŽVALGA

Radijo bangoms sklindant iš siųstuvo į imtuvą, jų signalo galia slopsta. Taip nutinka dėl įvairių kliūčių, kurios būna bangos sklidimo kelyje. Tai gali būti atmosferos poveikis, medžiai, pastatai, automobiliai ir pan. Projektuojant bet kokią radijo ryšio sistemą, būtina įvertinti kokiomis sąlygomis sklis radijo bangos ir apskaičiuoti kokio dydžio nuostolius jos patirs. Tam naudojami radijo bangų sklidimo modeliai. Tolimesniuose poskyriuose pateikiami populiariausi radijo bangų sklidimo lauke, į pastatus bei patalpose modeliai.

Toliau pateikiami koeficientai, kurie bus naudojami aprašant bangų sklidimo modelius (žr. 2.1 pav.) [16, p. 163]:

h_m – judriosios stoties antenos aukštis [m], dažniausiai naudojama reikšmė – 1,5 m;

d_m – atstumas tarp mobilios stoties ir artimiausio pastato [m];

h_0 – vidutinis pastatų aukštis [m];

h_b – bazinės stoties antenos aukštis [m];

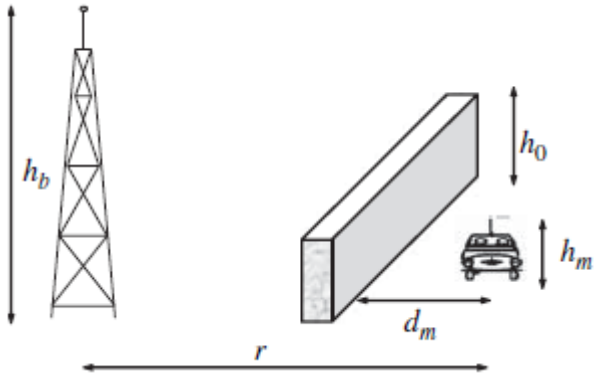
r – ortodrominis atstumas tarp bazinės stoties ir mobilios stoties [m];

$R = r \times 10^{-3}$ – ortodrominis atstumas tarp bazinės stoties ir judriosios stoties [km];

f – nešlio dažnis [Hz];

f_c – nešlio dažnis [MHz];

λ –bangos ilgis [m].



2.1 pav. Radijo bangų sklidimo modelių parametrų vizualizacija [16, p. 164]

2.1. Radijo bangų sklidimo lauke modeliai

Didžiausią radijo bangos sklidimo kelio atstumą dažniausiai sudaro jos sklidimas lauke. Tolimesniuose punktuose aprašomi populiariausi radijo bangų sklidimo lauke modeliai.

2.1.1. Laisvosios erdvės modelis

Laisvosios erdvės modelis yra pats paprasčiausias radijo bangų sklidimo modelis, nes jame neatsižvelgiama į jokias fizines kliūtis esančias tarp siųstuvo ir imtuvo [17]. Bangų sklidimo nuostoliai laisvojoje erdvėje yra apskaičiuojame pagal Frii lygtį [18, p. 67]:

$$L = G_T G_R \left(\frac{\lambda}{4\pi r}\right)^2. \tag{2.1}$$

Čia

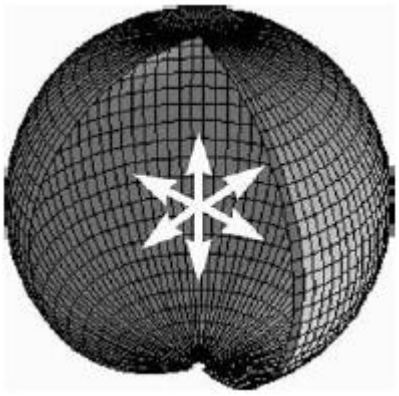
G_T – siųstuvo antenos stiprinimas;

G_R – imtuvo antenos stiprinimas;

r – atstumas tarp siųstuvo ir imtuvo antenų;

λ – bangos ilgis.

Ji gali būti vizualizuojama kaip sferinės galios sklidimas 1 m spindulio sferos, kurios centras sutampa su antenos pozicija, paviršiumi (žiūrėti 2.2 pav.) [16, p. 97].



2.2 pav. Izotropinės spinduliuotės vizualizacija [16, p. 97]

Kadangi spinduliavimo galia sklinda sferos paviršiumi, kuris didėja r^2, tai fiksuotos apertūros imtuvo antena priima r^2 mažesnės galios bangas.

2.1 formulė gali būti pertvarkyta, taip kad išreikštų bangos slopimą laisvojoje erdvėje:

$$L_F = \left(\frac{4\pi r}{\lambda}\right)^2 = \left(\frac{4\pi r f}{c}\right)^2. \tag{2.2}$$

Slopimą laisvojoje erdvėje išreiškus decibelais, dažnį megahercais, o atstumą kilometrais, gaunamas toks matematinis modelis:

$$L_{F(dB)} = 32{,}4 + 20\log R_{km} + 20\log f_{MHz}. \quad (2.3)$$

Taigi, padvigubėjus dažniui arba atstumui, slopimas laisvojoje erdvėje padidėja 6 dB arba 20 dB kiekvienai dažnio ar atstumo dešimčiai.

Tik anomaliomis sąlygomis bangos slopimas gali būti mažesnis nei slopimas laisvojoje erdvėje. Taip gali nutikti, jei banga sklinda apribota erdve, pavyzdžiui bangolaidžiu.

2.1.2. Okumura–Hata modelis

Okumura modelis paremtas empiriniais matavimais 200 MHz – 2 GHz dažnių diapazone, kurie dar 1968 m. buvo atlikti Tokijo mieste. Prognozavimas buvo vykdomas remiantis atliktų skaičiavimų grafikais. 1980 m. Hata šiuos duomenis apibendrino ir iš jų išvedė matematinį modelį. Šių dviejų darbų nuoseklumas lėmė tai, kad Okumura-Hata modelis yra vienas populiariausių ir dažnai laikomas etalonu, su kuriuo lyginami nauji modeliai. Šio modelio naudojimą tankiai apgyvendintose vietovėse standartizavo ITU organizacija [16, p. 167].

Okumura-Hata modelį sudaro trys dalys skirtos naudoti skirtingose vietovėse:

- atviroms vietovėms, kuriose nėra aukštų medžių ar pastatų ir yra tiesioginis matomumas 300 – 400 m. į priekį;
- priemiesčių vietovėms, kuriose yra netankiai išsidėsčiusių medžių ar pastatų bei nedaug kitų, judriąsias stotis užstojančių, kliūčių;
- miesto vietovėms, kurioms priskiriami miestai bei didmiesčiai su aukštais pastatais, namais su dviem ar daugiau aukštų ir aukštais vešliais medžiais.

Okumura miesto vietoves naudojo kaip pagrindą ir kitoms vietovėms pritaikė įvesdamas atitinkamas korekcijas modeliuose. Tai buvo logiškas sprendimas, nes miesto tipo vietovės būna panašios, su įvairių tipų kliūtimis, kurių dažnai nebūna kitų tipų vietovėse.

Signalo slopimo prognozavimas atliekamas naudojant tokias Hata aproksimacijas:

$$\begin{aligned} &\text{miesto vietovėse} && L_{dB} = A + B * \log(R) - E; \\ &\text{priemiesčių vietovėse} && L_{dB} = A + B * \log(R) - C; \\ &\text{atvirose vietovėse} && L_{dB} = A + B * \log(R) - D; \end{aligned} \tag{2.4}$$

Čia

$$\begin{aligned} &A = 69{,}55 + 26{,}16 * \log(f_c) - 13{,}82 * \log(h_b); \\ &B = 44{,}9 - 6{,}55 * \log(h_b); \\ &C = 2(\log(f_c/28))^2 + 5{,}4; \\ &D = 4{,}78(\log(f_c))^2 - 18{,}33 * \log(f_c) + 40{,}94; \\ &E = 3{,}2(\log(11{,}75h_m))^2 - 4{,}97 \text{ skirta didmiesčiams, kai } f_c \geq 300 \text{ MHz}; \\ &E = 8{,}29(\log(1{,}54h_m))^2 - 1{,}1 \text{ skirta didmiesčiams, kai } f_c < 300 \text{ MHz}; \\ &E = (1{,}1 * \log(f_c) - 0{,}7)h_m - (1{,}56 * \log(f_c) - 0{,}8) \text{ skirta vidutinio} \end{aligned} \tag{2.5}$$

dydžio ir mažiems miestams.

Modelis teisingas, kai 150 MHz ≤ f_c ≤ 1500 MHz, 30 m ≤ h_b ≤ 200 m, 1 m < h_m < 10 m ir R > 1 km. Signalo slopimo eksponentė lygi *B*/10 (šiek tiek mažiau nei 4), ji yra atvirkščiai proporcinga bazinės stoties antenos aukščiui. Matavimai rodo, kad šis faktorius taip pat priklauso nuo atstumo.

Bazinės stoties antenos aukštis h_b apibrėžiamas kaip aukštis virš vidutinio žemės lygio 3 – 10 km atstumu nuo bazinės stoties. Aukščio stiprinimo koeficientas kinta nuo 6 dB per oktavą iki 9 dB per oktavą, kai aukštis padidėja nuo 30 m iki 1 km.

Okumura nustatė, kad mobiliosios stoties antenos aukščio stiprinimas yra 3 dB per oktavą, kai h_m < 3 m ir 8 dB per oktavą esant didesniam aukščiui. Šis koeficientas dalinai priklauso ir nuo miesto tankumo, dėl pastatų aukščio įtakos bangos sklidimo kampui ir signalo praradimo dėl šešėlio efekto. Miestų vietovės yra skirstomos į didmiesčius ir vidutinio dydžio arba mažus miestus. Didmiesčiui priskiriama vietovė, kurioje vidutinis pastatų aukštis viršija 15 m. [16, p. 167].

2.1.3. COST 231–Hata modelis

Okumura-Hata modelis buvo praplėstas 1500 MHz < f_c < 2000 MHz dažnių ruožo skaičiavimams vidutinio dydžio ir mažuose miestuose [16, p. 169]:

$$L_{dB} = F + B * \log(R) - E + G. \tag{2.6}$$

Čia

$$F = 46{,}3 + 33{,}9 * \log(f_c) - 13{,}82 * \log(h_b)\,; \tag{2.7}$$

E apibrėžta vidutinio dydžio ir mažiems miestams skirtoje 2.5 formulėje;

$$G = \begin{cases} 0\ \text{dB} \\ 3\ \text{dB} \end{cases} \quad \begin{matrix} \text{mažiems miestams ir priemiesčiams} \\ \text{tankiai apgyvendintoms miestų vietovėms} \end{matrix} \tag{2.8}$$

2.1.4. SUI modelis

SUI (angl. *Stanford University Interim*) modelis sukurtas Stanfordo universitete. Jis naudojamas prognozuojant 1900 MHz ir aukštesnių dažnių radijo bangų sklidimo nuostolius netiesioginio matomumo aplinkose. Yra trys šio modelio modifikacijos, kurios naudojamos skirtingų tipų (A, B ir C) vietovėse. A tipo vietovėse yra didžiausias signalo slopimas, tai gali būti tankiai apgyvendintos vietos. B tipo vietovėse signalo slopimas yra vidutinis, tai gali būti priemiesčiai. C tipo vietovėse signalo slopimas yra pats mažiausias, tai gali būti kaimo vietovės arba lygumos. 2.1 lentelėje pateikiami SUI modelyje naudojamų parametrų reikšmės, kurios kinta priklausomai nuo vietovės [19].

Slopinimas apskaičiuojamas pagal:

$$L = 10\gamma \log\left(\frac{d}{d_0}\right) + X_f + X_h + s. \tag{2.9}$$

Čia

d_0 – atstumo etalonas lygus 100 m;

A – laisvos erdvės slopinimas d_0 atstumu [dB];

γ – nuostolių eksponentė priklausanti nuo bazinės stoties aukščio;

d – atstumas tarp stočių;

X_f – slopinimas dėl dažnio pataisos [dB];

X_h – slopinimas dėl aukščio pataisos [dB];

s – šešėlinimo standartinė deviacija.

Laisvosios erdvės slopinimas etaloniniu atstumu apskaičiuojamas pagal:

$$A = 20 \log\left(\frac{4\pi d_0}{\lambda}\right). \tag{2.10}$$

γ faktorius – tai nuostolių eksponentė, kuri priklauso nuo bazinės stoties aukščio ir naudojama vietovės, kurioje prognozuojami radijo bangų sklidimo nuostoliai, savybių įvertinimui. Apskaičiuojama pagal:

$$\gamma = \left(a - bh_b \frac{c}{h_b}\right). \tag{2.11}$$

Čia *a, b, c* – empiriškai nustatyti koeficientai (žr. 2.1 lentelę).

2.1 lentelė. SUI modelio parametrai [19]

Modelio parametrai	Vietovės tipas A	Vietovės tipas B	Vietovės tipas C
a	4,6	4	3,6
b	0,0075	0,0065	0,005
c	12,6	17,1	20

Dažnio ir aukščio slopinimo pataisų koeficientai apskaičiuojami atitinkamai:

$$X_f = 6log\left(\frac{f_c}{2000}\right), \tag{2.12}$$

$$X_h = \begin{cases} -10{,}8\log\left(\frac{h_m}{2}\right) & A \text{ arba } B \text{ vietovėms} \\ -20\log\left(\frac{h_m}{2}\right) & C \text{ vietovei} \end{cases} \tag{2.13}$$

2.2. Radijo bangų sklidimo į pastatus modeliai

Mobiliojo ryšio vartotojai paslaugomis naudojasi ne tik lauke, bet ir patalpose (namuose, biuruose, restoranuose ir pan.), todėl projektuojant blokavimo sistemą būtina įvertinti radijo bangų sklidimo nuostolius joms sklindant iš lauko į pastatus. Tolimesniuose punktuose pateikiami populiariausi radijo bangų sklidimo modeliai skirti tokiems nuostoliams apskaičiuoti.

2.2.1. COST231 tiesioginio matomumo modelis

Šis pusiau empirinis modelis su geometriniu pagrindimu (žr. 2.3 pav.) yra siūlomas tais atvejais, kai pastato fasadas yra siųstuvo antenos tiesioginio matomumo zonoje. 2.3 paveiksle esančiame brėžinyje parametras r_e yra tiesinis atstumas tarp siųstuvo antenos ir pasirinkto pastato sienos taško. Kadangi šis modelis naudojamas esant nedideliems atstumams, labai svarbu nurodyti tikslų bangos sklidimo kelio ilgį pagal tris dimensijas, o ne kelio ilgį matuojant pagal žemę. Bangos

sklidimo nuostoliai gali pastebimai kisti, nes bangos kritimo kampas, $\theta = \cos^{-1}(r_p/r_e)$ būna įvairus [16, p. 294].

Bendri bangų sklidimo nuostoliai apskaičiuojami pagal:

$$L_T = L_F + L_e + L_g(1 - cos\theta)^2 + \max(L_1, L_2). \quad (2.14)$$

Čia

L_F – viso bangos sklidimo kelio laisvojoje erdvėje ($r_i + r_e$) nuostoliai;

L_e – bangos sklidimo per išorinę pastato sieną nuostoliai, kai $\theta = 0°$;

L_g – papildomi bangos sklidimo pagal išorinę pastato sieną nuostoliai, kai $\theta = 90°$;

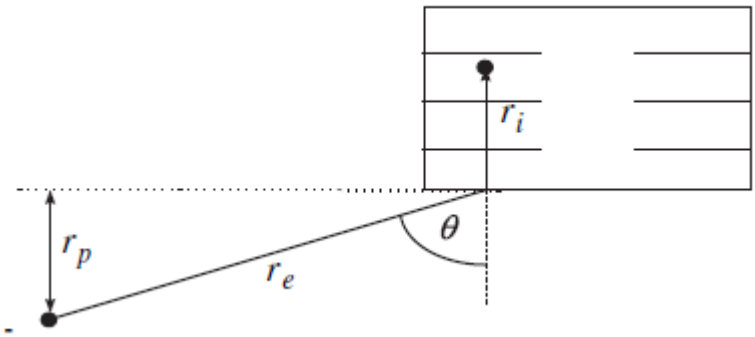
$$L_1 = n_w L_i;\ L_2 = \alpha(r_i - 2)(1 - cos\theta)^2; \quad (2.15)$$

Čia

n_w – sienų, kurias bangos sklidimo trajektorija r_i kerta pastato viduje, skaičius;

L_i – nuostoliai kirtus vidinę sieną;

α – specifinis slopinimas bangai sklindant laisvoje erdvėje pastato viduje, [dBm^{-1}].



2.3 pav. COST231 tiesioginio matomumo modelio geometrinis pagrindimas [16, p. 295]

COST 231 tiesioginio matomumo modelis galioja, kai atstumai neviršija 500 m.

2.2 lentelėje pateikiami 900-1800 MHz dažnių diapazonui rekomenduojami parametrai. Jie atitinka realius matavimus ir apima tipinių baldų įtaką.

2.2 lentelė. COST 231 tiesioginio matomumo modelio parametrai [16, p. 296]

Parametras	Medžiaga	Apytikslė reikšmė
L_e arba L_i [dBm^{-1}]	Medinės sienos	4
	Betonas su nemetalizuotais langais	7
	Betonas be langų	10-20
L_e [dB]	Nenurodyta	20
α [dBm^{-1}]	Nenurodyta	0,6

2.2.2. COST231 netiesioginio matomumo modelis

Šis modelis susieja signalo nuostolius pastato viduje, kai bangas skleidžia siųstuvas esantis pastato išorėje, su nuostoliais esančiais lauke, dviejų metrų aukštyje, toje pastato pusėje, kuri yra artimiausia atskaitos taškui. Bangų sklidimo nuostoliai apskaičiuojami pagal [16, p. 296]:

$$L_T = L_{out} + L_e + L_{ge} + \max(L_1, L_3) - G_{fh}. \quad (2.16)$$

Čia

$L_3 = \alpha r_i$;

r_i, α, L_e ir L_1 atitinka COST231 tiesioginio matomumo modelyje naudojamus parametrus (žr. 2.2.1 punktą), o pastato aukščio stiprinimas G_{fh} lygus:

$$G_{fh} = \begin{cases} nG_n \\ hG_h \end{cases}. \quad (2.17)$$

Čia

h – pastato vieno aukšto aukštis virš atskaitos aukščio lauke [m];

n – pastato aukšto numeris.

Šešėlio efektas prognozuojamas su normaliniu logaritminiu pasiskirstymu ir 4-6 dB nuokrypiais priklausomai nuo vietos. Kitų parametrų reikšmės pateikiamos 2.3 lentelėje.

2.3 lentelė. COST 231 netiesioginio matomumo modelio parametrai [16, p. 297]

Parametrai	Apytikslės reikšmės
L_{ge} [dB] kai dažnis 900 MHz	4
L_{ge} [dB] kai dažnis 1800 MHz	6
G_n [dB aukštui] kai dažnis 900/1800 MHz	1,5-2 normaliems pastatams 4-7 pastatams, kurių aukštai aukštesni nei 4 m

Tiek tiesioginio, tiek netiesioginio matomumo COST231 bangų sklidimo modeliuose nuostolių reikšmė labiausiai priklauso nuo bangos sklidimo per vieną išorinę sieną nuostolių. Tikslesnius rezultatus galima gauti sudedant visų sienų, pro kurias sklinda banga, slopinimą.

2.3. Radijo bangų sklidimo patalpose modeliai

Siekiant blokuoti mobilųjį ryšį patalpose, galimi du blokuojančios įrangos įrengimo vietos variantai: įrangą statyti lauke ir iš lauko apspinduliuoti pastatą arba ją įrengti pastato patalpose. Abiem atvejais reikia įvertinti radijo bangų sklidimo patalpose nuostolius. Tolimesniuose punktuose pateikiami populiariausi radijo bangų sklidimo patalpose modeliai.

2.3.1. Sienų ir aukštų faktoriaus modelis

Keenan ir Motley sienų ir aukštų faktoriaus modelis yra paremtas bangų sklidimo laisvojoje erdvėje modeliu. Pagal šį modelį, bangų sklidimo nuostolius patalpose sudaro nuostoliai laisvojoje erdvėje ir papildomi nuostoliai susiję su pastato aukštų n_f ir sienų, kurias kerta tiesi linija r nubrėžta tarp siųstuvo ir imtuvo, skaičiumi n_w [17]. Bangos sklidimo nuostoliai apskaičiuojami pagal [16, p. 283]:

$$L = L_1 + 20\log r + n_f a_f + n_w a_w. \tag{2.18}$$

Čia

a_f – vieno pastato aukšto slopinimas [dB];

a_w – vienos pastato sienos slopinimas [dB];

L_1 – slopinimas, kai r = 1 m.

2.3.2. COST231 daugelio sienų modelis

Šis bangų sklidimo modelis yra paremtas sienų ir aukštų faktoriaus modeliu. Jame teigiama, kad bangų sklidimo nuostoliai tiesiogiai proporcingi sienų, kurias kirto bangos, skaičiui ir netiesiškai priklauso nuo aukštų, kuriuos kirto bangos, skaičiaus [16, p. 285]:

$$L_T = L_F + L_c + \sum_{i=1}^{W} L_{wi} n_{wi} + L_f n_f{}^{((n_f+2)/(n_f+1)-b)}. \tag{2.19}$$

Čia

L_F – nuostoliai laisvojoje erdvėje tiesia trajektorija tarp siųstuvo ir imtuvo;

n_{wi} – sienų skaičius, kurias kerta tiesioginė i tipo trajektorija;

W – skirtingų sienų tipų skaičius;

L_{wi} – i tipo sienos slopinimas;

n_f – pastato aukštų, kuriuos kerta bangų sklidimo trajektorija, skaičius;

b ir L_c – empiriškai gautos konstantos;

L_f – vieno pastato aukšto slopinimas.

3. MOBILIOJO RYŠIO TINKLAS

Mobiliojo signalo fiksavimo ir perėmimo metodai buvo pradėti plėtoti GSM tinkle. Toliau aprašoma GSM tinklo struktūra ir jo veikimo pricipai. Taip pat detalizuojami GSM, UMTS ir LTE technologijų tinkluose vykdomi autentifikavimo bei šifravimo procesai. IMSI gaudyklės veikimo principas išnaudojant GSM tinklo saugos trūkumus nagrinėjamas 4.2 poskyryje.

3.1. Tinklo struktūra

Supaprastintą GSM tinklo modelį sudaro 4 pagrindiniai tinklo komponentai (žiūrėti 3.1 pav. Supaprastinta GSM tinklo architektūra) [20]:

1) Mobili stotis (MS)

Mobili stotis – tai mobilusis telefonas ar kitas mobilus įrenginys, į kurį dedama SIM kortelė. Kiekviena SIM kortelė tinkle identifikuojama pagal unikalų IMSI kodą, kurį sudaro 15 skaitmenų, suskirstytų į šiuos komponentus:

- 3 skaitmenų šalies kodą (MCC);
- 2 arba 3 skaitmenų tinklo kodą (MNC);
- iš visų likusių skaitmenų sudarytą abonento identifikacijos numerį (MSIN).

Mobilusis įrenginys identifikuojamas pagal unikalų IMEI kodą. Pagal jį identifikuojami pavogti telefonai arba įrenginys „pririšamas“ prie operatoriaus tinklo. SIM kortelėje taip pat saugomi 3 papildomi saugumo dėmenys:

- autentifikavimo algoritmas A3;
- rakto generavimo algoritmas A8;
- 128 bitų ilgio ilgalaikis saugos raktas K_i, kuris naudojamas abiejuose prieš tai išvardintuose algoritmuose ir saugomas GSM tinkle.

2) Bazinė stotis (BS)

Bazinė stotis tiesiogiai komunikuoja su mobilia stotimi. Kiekviena bazinė stotis valdo vieną mobiliojo tinklo celę. Celės dydis gali siekti nuo kelių šimtų metrų iki keliolikos kilometrų, priklausomai nuo geografinės vietovės, reljefo bei pastatų ar medžių. Tankiai apgyvendintose miesto vietovėse kiekvienai bazinei stočiai reikia daugiau celių, kad ji galėtų aptarnauti daugiau priskirto dažnių diapazono vartotojų.

Bazinė stotis taip pat atlieka skambučio ir kitos perduodamos informacijos duomenų šifravimą bei dešifravimą.

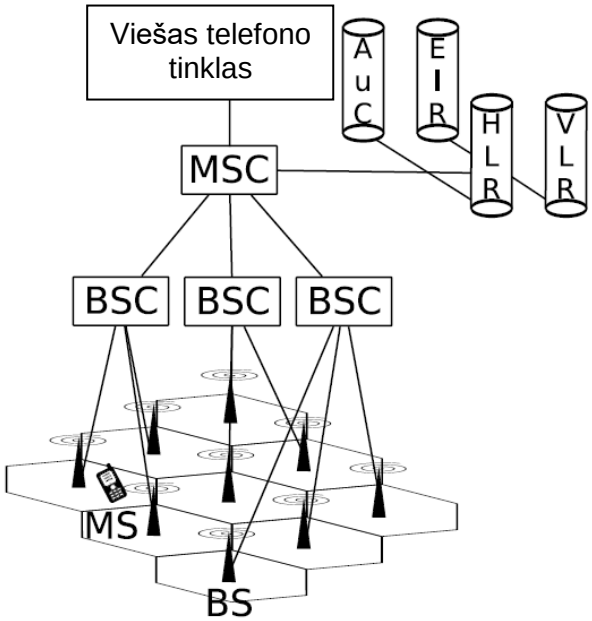
3) Bazinės stoties valdiklis (BSC)

Kiekvienas bazinės stoties kontroleris valdo kelias bazines stotis. Ryšio perkeltį, kai mobilusis įrenginys juda nuo vienos celės prie kitos, atlieka bazinės stoties valdiklis arba judriojo ryšio komutavimo centras.

4) Judriojo ryšio komutavimo centras (MSC)

Judriojo ryšio komutavimo centras GSM tinkle atlieka pagrindinį duomenų valdymą. Yra 4 duomenų bazės, kuriomis jis grindžiamas:

- buvimo registras (HLR). Kiekvienas GSM tinklas turi vienintelį HLR, kuriame saugoma visų tinklo abonentų asmeninė informacija, įskaitant ir IMSI kodą;
- lankytojo registras (VLR). Kiekvienas MSC turi jam skirtą VLR, kuriame saugoma asmeninė tinklo abonentų informacija, kurie yra MSC valdomoje vietovėje;
- autentifikavimo centras (AuC). Jame saugoma visų tinklo abonentų prieigos informacija – visų SIM kortelių ilgalaikiai saugumo kodai K_i.
- įrangos identifikavimo registras (EIR). Jame saugomi uždraustų ar pavogtų mobiliųjų įrenginių IMEI kodai, kuriems uždrausta prisijungti prie tinklo.



3.1 pav. Supaprastinta GSM tinklo architektūra [20]

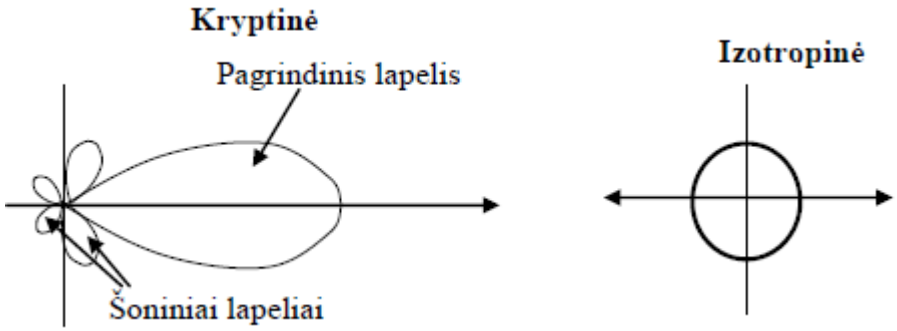
3.2. Antena

Vienas iš svarbiausių bet kokios telekomunikacijų sistemos komponentų yra antena. Ji skirta į atvirą erdvę spinduliuoti elektromagnetines bangas, kurios sukuriamos panaudojant energijos šaltinio tiekiamą elektros srovę, arba jas priimti bei perduoti į imtuvą. Dažniausiai antenos būna sudarytos iš vielos ir metalinių strypų prijungtų prie siųstuvo ar imtuvo. Jų dydis priklauso nuo to, kokio bangos ilgio bei dažnio bangoms jos skirtos [21, p. 4].

Antenos veikimo charakteristikas apibūdina jos pagrindiniai parametrai. Tolesniuose poskyriuose aprašomi šie parametrai: kryptingumas, stiprinimas, spinduliavimo diagrama bei poliarizacija.

3.2.1. Kryptingumas

Priklausomai nuo antenos konstrukcijos, bangos atmosferoje gali sklisti visomis kryptimis (izotropinė antena) arba tam tikra išreikšta kryptimi (kryptinė antena). 3.2 paveiksle pavaizduotos kryptinės ir izotropinės antenų kryptingumo diagramos. Kryptinės antenos kryptingumo diagrama turi pagrindinį ir šoninius lapelius.



3.2 pav. Kryptinės ir izotropinės antenų kryptingumo diagramos [22, p. 16]

Antenos kryptingumo koeficientas D (angl. *directivity*) yra susietas su antenos geometrinėmis charakteristikomis, kurios sąlygoja jos spinduliavimo diagramą. Kryptingumas yra lygus izotropinės ir kryptinės antenų spinduliuojamų galių, priėmimo taške sukuriančių vienodą lauko stiprumą, santykiui. Kryptingumą galima apskaičiuoti į abi antenas paduodant vienodas įėjimo galias. Tada antenos kryptingumas gali būti apibrėžiamas kaip energijos intensyvumo maksimalia antenos spinduliavimo kryptimi santykis su vidutiniu intensyvumu arba su izotropinio spinduolio intensyvumu [23]:

$$D = \frac{U_m(\theta, \varphi)}{U_0}. \tag{3.1}$$

Čia

U_m – maksimalus spinduliavimo intensyvumas [W/rad^2];

U_0 – vidutinis spinduliavimo intensyvumas [W/rad^2].

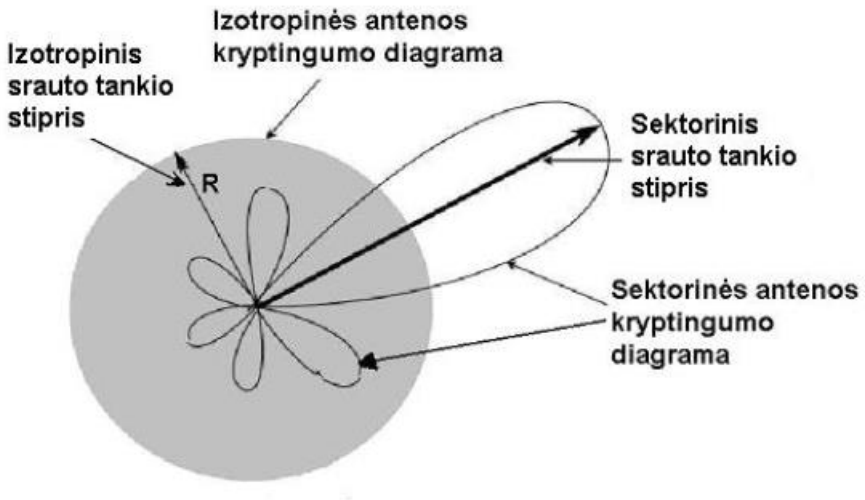
Vidutinis spinduliavimo intensyvumas arba izotropinio spinduolio intensyvumas apibrėžiamas taip:

$$U_0 = \frac{P}{4\pi}. \tag{3.2}$$

Čia P – išspinduliuojama antenos galia.

Kryptingumas bendru atveju gali būti nusakomas ir kaip elektromagnetinės bangos galios tankio maksimalia spinduliavimo kryptimi santykis su vidutiniu galios tankiu visomis kryptimis (žr. 3.3 pav.) [23], [24]:

$$D = \frac{P_{Sek}}{P_{Iz}}. \tag{3.3}$$



3.3 pav. Sektorinės ir izotropinės antenų kryptingumo diagramos [24]

3.2.2. Stiprinimas

Kryptingumo koeficientas D neįvertina nuostolių antenoje, todėl praktikoje yra naudojamas antenos stiprinimo koeficientas G (angl. *gain*), kuris yra susietas su kryptingumu D tokiu sąryšiu [23]:

$$G = \eta D. \tag{3.4}$$

Čia η – antenos naudingumo koeficientas.

Antenos naudingumo koeficientas yra lygus spinduliuojamos ir visos galios, siunčiamos į anteną, santykiui [23]:

$$\eta = \frac{P_r}{P_A} = \frac{0{,}5I_m^2 R_r}{0{,}5I_m^2 R_A} = \frac{R_r}{R_A} = \frac{R_r}{R_r + R_N}. \quad (3.5)$$

Čia

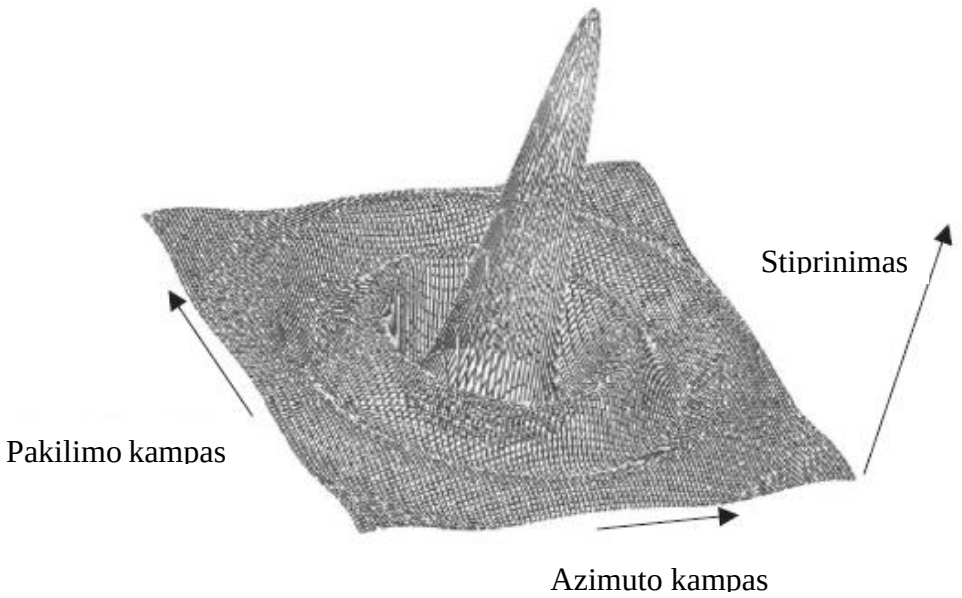
R_r – antenos spinduliavimo varža;

R_N – antenos nuostolių varža.

Taigi, antenos stiprinimo koeficientas nurodo, kiek kartų galima sumažinti į kryptinę anteną siunčiamą galią, palyginus su galia siunčiama į izotropinę anteną, norint gauti vienodą elektrinio lauko stiprumą priėmimo taške. Antenos stiprinimas didėja mažėjant antenos spinduliavimo kampų dydžiams.

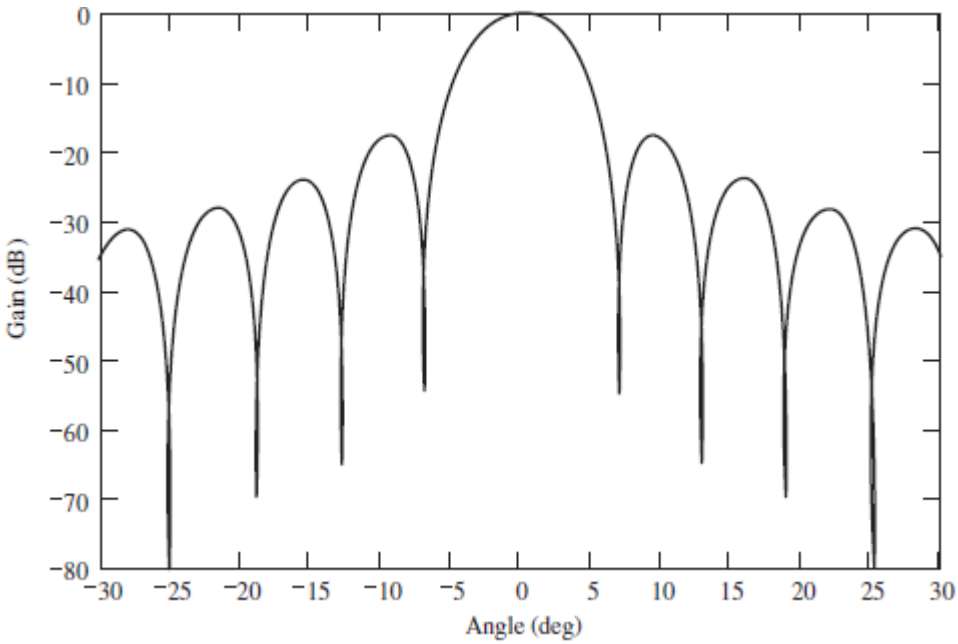
3.2.3. Spinduliavimo diagrama

Antenos spinduliavimo diagrama yra grafinis stiprinimo vaizdavimas kampo atžvilgiu, dažniausiai išreiškiamas decibelais. Tai yra dvimatė diagrama, azimuto ir pakilimo kampų funkcija. Apskritiminės apertūros antenos spinduliavimo diagrama pavaizduota 3.4 paveiksle.



3.4 pav. Trimatis dvimatės antenos spinduliavimo diagramos vaizdas [18]

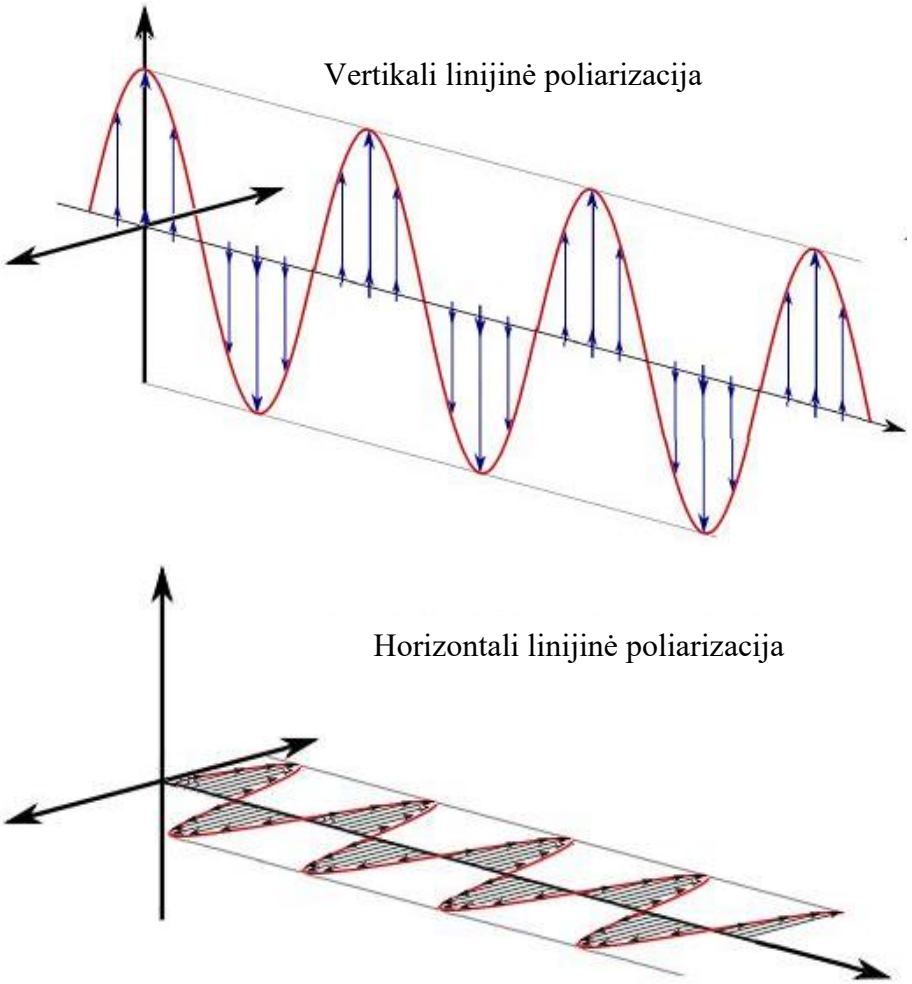
Praktikoje dažniausiai naudojami principinės spinduliavimo diagramos pjūviai (žr. 3.5 pav.). Šie pjūviai apibūdina tolimojo lauko diagramas, kuriose stiprinimas ir kryptingumas yra tik reljefo kampų funkcijos ir visai nepriklauso nuo atstumo [18].



3.5 pav. Vienmatis tipinės antenos spinduliavimo diagramos (normalizuotas stiprinimas) vaizdas [18]

3.2.4. Poliarizacija

Antenos poliarizacija tai procesas, kurio metu spinduliuojamos ar priimamos tam tikros poliarizacijos elektromagnetinės bangos. Antena, kuri skirta priimti vertikaliosios poliarizacijos signalą, gali priimti ir horizontaliosios poliarizacijos signalą arba atvirkščiai, tačiau tai bus atliekama su labai dideliu signalo praradimu. Vertikalios ir horizontalios poliarizacijos bangų pavyzdžiai patekti 3.6 paveiksle. Mobiliojo ryšio bazinėse stotyse dažniausiai naudojamos vertikalios poliarizacijos antenos. Vertikaliai poliarizuoto signalo sklidimas yra geresnis nei horizontaliai poliarizuoto, nes aplinkoje yra gerokai daugiau vertikalių objektų, nuo kurių bangos gali atsispindėti. Taip pat vertikaliosios poliarizacijos antenų gamyba yra paprastesnė, o tai lemia ir mažesnę kainą [24].



3.6 pav. Vertikalios ir horizontalios poliarizacijų elektromagnetinių bangų pavyzdžiai

3.3. Celės pasirinkimo sąlygos ir kriterijai

Judrioji stotis turi nuolat palaikyti geriausią įmanoma ryšį su bazine stotimi, pasirenkant geriausią celę prisijungimui. Ji, būdama prisijungusi prie savo mobiliojo tinklo operatoriaus celės, gali pradėti ieškoti kitos celės prisijungimui, jei [25]:

- signalo slopinimas pasidarė per didelis korektiškam veikimui;
- nepavyksta žemynkryptis signalizavimas;
- dabartinė celė buvo užblokuota;
- dabartinėje registracijos vietoje atsirado „geresnė“ celė (pagal naujos celės pasirinkimo kriterijus);

3.3.1. Celės pasirinkimo ir persirinkimo kriterijai

Judrioji stotis celę prisijungimui pasirenka pagal tolimesniuose punktuose aprašytus kriterijus.

3.3.1.1. GSM

Pirminiam celės pasirinkimui ir naujos celės atrankai judrioji stotis naudoja signalo slopinimo kriterijaus parametrą C1, kuris leidžia nuspręsti ar celė yra tinkama prisijungimui. C1 apibrėžiamas taip [26]:

$$C1 = (A - Max(B, 0)). \tag{3.6}$$

Čia

$$A = RLA\_C - RXLEV\_ACCESS\_MIN; \tag{3.7}$$

$$B = MS\_TXPWR\_MAX\_CCH - P. \tag{3.8}$$

3-ios klasės DCS 1800 judriajai stočiai:

$$B = MS\_TXPWR\_MAX\_CCH + POWER\ OFFSET - P. \tag{3.9}$$

Čia

RLA_C – priimtų signalų lygio vidutinė reikšmė;

RXLEV_ACCESS_MIN – minimalus operatoriaus nustatytas signalo lygis, leidžiantis judriajai stočiai prisijungti prie tinklo;

MS_TXPWR_MAX_CCH – maksimalus leidžiamas judriosios stoties siųstuvo galios lygis, kurį ji gali pasiekti jungdamasi prie tinklo;

POWER OFFSET – galios kompensacija, kuri skirta 3-ios klasės DCS 1800 judriajai stočiai naudoti su *MS_TXPWR_MAX_CCH* parametru;

P – maksimali judriosios stoties galia.

Visi parametrai išreiškiami decibelmetrais [dBm]. Signalo slopinimo kriterijus tenkinamas, jei C1 > 0.

Siekiant optimizuoti naujos celės pasirinkimą gali būti naudojami papildomi atrankos parametrai, kurios, kaip sistemos informaciją, siunčia kiekviena celė. Naujos celės pasirinkimo procese yra naudojamas celės pasirinkimo kriterijus C2, kuris priklauso nuo minėtų parametrų. Jis išreiškiamas taip:

$$C2 = C1 + CELL_{RESELECT_{OFFSET}} - TEMPORARY\ OFFSET * H(PENALTY\_TIME - T), \tag{3.10}$$

kai *PENALTY_TIME* <> 11111.

$$C2 = C1 - CELL\_RESELECT\_OFFSET, \tag{3.11}$$

kai *PENALTY_TIME* = 11111,

čia

gretimai celei:

$$H(x) = \begin{cases} 0, kai\ x\ <\ 0 \\ 1, kai\ x\ \geq\ 0 \end{cases} \quad (3.12)$$

celei prie kurios yra prisijungta:

$$H(x) = 0. \quad (3.13)$$

T - laikmatis naudojamas kiekvienai stipriausių operatorių sąraše esančiai celei. *T* turi būti pradėtas nuo nulio kai judrioji stotis įtraukia celę į sąrašą, nebent į sąrašą pridedama celė, prie kurios prieš tai buvo prisijungta. Tokiu atveju *T* turi būti suteikiama *PENALTY_TIME* reikšmė - tai reiškia pasibaigęs.

CELL_RESELECT_OFFSET – C2 naujos celės pasirinkimo kriterijaus kompensacija konkrečiai celei. Šis parametras gali būti taikomas skirtingų dažnių juostų celių prioretizavimui.

TEMPORARY_OFFSET – neigiama C2 parametro kompensacija taikoma PENALTY_TIME laiko intervalą nuo celės laikmačio T skaičiavimo pradžios.

PENALTY_TIME – tai yra trukmė, kurią taikoma *TEMPORARY_OFFSET* kompensacija. Kai judrioji stotis įtraukia celę į stipriausių sąrašą, paleidžiamas laikmatis, kuris baigiasi po *PENALTY_TIME* trukmės. Kai celė pašalinama iš sąrašo, jis paleidžiamas iš naujo. Visą laikmačio trukmę C2 turi neigiamą reikšmę. Tokiu būdu greitai judančios judriosios stotys nesirinks tokios celės.

CELL_RESELECT_OFFSET, TEMPORARY_OFFSET, PENALTY_TIME ir *CELL_BAR_QUALIFY* parametrai yra pasirinktinai transliuojami celės transliavimo valdymo kanalu. Jei jie netransliuojami, tuomet taikomos numatytosios reikšmės – *CELL_BAR_QUALIFY*=0 ir C2 = C1.

Šie parametrai naudojami užtikrinimui, kad judrioji stotis bus prisijungusi prie celės, kuri turi didžiausią tikimybę užtikrinti kokybišką aukštynkryptį ir žemynkryptį signalo perdavimą.

3.3.1.2. UMTS

Celės pasirinkimo kriterijus S tenkinamas, kai [27]:

FDD celėms:

$$S_{rxlev}\ >\ 0\ \ ir\ S_{qual}\ >\ 0. \quad (3.14)$$

TDD celėms:

$$S_{rxlev} > 0. \tag{3.15}$$

Čia

$$S_{qual} = Q_{qualmeas} - (Q_{qualmin} + Q_{qualminOffset}) - Q_{offsettemp}; \tag{3.16}$$

$$S_{rxlev} = Q_{rxlevmeas} - (Q_{rxlevmin} + Q_{rxlevminOffset}) - P_{compensation} - Q_{offsettemp}. \tag{3.17}$$

Čia

S_{qual} – celės pasirinkimo kokybės vertė [dB];

S_{rxlev} – celės pasirinkimo priimamo signalo lygio vertė [dB];

$Q_{offsettemp}$ – laikinai taikoma kompensacija [dB];

$Q_{qualmeas}$ – išmatuotos celės kokybės vertė [dB];

$Q_{qualmin}$ – minimalios reikalaujamos celės kokybės vertė [dB];

$Q_{qualminOffset} - Q_{qualmin}$, dėl periodinės didesnio prioriteto mobiliojo ryšio tiekėjo tinklo paieškos, taikoma kompensacija;

$Q_{rxlevmin}$ – minimalios reikalaujamos celės kokybės vertė [dBm];

$Q_{qualminOffset} - Q_{rxlevmin}$, dėl periodinės didesnio prioriteto mobiliojo ryšio tiekėjo tinklo paieškos, taikoma kompensacija;

$$P_{compensation} = max(UE\_TXPWR\_MAX\_RACH - P\_MAX, 0); \tag{3.18}$$

Čia

UE_TXPWR_MAX_RACH - maksimalus leidžiamas judriosios stoties siųstuvo galios lygis, kurį ji gali pasiekti jungdamasi prie tinklo [dBm];

P_MAX - maksimali judriosios stoties galia [dBm].

Dabartinės ir gretimos celių vertinimo kriterijai (atitinkamai R_s ir R_n) apibrėžiami taip:

$$R_s = Q_{meas,s} + Qhyst_s + Qoffmbms - Qoffset_{temp}; \tag{3.19}$$

$$R_n = Q_{meas,n} - Qoffset_{s,n} + Qoffmbms - TO_n * (1 - L_n) - Qoffset_{temp}. \tag{3.20}$$

Čia

$Q_{meas,s}$, $Q_{meas,n}$ – išmatuotos dabartinės ir kaimyninės celių kokybės vertės [dB];

$Qhyst_s$ – dabartinės celės histerezės vertė;

Qoffmbms – papildoma kompensacija pridedama celėms, kurios priklauso MBMS palankančiam tinklui;

$Qoffset_{temp}$ – papildoma kompensacija, laikinai naudojama FDD celėms, kai nepavyksta RRC sujungimas;

$Qoffset_{s,n}$ – kompensacija tarp dabartinės ir gretimos celių;

$$TO_n = TEMP\_OFFSET_n * W(PENALTY\_TIME_n - T_n); \quad (3.21)$$

$$L_n = \begin{cases} 0, kai\ HCS\_PRIO_n = HCS\_PRIO_s \\ 1, kai\ HCS\_PRIO_n <> HCS\_PRIO_s \end{cases} \quad (3.22)$$

$$W(x) = \begin{cases} 0, kai\ x < 0 \\ 1, kai\ x \geq 0 \end{cases} \quad (3.23)$$

Čia $TEMP\_OFFSET_n$ – *R* parametro kompensacija taikoma $PENALTY\_TIME_n$ laiko intervalą nuo celės laikmačio T_n skaičiavimo pradžios.

3.3.1.3. LTE

LTE technologijoje naudojami tokie patys celės pasirinkimo kriterijai (žiūrėti 3.14, 3.16, 3.17 formules), kaip ir UMTS technologijoje. Celės persirinkimo kriterijai apibrėžiami taip [28]:

$$R_s = Q_{meas,s} + Qhyst_s - Qoffset_{temp}; \quad (3.24)$$

$$R_n = Q_{meas,n} - Qoffset_{s,n} - Qoffset_{temp}. \quad (3.25)$$

3.4. Autentifikavimas ir šifravimas

Judriajai stočiai jungiantis prie bazinės stoties yra vykdomas autentifikavimo procesas, kurio metu nustatoma vartotojo (GSM, UMTS, LTE) bei tinklo (UMTS, LTE) tapatybė. Tolimesniuose punktuose detalizuojami GSM, UMTS bei LTE technologijų tinkluose vykdomos autentifikavimo procedūros bei duomenų šifravimo algoritmai.

3.4.1. GSM

Kai mobili stotis bando prisijungti prie tinklo, ji turi save autentifikuoti, nors bazinės stoties autentifikavimas nėra vykdomas. Ši procedūra parodyta 3.7 paveiksle.

Pirmiausia mobili stotis per bazinę stotį siunčia savo saugumo parametrus lankytojo registrui (VLR). Tai nurodo tinklui, kokius A5 šifravimo protokolus ji palaiko. Tada VLR mobiliai stočiai siunčia tapatybės užklausos komandą, kuri reikalauja mobilią stotį atsiųsti savo IMSI kodą. Kuomet žinomas mobilios stoties IMSI kodas, lankytojo registras (VLR) siunčia autentifikavimo parametrų užklausą buvimo registrui (HLR), kuri persiunčiama į autentifikavimo centrą (AuC). AuC pirmiausia sugeneruoja 128 bitų atsitiktinį numerį *RAND*. Tada remiantis *RAND* ir turimu ilgalaikiu saugos raktu K_i, kuris priklauso nurodytai SIM, apskaičiuoja 32 bitų patvirtinimo atsakymą (*SRES*):

$$SRES = A3(RAND, K_i), [VLR]. \quad (3.26)$$

AuC taip pat sugeneruoja 64 bitų sesijos raktą K_c, panaudojant A8 algoritmą:

$$K_c = A8(RAND), [VLR]. \quad (3.27)$$

Atsitiktinis numeris *RAND*, patvirtinimo atsakymas *SRES* ir serijos raktas K_c siunčiami atgal į VLR. VLR mobiliajai stočiai persiunčia tik *RAND*. Panaudojant ilgalaikį saugos raktą K_i, kuris saugomas SIM kortelėje, mobili stotis apskaičiuoja:

$$SRES' = A3(RAND, K_i), [\text{SIM}]. \quad (3.28)$$

Tuomet mobili stotis siunčia *SRES'* į VLR. Jei *SRES* ir *SRES'* nesutampa, autentifikavimo užklausa yra atmetama. Priešingu atveju, ji patvirtinama ir VLR mobiliajai stočiai priskiria laikiną mobiliojo ryšio tinklo vartotojo kodą (TMSI) ir nurodo, kurį A5 šifro režimą naudoti.

Galimi šifro režimai:

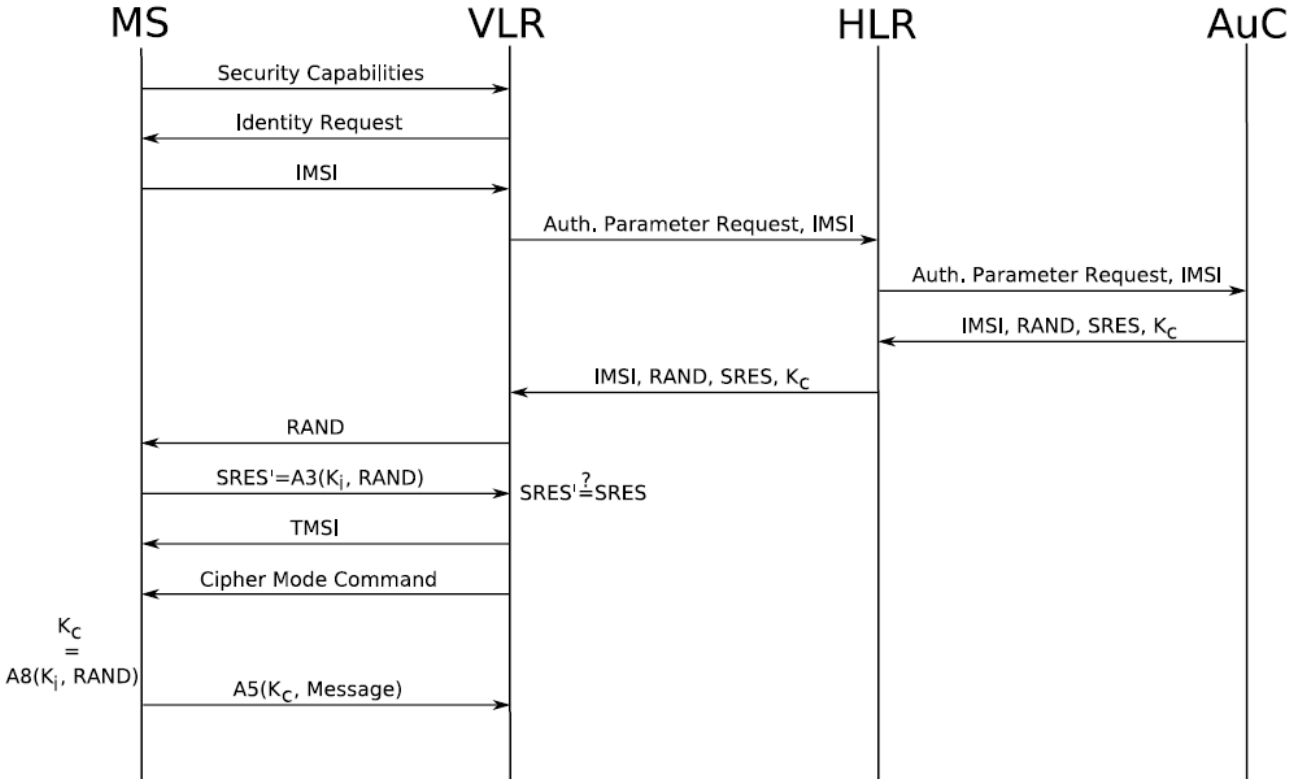
- A5/0 – jokio šifravimo;
- A5/1;
- A5/2;
- A5/3 – šifravimas paremtas KASUMI algoritmu.

TMSI kodas naudojamas didesniam saugumui užtikrinti, nes taip sumažimas IMSI kodo persiuntimų skaičius. Jis naudojamas tolimesniam bendravimui su VLR. Reikia pabrėžti, kad mobiliajai stočiai naudojant tarptinklinį ryšį (angl. *roaming*), kito tiekėjo tinklas neatpažins jos TMSI, todėl ji turės persiųsti savo IMSI kodą. Kito tiekėjo tinklas norėdamas identifikuoti vartotoją, kreipsis į mobiliosios stoties naudojamo tiekėjo tinklą tapatybės patvirtinimui ir tik tada išduos TMSI.

Jei pasirenkamas bet kuris, išskyrus A5/0, šifravimo režimas, mobili stotis naudodama A8 algoritmą pagal *RAND* numerį ir ilgalaikį saugos raktą K_i apskaičiuoja sesijos raktą K_c. Pasirinktas A5 algoritmas yra naudojamas šifruoti visus tolesnius ryšius tarp mobiliosios stoties ir bazinės stoties:

$$\text{ŠIFRAS}=A5(K_c, \text{PRANEŠIMAS}). \tag{3.29}$$

Sesijos raktas K_c naudojamas tol, kol būna inicijuojama nauja autentifikavimo užklausa. Naujos autentifikavimo užklausos inicijavimo atvejus kiekvienas operatoriaus nustato individualiai. Praktikoje tas pats sesijos raktas naudojamas ir tolimesniems skambučiams atlikti ar pranešimams išsiųsti [29].



3.7 pav. GSM tinkle naudojama autentifikavimo procedūra [20]

GSM tinklo saugumo spragos, kuriomis naudojantis veikia IMSI gaudyklės, yra IMSI kodo siuntimas bazinei stočiai ir vienpusis autentifikavimas, t. y. tik bazinė stotis reikalauja mobiliosios stoties autentifikuoti save, bet ne atvirkščiai.

3.4.2. UMTS

Kartu su UMTS tinklo sukūrimu buvo įdiegti saugumo patobulinimai. Svarbiausias iš jų – mobiliosios stotys atlieka tinklo, prie kurio jungiasi, autentifikavimą, taip siekiama apsisaugoti nuo prisijungimų prie netikrų bazinių stočių. Taip pat, UMTS tinklas vietoj A5/1 šifro naudoja saugesnį KASUMI blokinį šifrą.

UMTS sistemoje autentifikavimo mechanizmą sudaro trys nariai:

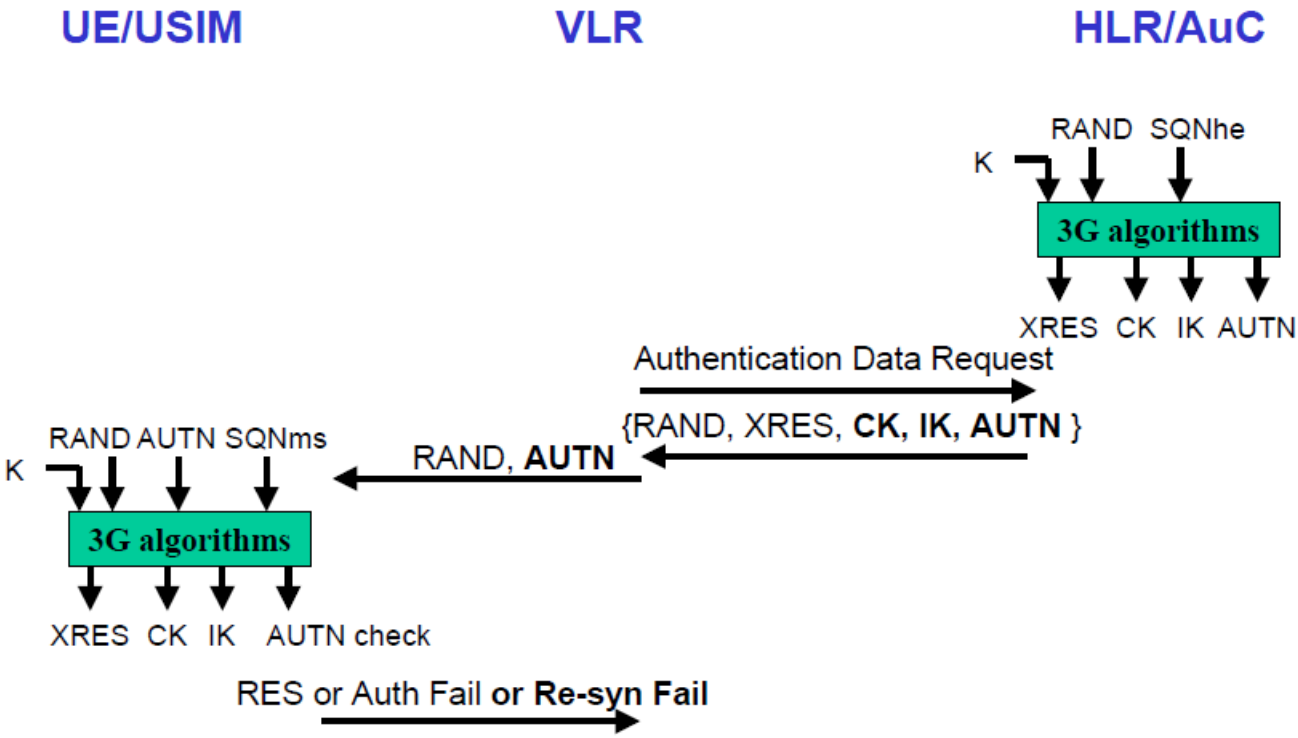
- autentifikavimo centras (AuC);
- lankytojo registras (VLR);
- USIM kortelė.

Autentifikavimo centre saugoma abonento saugumo rakto *K* kopija. AuC gavęs tinklo užklausą sudaro autentifikavimo vektorių, kuris susideda iš penkių komponentų [30]:

- atsitiktinio numerio *RAND*;
- atsakymo patvirtinimo numerio *XRES*;
- šifro rakto *CK*;
- vientisumo rakto *IK*;
- autentifikavimo rakto *AUTN*.

XRES, CK, IK, AUTN yra apskaičiuojami naudojant *RAND, K* ir užklausos eilės numerį *SQN*. UMTS tinkle kiekvienam autentifikavimui reikalingas unikalus autentifikavimo vektorius. Tinklas siunčia vartotojui autentifikavimo užklausą, kurią sudaro du autentifikavimo vektoriaus dėmenys: *RAND* ir *AUTN*. Šie parametrai perduodami į USIM modulį. Jame saugomas pagrindinis raktas *K*, kurį panaudojant kartu su *RAND* ir *AUTN* parametrais, USIM atlieka skaičiavimus pagal autentifikavimo ir rakto susitarimo AKA (angl. *Authentication and key agreement*) algoritmus. Panaudojant skaičiavimų metu gautus rezultatus USIM modulis nustato, ar *AUTN* parametrą tikrai sugeneravo AuC ir jis yra unikalus, t. y. nebuvo siųstas anksčiau. Pastarasis tikrinimas paremtas *SQN* parametro reikšme. Siekiant užtikrinti, kad AuC ir USIM esantys užklausų eilės skaitikliai sutaptų, jie yra sinchronizuojami. Jei USIM patvirtina tinklo autentiškumą, apskaičiuotas atsakymo parametras *RES* su vartotojo autentifikavimo atsakymo pranešimu siunčiamas tinklui. Tuomet iš vartotojo gautas *RES* palyginamas su iš anksto apskaičiuotu atsakymo patvirtinimo numeriu *XRES,* kuris buvo pateiktas autentifikavimo vektoriuje. Jei parametrai sutampa, autentifikavimas užbaigiamas teigiamai ir vartotojui leidžiama naudotis tinklo paslaugomis [30].

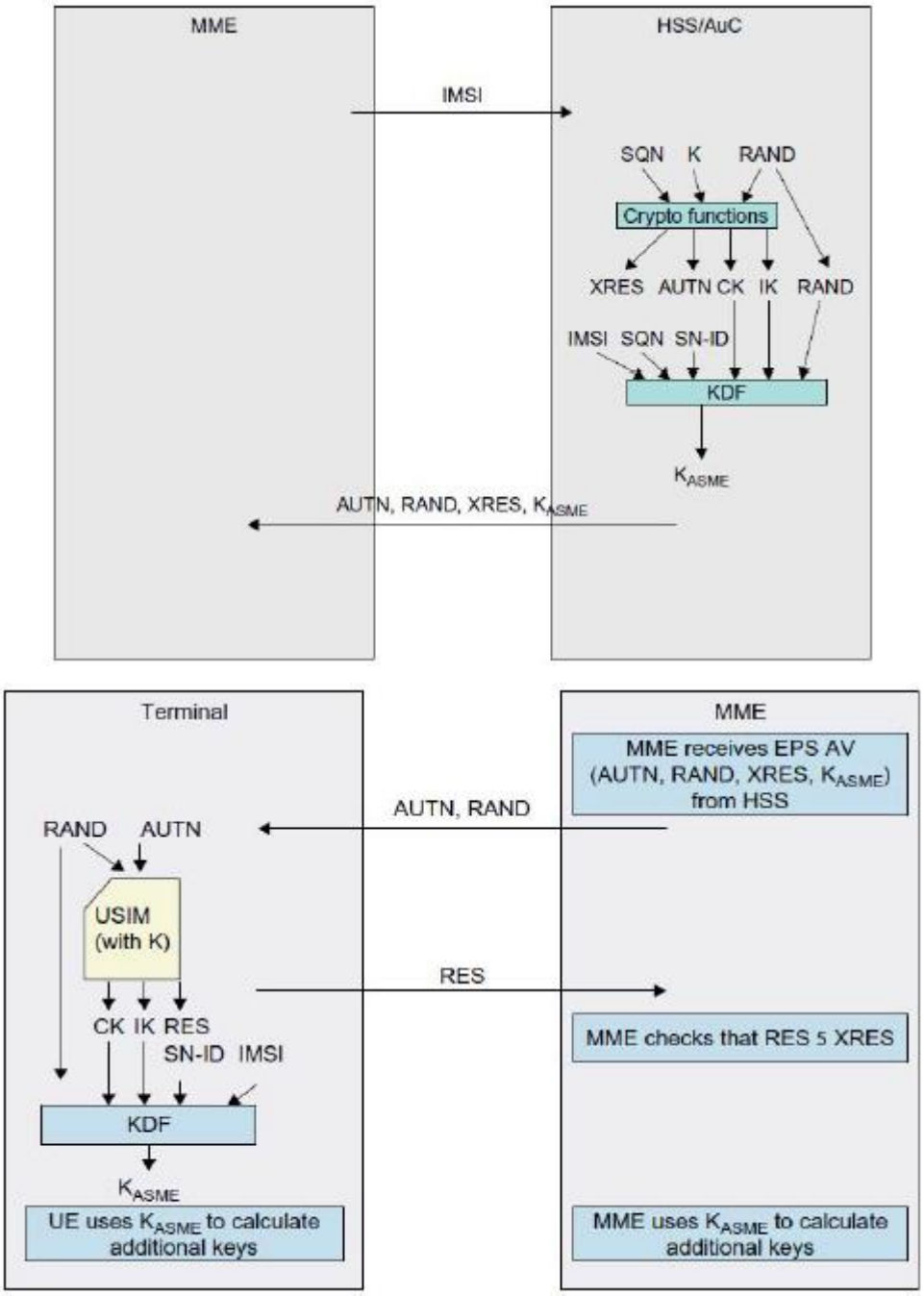
3.8 paveiksle pateikiama UMTS tinkle vykdoma autentifikavimo procedūra. Nauji elementai, lyginant su GSM technologija, yra pajuodinti.



3.8 pav. UMTS tinkle atliekamo autentifikavimo protokolo schema [31]

3.4.3. LTE

Pagrindinis saugumo patobulinimas lyginant LTE ir UMTS sistemose naudojamus AKA algoritmus yra tai, kad *CK* ir *IK* raktai nėra niekur persiunčiami iš HSS (angl. *Home Subscriber Server*) – HLR ir AuC junginio. Vartotojo įrenginys (UE) pradiniame jungimosi prie tinklo pranešime nurodo, kokio tipo prieigos tinklą jis naudos. Jei tai LTE, tuomet *AMF* vėliavėlės reikšmė nustatoma į 1, tai nurodo HSS, kad autentifikavimo vektoriuje, vietoj *CK* ir *IK* raktų, siųstų pagrindinį saugos raktą K_{ASME} [32]. K_{ASME} sugeneruojamas panaudojant *CK, IK* ir kitus parametrus, tarp kurių yra ir paslaugas teikiančio tinklo tapatybės kodas (SN ID). Jį sudaro MCC ir MNC kodai. SN ID įtraukiamas į K_{ASME} generavimo procesą, tam kad būtų galima užtikrinti, jog K_{ASME} raktas yra unikalus ir jo nebūtų galima panaudoti kitame tinkle [33]. 3.9 paveiksle pateikiamas LTE tinkle vykdomo autentifikavimo procedūros algoritmas.



3.9 pav. LTE tinkle atliekamo autentifikavimo procedūros algoritmas [33]

4. MOBILIOJO RYŠIO SIGNALO PAGAVIMO IR BLOKAVIMO METODŲ ANALIZĖ

Pirmieji ryšio blokavimo įrenginiai buvo sukurti ir naudojami kariniais tikslais. Jų poreikis kilo siekiant sutrukdyti informacijos perdavimą tarp siuntėjo ir gavėjo. Šiais laikais mobiliojo ryšio blokavimo prietaisai dažniau naudojami civilinėms reikmėms nei elektroniniam karui, nes kartu su mobiliųjų telefonų vartotojų skaičiaus didėjimu didėjo ir poreikis neutralizuoti mobiliuosius telefonus tose vietose, kur jų naudojimas nepageidautinas. Tolesniame poskyryje apžvelgiami pagrindiniai mobiliojo ryšio signalo blokavimo metodai.

4.1. Mobiliojo signalo blokavimas

Mobiliojo ryšio signalą galima blokuoti įvairiais metodais. Yra išskiriami penki pagrindiniai mobiliojo signalo blokavimo įrenginių tipai [34]. Tolimesniame punkte aprašomi šių įrenginių veikimo principai.

4.1.1. Mobiliojo signalo blokavimo įrenginių tipų apžvalga

„A“ tipo įrenginiai

Šie įrenginiai naudingą mobiliojo ryšio signalą užgožia stipriu radijo triukšmo signalu. Juose montuojami keli nepriklausomi radijo signalo generatoriai, kurių generuojami signalai interferuoja su mobiliojo ryšio kontrolinių kanalų dažniais. „A“ tipo įrenginių aprėpties zonoje esantys mobilieji įrenginiai negali nei atlikti, nei priimti skambučių. Šio tipo įrenginiai tik skleidžia blokuojančiuosius signalus. Didžiausias jų trūkumas - labai prastas dažnio išrinkimas, kuris sukelia ne tik norimų blokuoti, bet ir gretimų dažnių interferenciją.

„A“ tipo įrenginiai gali būti naudojami be ryšio operatoriaus žinios, tačiau jie daro neigiamą poveikį tinklo veikimui, nes radijo triukšmo lygis padidėja ir aplink blokavimo zoną.

„B“ tipo įrenginiai

Šio tipo įrenginiai dar vadinami išmaniaisiais mobiliojo ryšio blokatoriais, tačiau jie neskleidžia kontrolinius kanalus blokuojančių signalų. Numatytoje „tyliojoje“ zonoje toks įrenginys veikia kaip detektorius. Jis turi unikalų identifikacinį numerį, kuris skirtas komunikavimui su bazine stotimi. Kai „B“ tipo įrenginys aptinka mobilųjį telefoną blokavimo zonoje, bazinės stoties programinė įranga neleidžia mobiliajam telefonui atlikti ar priimti skambučių. Kuomet bazinė stotis siunčia signalizacijos signalą konkrečiam vartotojui ir įrenginys jį aptinka, jis informuoja bazinę stotį, kad vartotojas yra blokavimo zonoje, todėl ryšį reikia nutraukti. Tokiu atveju skambučiai gali būti nukreipiami į balso paštą, jei abonentas yra aktyvavęs

šią paslaugą. Toks skambučio aptikimo ir nutraukimo procesas atliekamas per laiko intervalą, kuris skirtas signalizacijos signalo perdavimui ir ryšio patvirtinimui. Išmanusis mobiliojo ryšio blokatorius gali taikyti išimtis tam tikrai vartotojų grupei. Šie vartotojai turi būti iš anksto nurodyti ryšio operatoriui. Kai gaunamas įeinantis skambutis, detektorius atpažįsta numerį ir skambutis užmezgamas numatytam laiko intervalui. Išimtinei grupei priklausantiems vartotojams leidžiama atlikti ir išeinančius skambučius. Taip pat ši sistema atpažįsta ir leidžia atlikti skambučius specialiosioms tarnyboms, pavyzdžiui, 112, 911 ir pan.

Pabrėžtina, kad „B“ tipo įrenginiai turi būti visiškai integruoti į ryšio operatoriaus tinklą ir būti jo dalimi, todėl be ryšio operatoriaus sutikimo tokių įrenginių neįmanoma panaudoti.

„C“ tipo įrenginiai

Šie įrenginiai, kaip ir „B“ tipo įrenginiai, neskleidžia kontrolinius kanalus blokuojančių signalų. Toks įrenginys numatytoje vietoje veikia kaip „švyturys“, kuris visiems suderinamiems mobiliesiems įrenginiams nurodo išjungti skambėjimo toną arba visai riboti mobilųjį ryšį, kol jie yra „švyturio“ aprėpties zonoje. Į tokius nurodymus reaguoti gali tik įrenginiai, kurie turi suderinamus imtuvus. Jų veikimas paremtas ne mobiliojo ryšio technologija, o kokia nors kitokia, pavyzdžiui, *Bluetooth*. Dėl šios priežasties „C“ tipo įrenginys nedaro jokios įtakos mobiliojo ryšio operatoriaus tinklo veikimui ir nereikalauja jokių pakeitimų jame.

Iš anksto numatytiems vartotojams gali būti suteikiama speciali mygtukų kombinacija, kurią suvedus įrenginys nereaguotų į „švyturio“ siunčiamus nurodymus. Tačiau itin sudėtinga užtikrinti, kad tokia kombinacija bus naudojama tik tų vartotojų, kurie turi tam teisę.

Didžiausias šios technologijos trūkumas – tai, kad ji veikia tik su tais įrenginiais, kurie turi suderinamą imtuvą. Įrenginiai, kurie tokio imtuvo neturi, „švyturio“ veikimo zonoje nepatirtų poveikio ir veiktų įprastai.

„D“ tipo įrenginiai

Toks ryšio blokatorius veikia kaip maža nepriklausoma kilnojama bazinė stotis, kuri gali tiesiogiai komunikuoti su mobiliuoju telefonu. Blokatorius veikia imtuvo režimu ir pats pasirenka ar komunikuoti ir blokuoti mobilųjį telefoną, jei jis yra veikimo zonoje.

Atrankinis blokavimo metodas naudoja imtuvą, kuris nustato blokuotiną siųstuvą. Tokio metodo privalumas yra tai, kad mažiau teršiamas radijo eteris. Blokuojantysis signalas transliuojamas tik tol, kol mobilusis telefonas bando prisijungti prie bazinės stoties. Sutrukdžius mobiliajam telefonui prisijungti prie bazinės stoties blokatorius persijungia į pasyvų imtuvo režimą.

„D“ tipo įrenginiai gali būti naudojami be mobiliojo ryšio operatoriaus žinios, tačiau neigiamai įtakoja tinklo veikimą. Lyginant su „B“ tipo įrenginiais, šių privalumas – tai, kad

nereikia eikvoti laiko komunikuojant su operatoriaus tinklu. Taip pat, kaip ir „B“ tipo įrenginiai, šie įrenginiai gali leisti atlikti skambučius specialiųjų tarnybų numeriais.

„E“ tipo įrenginiai

Šis metodas naudoja elektromagnetinės interferencijos technologiją paversdamas patalpą vadinamuoju „Faradėjaus narvu“ [35]. Nors toks įrengimas reikalauja daug darbo, „Faradėjaus narvas“ sustabdo arba stipriai sumažina visos elektromagnetinės spinduliuotės patekimą iš išorės arba išėjimą iš narvo – izoliuojamos patalpos.

Panaudojant rinkoje esančius elektromagnetinės interferencijos ekranavimo produktus jau projektuojant pastatus, galima iš anksto suplanuoti ir įrengti vadinamuosius „tyliuosius“ kambarius.

4.1.2. Blokuojančio ir blokuojamo signalų santykis

Blokavimo efektyvumas priklauso nuo blokuojančio ir blokuojamo signalų santykio. Šis santykis gali būti apskaičiuotas pagal [4]:

$$\frac{J}{S} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j}. \tag{4.1}$$

Čia

P_j – blokuojančio įrenginio siųstuvo galia;

P_t – blokuojamo signalo siųstuvo galia;

G_{jr} – blokuojančio įrenginio antenos stiprinimas blokuojamo signalo imtuvo kryptimi;

G_{rj} – blokuojamo signalo imtuvo antenos stiprinimas blokuojančio įrenginio kryptimi;

G_{tr} – blokuojamo signalo siųstuvo antenos stiprinimas blokuojamo signalo imtuvo kryptimi;

G_{rt} – blokuojamo signalo imtuvo antenos stiprinimas blokuojamo signalo siųstuvo kryptimi;

B_r – blokuojamo signalo imtuvo dažnių juostos plotis;

B_j – blokuojančio įrenginio siųstuvo dažnių juostos plotis;

R_{tr} – atstumas tarp blokuojamo signalo siųstuvo ir blokuojamo signalo imtuvo;

R_{jt} – atstumas tarp blokuojančio signalo siųstuvo ir blokuojamo signalo imtuvo;

L_j – blokuojančio signalo slopimas, įskaitant poliarizacijos nesutapimą;

L_r – blokuojamo signalo slopimas.

Iš 4.1 formulės matyti, kad padvigubėjus atstumui tarp blokuojančio įrenginio ir blokuojamą signalą priimančio įrenginio, blokuojančio įrenginio siunčiamo signalo galią reikia padidinti keturis kartus, jog būtų pasiektas toks pats efektas.

4.2. Mobiliojo signalo pagavimas

Signalo, tarp mobiliojo ryšio vartotojo ir mobiliojo ryšio tinklo, pagavimui naudojami įrenginiai vadinami IMSI gaudyklėmis (angl. *IMSI catcher*). IMSI gaudyklė buvo sukurta visų netoliese esančių mobiliųjų įrenginių elektroninei tapatybei nustatyti. Elektroninę telefono tapatybę nusako IMSI kodas, kuris yra susijęs su abonento SIM kortele, ir IMEI kodas, kuris atitinka mobiliojo telefono serijos numerį. IMSI gaudyklė yra naudojama „tarpiniam įsilaužimui“ (angl. *man-in-the-middle attack*), nes ji įsiterpia tarp mobiliojo įrenginio ir tinklo bazinės stoties. Iš esmės tai yra nedidelė bazinė stotis, kuri priverčia mobilųjį telefoną naudotis jos, o ne tikrosios tinklo bazinės stoties paslaugomis, nes skleidžia stipresnį signalą nei nutolusi bazinė stotis.

1996 m. Vokietijoje įsikūręs radijo įrangos gamintojas *Rohde & Schwarz* Miuncheno mieste pristatė pirmąją IMSI gaudyklę *GA 090*. Pristatyto įrenginio tikslas buvo identifikuoti vartotoją priverčiant jį atsiųsti savo IMSI kodą, pagal kurį, su ryšio operatoriaus pagalba, galima nustatyti jam priskirtą telefono numerį. 1997 m. buvo išleista patobulinta gaudyklė *GA 900,* kuri leido ne tik nustatyti IMSI kodą, bet ir perimti išeinančius skambučius [20].

Liūdnai pagarsėjusį kompiuterių hakerį Kevin Mitnick 1995 m. FTB agentai surado panaudoję aktyvaus bazinės stoties imitatoriaus ir pasyvaus *TriggerFish, Harris Corporation* kompanijos pagaminto skaitmeninio analizatoriaus, derinį. Aktyvus bazinės stoties imitatorius į Mitnick telefoną nusiuntė pranešimą nesukeliantį jokio garsinio įspėjimo, tuomet panaudojant pasyvų *TriggerFish* analizatorių buvo nustatyta telefono buvimo vieta. 2003 m. *Harris Corporation* pristatė žymiai tobulesnį *StingRay* produktą, kuris atliko aktyvų skaitmeninių mobiliųjų telefonų sekimą. Ši kompanija dabar gamina paltų mobiliųjų telefonų sekimo produktų, kurie gali būti montuojami automobiliuose, lėktuvuose ir dronuose ar būti nešami žmogaus, asortimentą [36].

IMSI gaudyklės surenka visus IMSI kodus, kurie yra aktyvūs geografinėje vietovėje. Tai padaryti galima dviem skirtingais būdais: pasyviu arba aktyviu. Pasyvusis būdas – tai belaidžio srauto stebėjimas ir visų sugautų IMSI kodų saugojimas. Žymiai efektyvesnis yra antrasis, aktyvusis būdas, kai sumontuojama netikra bazinė stotis, prie kurios bando prisijungti visi netoliese esantys mobilieji įrenginiai. Tuomet netikra bazinė stotis pareikalauja, kad kiekvienas mobilusis telefonas identifikuotų save. Šiuo būdu IMSI kodai gali būti gauti bet kuriuo metu, o naudojant pasyvųjį metodą, reikia laukti, kol telefonai patys išsiųs savo IMSI kodus. Bėgant laikui

komercinės IMSI gaudyklės buvo gerokai patobulintos, pridedant tokių papildomų funkcijų kaip pokalbių pasiklausymas ar skambučių blokavimas [15]. Tolimesniame punkte aprašomas IMSI gaudyklės veikimo algoritmas.

4.2.1. IMSI gaudyklės veikimo algoritmas

Nors IMSI gaudyklių funkcionalumai gali būti skirtingi, jos visos veikia panašiu principu. Šiame punkte detalizuojamas jos veikimo principo algoritmas pagal [20], [13], [37], [38].

IMSI kodo gavimas

Kuomet vietovėje yra daugiau nei viena mobilaus ryšio operatoriaus bazinė stotis, judrioji stotis visada prisijungia prie tos bazinės stoties, kurios siunčiamas signalas yra stipriausias. Todėl IMSI gaudyklė siųsdama pakankamai stiprų signalą, gali priversti visas judriąsias stotis, esančias nedideliu spinduliu, prisijungti prie jos.

Tokiu atveju IMSI gaudyklė imituoja tikros bazinės stoties veikimą. Pirmiausiai judrioji stotis yra priversta siųsti informaciją apie palaikomą šifravimą, tačiau šią informaciją IMSI gaudyklė gali ignoruoti ir informacijos perdavimui nenaudoti jokio šifravimo. Tuomet IMSI gaudyklė siunčia reikalavimą save identifikuoti (angl. *identity request*), į kurį judrioji stotis privalo atsakyti persiusdama savo IMSI kodą.

Tinklo ryšio inicijavimas

IMSI gaudyklė, gavusi judriosios stoties IMSI kodą, gali jungtis prie mobiliojo ryšio tinklo siųsdama buvimo vietos atnaujinimo užklausą (angl. *location update request*). Kai tinklas atsako reikalaudamas save identifikuoti, IMSI gaudyklė atsako persiųsdama iš judriosios stoties gautą IMSI kodą.

Vėliau autorizacijos patvirtinimui tinklas siunčia atsitiktinį numerį *RAND*. Kadangi IMSI gaudyklė neturi ilgalaikio saugos rakto K_i, ji negali atsakyti į šią užklausą.

Judriosios stoties prijungimas

Kadangi IMSI gaudyklė negali atsakyti į gautą autorizacijos patvirtinimo užklausą, toliau tęsiant komunikaciją, ją persiunčia judriajai stočiai. Judrioji stotis gavusi minėtą užklausą, naudodama korektišką ilgalaikį saugos raktą K_i, apskaičiuoja patvirtinimo atsakymą *SRES'* ir jį persiunčia IMSI gaudyklei. Šiame etape IMSI gaudyklei nereikia tikrinti *SRES'* korektiškumo, todėl jis tiesiog ignoruojamas, o judriosios stoties autorizacija patvirtinama ir užbaigiamas sujungimas. Jei nėra reikalingas sujungimas su bazine stotimi, tai IMSI gaudyklė pati gali

sugeneruoti savo atsitiktinį numerį RAND ir kartu su autorizacijos patvirtinimo užklausa nusiųsti judriajai stočiai, taip imituojant autorizaciją.

Kadangi GSM protokole bazinė stotis nustato šifravimo režimą, tai IMSI gaudyklė gali nurodyti judriajai stočiai naudoti A5/0 šifro režimą – nešifruoti siunčiamos informacijos. Tuomet judriajai stočiai ji priskiria TMSI kodą ir priima buvimo vietos atnaujinimo užklausą. Nuo šio momento IMSI gaudyklė gali laisvai komunikuoti su judriąja stotimi ir perimti siunčiamą informaciją.

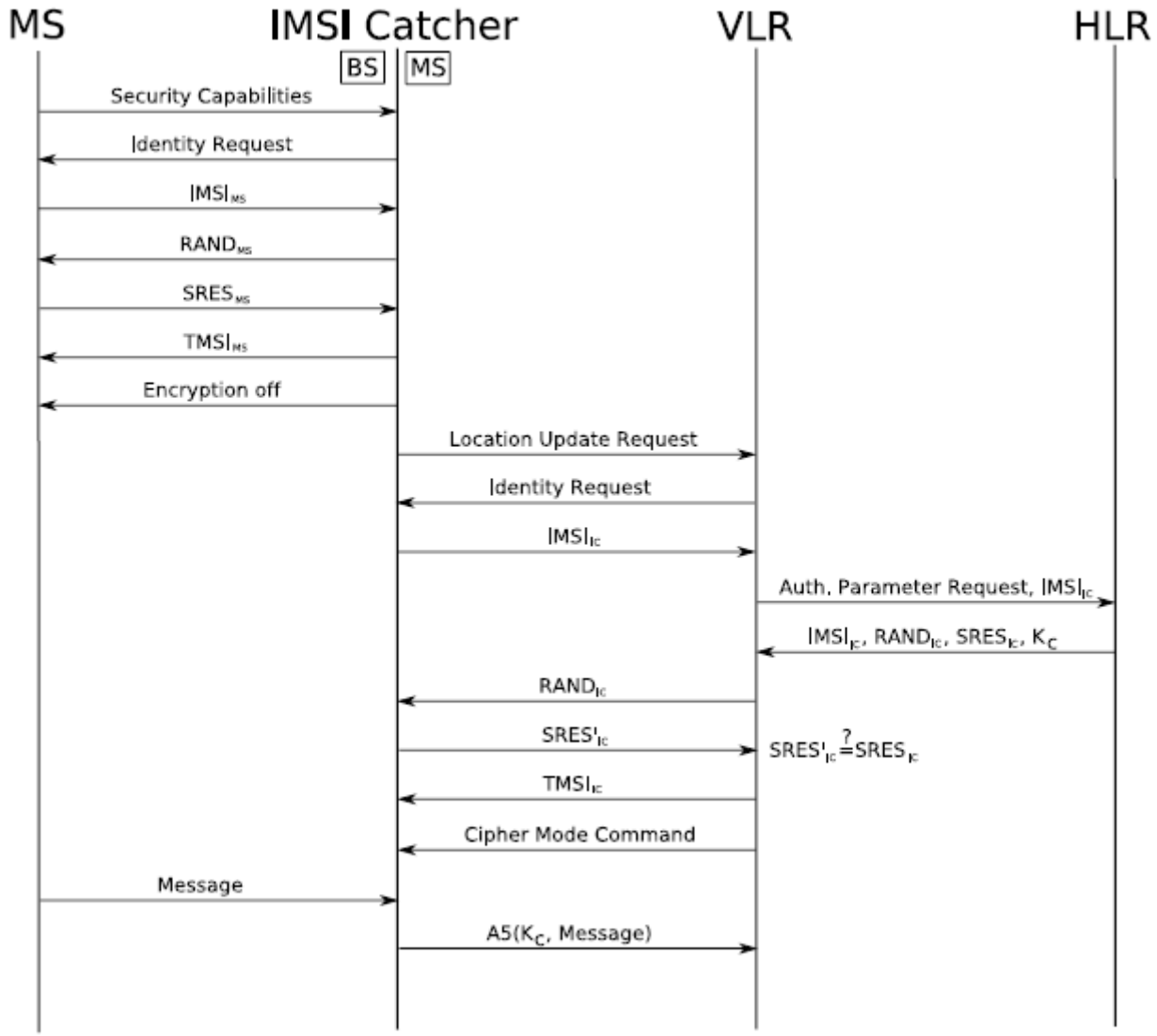
IMSI gaudyklės prisijungimas prie tinklo

IMSI gaudyklė bazinei stočiai persiunčia iš judriosios stoties gautą pasirašytą atsakymą ir *SRES'* kodą, taip užbaigiama autentifikavimo tinkle procedūra.

Jei tinklas bando nustatyti A5/1, A5/2 arba A5/3 šifro režimą, IMSI gaudyklė gali atsisakyti šifravimo nurodydama, kad nepalaiko informacijos šifravimo funkcijos, taip nustatant A5/0 šifro režimą. Nuo šio momento IMSI gaudyklė gali pilnai komunikuoti su mobiliojo ryšio tiekėjo tinklu. Visas IMSI gaudyklės prisijungimo prie judriosios stoties bei mobiliojo ryšio tiekėjo tinklo algoritmas pateikiamas 4.1 paveiksle.

Judriosios stoties izoliavimas

Kuomet IMSI gaudyklė užbaigia prisijungimą prie mobiliojo ryšio tiekėjo tinklo, ji gali bandyti apriboti judriosios stoties prisijungimo prie kitos bazinės stoties. Įprastai bazinės stotys pateikia kitų, netoliese esančių, bazinių stočių sąrašą (angl. *neighboring cell list*), kad vartotojų įrenginiai galėtų lengvai ir be ryšio nutrūkimų persijungti tarp skirtingų celių. IMSI gaudyklė vietoje to gali pateikti tuščią sąrašą arba bazinių stočių sąrašą, kurios judriajai stočiai yra nepasiekiamos.



4.1 pav. IMSI gaudyklės prisijungimo prie judriosios soties ir mobiliojo ryšio tinklo algoritmas [20]

5. RYŠIO BLOKAVIMO EFEKTYVUMO DIDINIMO GALIMYBIŲ TYRIMAS

Siekiant efektyviai užblokuoti mobilaus ryšio radijo bangas tam tikroje vietovėje, reikia atlikti kuo tikslesnį blokuojančio signalo sklidimo prognozavimą ir atitinkamai išdėstyti šį signalą skleidžiančią įrangą. Priešingu atveju gali nepavykti pasiekti norimo rezultato arba paveikti didesnę teritoriją bei daugiau vartotojų, nei buvo planuota. Naudojant signalo blokavimo prietaisą, yra blokuojami visi įrenginiai, esantys blokatoriaus veikimo zonoje, be išimties, nebent naudojamas „B“ tipo blokavimo įrenginys. Tačiau šio tipo įrenginio veikimo įgyvendinimui būtinas jo integravimas į mobilaus ryšio tiekėjo tinklą. Tai net tik reikalauja papildomų investicijų, bet ir būtinas operatoriaus sutikimas. Dėl šių priežasčių mobiliojo ryšio blokavimui geriau naudoti IMSI gaudyklę. Tuomet yra galimybė valdyti blokuotinų vartotojų sąrašą, nebūtinas įrenginio integravimas į operatoriaus tinklą, triukšmu neteršiamas radijo eteris. 5.1 poskyryje atliekamas mobiliojo ryšio signalą pagaunančios įrangos tinklo padengimo modeliavimas Pravieniškių pataisos namų-atvirosios kolonijos teritorijoje.

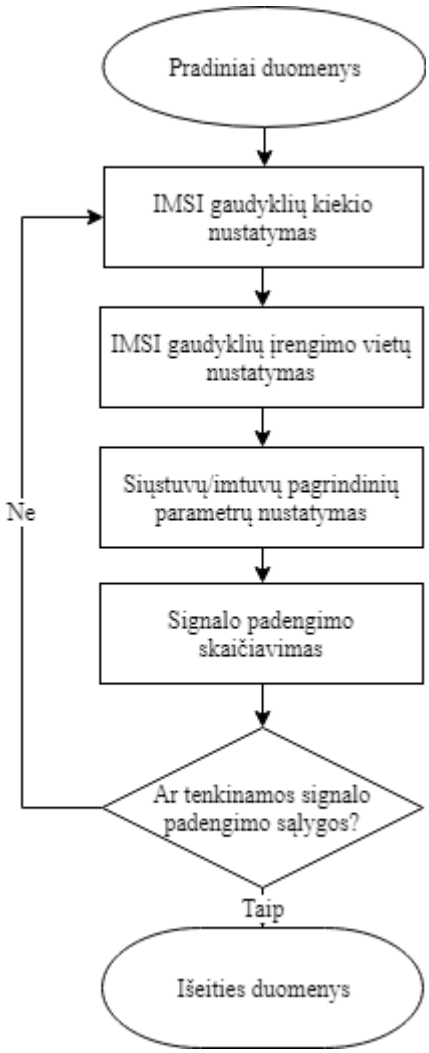
Šiuo metu yra vystomas ne vienas atvirojo kodo projektas, kurio pagalba galima nustatyti ar judrioji stotis yra prisijungusi prie IMSI gaudyklės arba įspėti vartotoją, jei jo buvimo teritorijoje veikia netikra bazinė stotis. Vienas labiausiai išvystytų projektų yra *Security Research Labs* kompanijos sukurta, *Android* operacinei sistemai skirta, aplikacija *SnoopSnitch* [1]. Dar viena paminėjimo verta aplikacija yra *SecUpwN* kompanijos sukurta *Android IMSI-Catcher Detector (AIMSICD)*, kuri taip pat skirta *Android* operacinei sistemai [2].

5.2 poskyryje aprašomos IMSI gaudyklių atpažinimui ir identifikavimui naudojamos jų veikimo anomalijos (lyginant su tikromis bazinėmis sotimis), kuriomis paremtas aukščiau aprašytų aplikacijų veikimas. Taip pat prie kiekvieno iš atpažinimo požymių, pateikiami siūlomi sprendimai, kurių pagalba IMSI gaudyklės būtų sunkiau atpažįstamos.

5.1. IMSI gaudyklių tinklo padengimo modeliavimas

Šiame poskyryje atliekamas mobiliojo ryšio signalą pagaunančios įrangos tinklo signalo padengimo modeliavimas Pravieniškių pataisos namų-atvirosios kolonijos teritorijoje. Vieta pasirinkta atsitiktiniu būdu. Skaičiavimai atliekami *ArcGIS* ir *CellularExpert* programine įranga.

Tinklo projektavimas yra iteracinis procesas. Priklausomai nuo rezultatų yra vykdomos parametrų ar bazinės stoties pozicijos korekcijos ir skaičiavimai kartojami tol, kol gaunami tenkinantys rezultatai – šiuo atveju, IMSI gaudyklės (-ių) skleidžiamo signalo lygis visoje įkalinimo įstaigos teritorijoje, turi būti bent 5 dB didesnis nei realių bazinių stočių, o už teritorijos ribų atvirkščiai – mažesnis. Veiksmai atliekami pagal 5.1 pav. pateikiamą algoritmą.



5.1 pav. IMSI gaudyklių įrengimo vietų ir pagrindinių parametrų nustatymo algoritmas

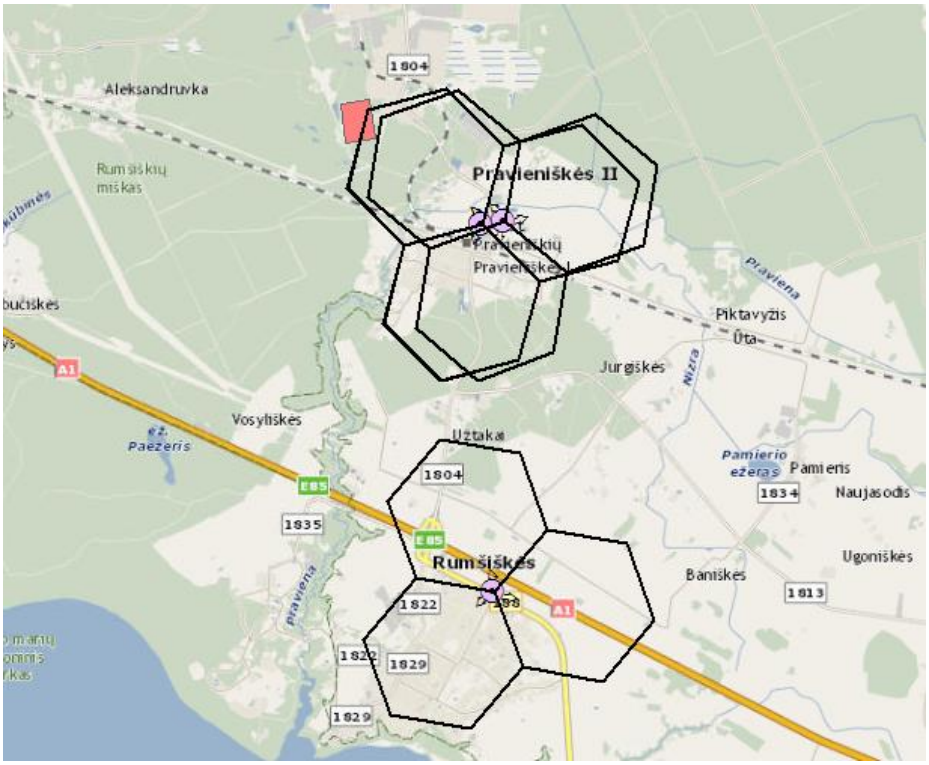
Kadangi bausmę atliekantys piliečiai yra apgyvendinti triaukščiuose pastatuose, todėl signalo lygis turi būti įvertinamas keturiuose skirtinguose aukščiuose: 1,5 m, 5 m, 10 m ir 15 m. Tai atitinka buvimą kieme, pirmajame, antrajame bei trečiajame pastato aukštuose. 5.2 pav.eiksle pateikiama įkalinimo įstaigos teritorijos nuotrauka iš oro. Raudonai pažymėtoje teritorijoje reikalingas ryšio blokavimas.

5.2 pav. Pravieniškių pataisos namų-atvirosios kolonijos teritorijos nuotrauka iš oro

Tolimesniuose punktuose pateikiamas trijų skirtingų technologijų (GSM, UMTS, LTE) signalo padengimo modeliavimas. Modeliuojant bazinės stotys išdėstytos taip, kad atitiktų realias sąlygas. 5.1 lentelėje pateikiamos bazinių stočių koordinatės, aukščiai, sektorių kryptys bei antenų palinkimo kampai, o 5.3 pav.eiksle matomas grafiškas bazinių stočių išdėstymas žemėlapyje (raudonu keturkampiu pažymėta įkalinimo įstaigos teritorija).

5.1 lentelė. Bazinių stočių sektorių duomenys

Sektorius	Platuma	Ilguma	Azimutas, °	Palink. kamp., °	Aukštis, m
site2_1	54° 54' 11,58"	24° 13' 24,65"	315	2	60
site2_2	54° 54' 11,58"	24° 13' 24,65"	75	2	60
site2_3	54° 54' 11,58"	24° 13' 24,65"	195	2	60
site3_1	54° 54' 11,58"	24° 13' 24,77"	315	2	60
site3_2	54° 54' 11,58"	24° 13' 24,77"	75	2	60
site3_3	54° 54' 11,58"	24° 13' 24,77"	195	2	60
site4_1	54° 54' 12,43"	24° 13' 36,56"	310	2	60
site4_2	54° 54' 12,43"	24° 13' 36,56"	70	2	60
site4_3	54° 54' 12,43"	24° 13' 36,56"	190	2	60
site5_1	54° 52' 21,18"	24° 13' 30,56"	340	2	60
site5_2	54° 52' 21,18"	24° 13' 30,56"	220	2	60
site5_3	54° 52' 21,18"	24° 13' 30,56"	100	2	60



5.3 pav. Bazinių stočių išdėstymas žemėlapyje

Optimaliausi IMSI gaudyklių siųstuvų ir antenų nustatymai randami bandymų būdu. Atlikus modeliavimą įvertinamas IMSI gaudyklės (-ių) ir bazinių stočių signalo padengimo santykis, jei jis netenkina sąlygų, tuomet koreguojami siųstuvų parametrai ir/arba įrengimo vietos bei kartojamas modeliavimas, kaip parodyta 5.1 pav.eiksle pavaizduotame algoritme.

5.1.1. GSM

Signalo padengimo modeliavimas buvo pradėtas nuo 900 MHz dažnio GSM technologijos. Parinkti tokie bazinių stočių siųstuvų parametrai:

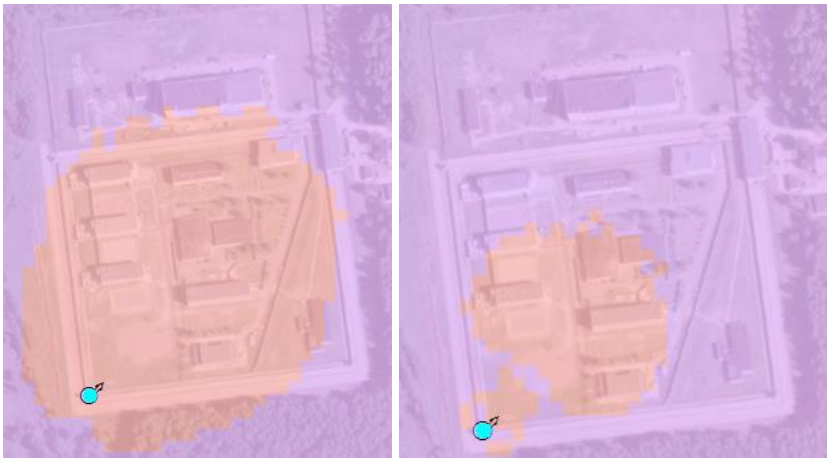
- siųstuvo galia: 33 dBm;
- antenos stiprinimas: 17,2 dBi;
- antenos spinduliavimo kampas: 90°.

Siekiant apspinduliuoti teritoriją visoje 1,5 – 15 m. aukščio amplitudėje, IMSI gaudyklės (-ių) anteną (-as) reikia pakelti kuo aukščiau ir palenkti ją (-as) žemyn. Jų įrengimui puikiai tinka teritorijoje esantys pastatai.

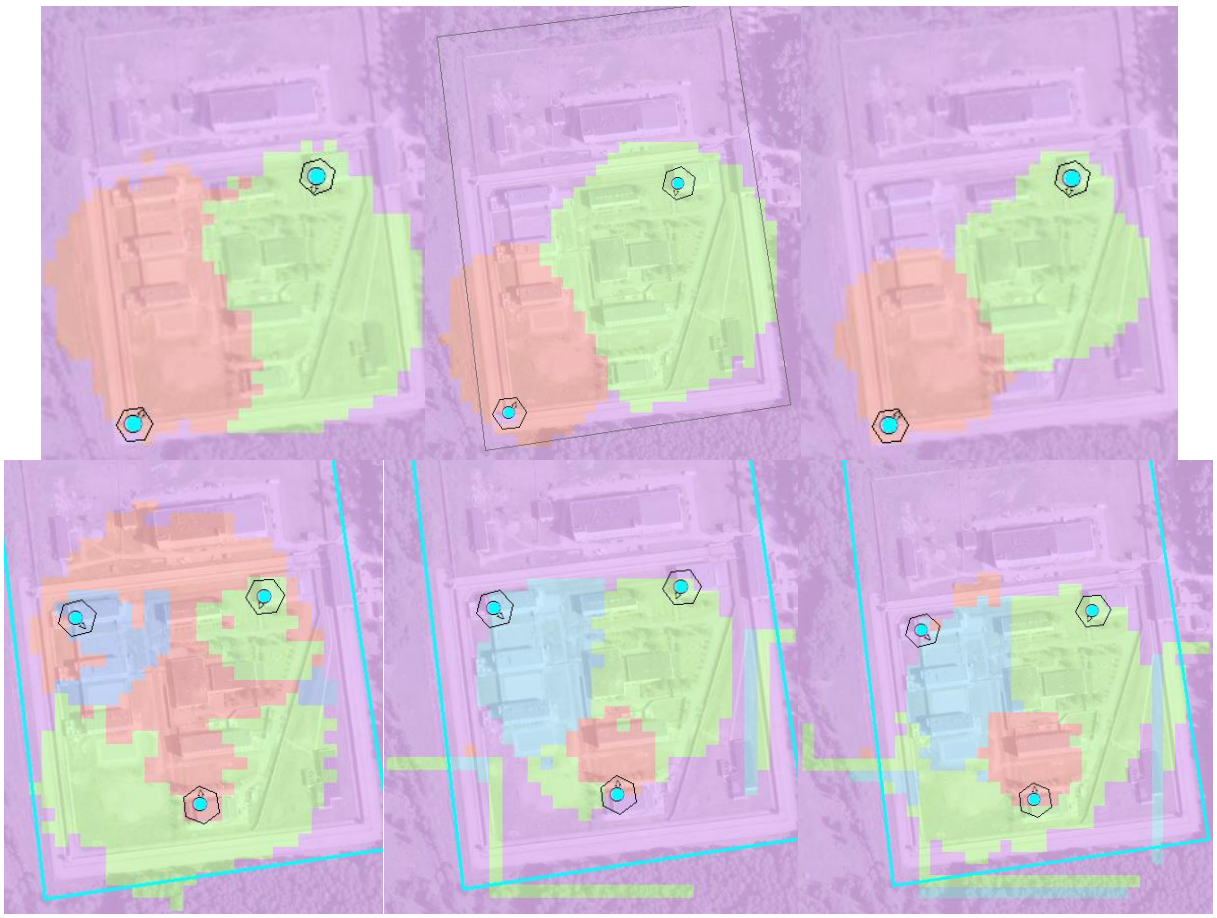
Pirmam bandymui pasirinktas nenaudojamas pastatas esantis įkalinimo įstaigos teritorijos šiaurinėje dalyje. Jis yra ~15 m aukščio, o nuo jo stogo matosi visa teritorija, tačiau šioje pozicijoje nepavyko pasiekti norimo signalo padengimo – nors buvo dengiama visa teritorija, bet IMSI gaudyklės ir tikrų bazinių stočių signalų skirtumas buvo per mažas, o dar labiau padidinus galią

signalas pasiekė ir gyvenamas zonas už įkalinimo įstaigos teritorijos ribų. Vėliau atlikta dar ~100 5.1 pav.eiksle pavaizduoto algoritmo iteracijų, kol galiausiai buvo rastas optimaliausia konfigūracija. Žemiau pateikiami keli išbandyti įrangos išdėstymo variantai (žiūrėti 5.4 pav.) ir signalo padengimo lygiai (žiūrėti 5.5 pav. 5.6 pav.).

5.4 pav. Bandymo būdu patikrintos galimos IMSI gaudyklių išdėstymo vietos



5.5 pav. IMSI gaudyklės signalo padengimas 1,5 m. aukštyje (kairėje) ir 15 m. aukštyje (dešinėje)



5.6 pav. IMSI gaudyklės signalo padengimas 1,5 m. aukštyje (kairėje), 10 m. aukštyje (viduryje) ir 15 m. aukštyje (dešinėje)

Galutinis IMSI gaudyklių išdėstymas pateikiamas 5.7 pav.eiksle, o parametrai 5.2 lentelėje.

5.7 pav. Galutinis IMSI gaudyklių išdėstymas

5.2 lentelė. IMSI gaudyklių duomenys

Sektorius	Platuma	Ilguma	Azimutas, °	Palink. kamp., °	Aukštis, m	Siųstuvo galia, dBm	Antenos stiprinimas, dBi
site1-1_1	54° 54' 38,54"	24° 12' 20,44"	353	6,5	17	13	17,2
site1-2_1	54° 54' 43,79"	24° 12' 23,26"	205	3	16	13	17,2
site1-3_1	54° 54' 43,26"	24° 12' 15,03"	135	3,5	16	11,5	17,2

Esant tokioms sąlygoms buvo gautas geriausias signalo padengimas visuose aukščiuose: 1,5 m., 5 m., 10 m. ir 15 m.

Siekiant tiksliai įvertinti signalų lygius buvo naudojamas ne tik grafinis atvaizdavimas, bet ir pasirinkti šeši kontroliniai taškai, kuriuose matuojami signalų lygiai (žiūrėti 5.8 pav. ir 5.3 lentelėę).

5.8 pav. Kontrolinių taškų išdėstymas teritorijoje

5.3 lentelė. Kontrolinių taškų duomenys

Pavadinimas	Platuma	Ilguma
cust1	54° 54' 38,75"	24° 12' 21,91"
cust2	54° 54' 40,49"	24° 12' 22,12"
cust3	54° 54' 40,89"	24° 12' 15,70"
cust4	54° 54' 41,81"	24° 12' 23,29"
cust5	54° 54' 43,50"	24° 12' 16,96"
cust6	54° 54' 43,39"	24° 12' 21,46"

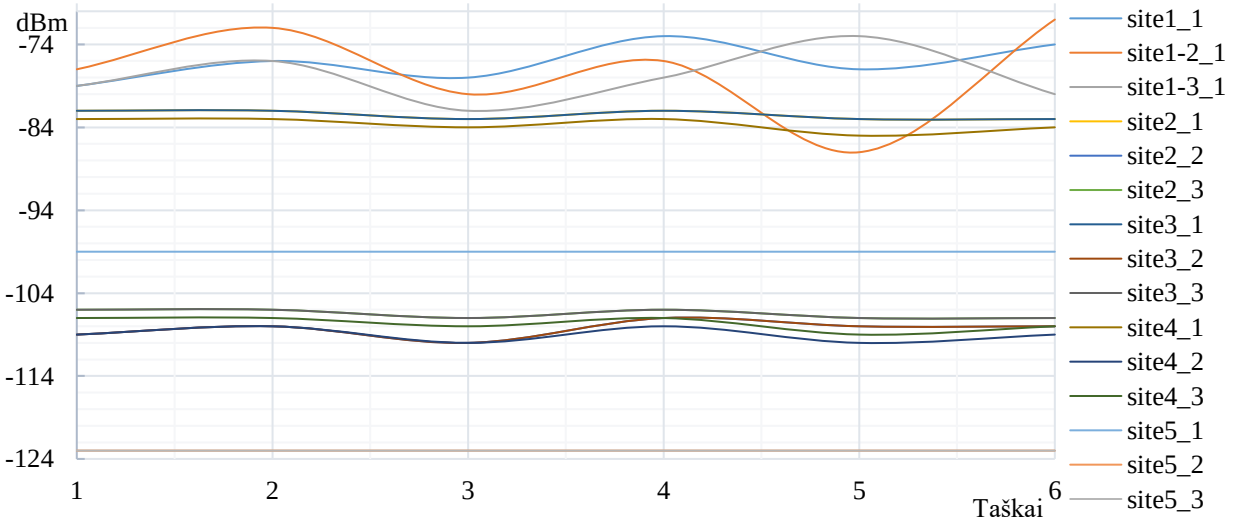
Toliau pateikiami detalūs signalo padengimo visuose matuotuose aukščiuose rezultatai:

- signalo padengimas 1,5 m. aukštyje:

5.9 pav. Signalo padengimas 1,5 m. aukštyje

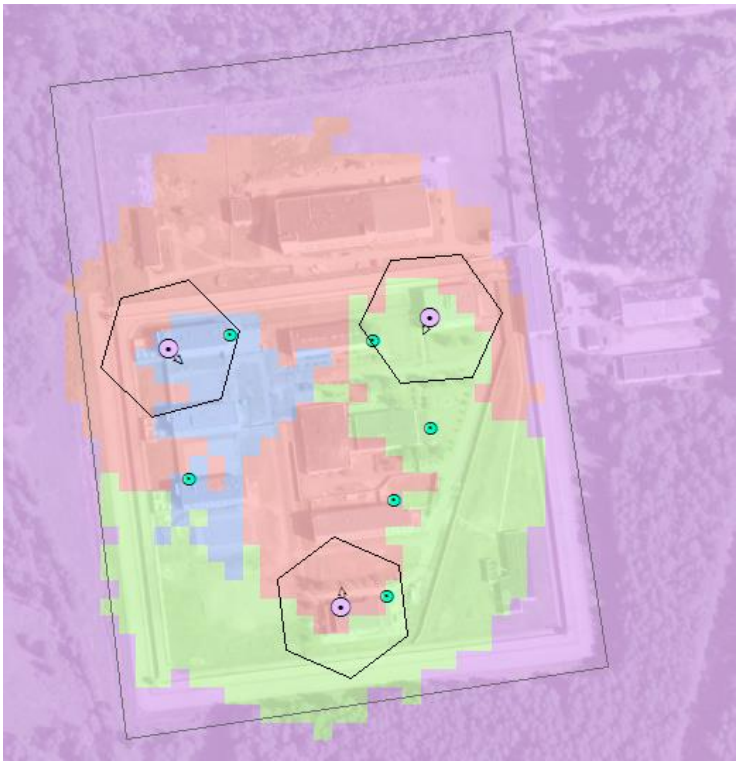
5.4 lentelė. Signalų lygis kontroliniuose taškuose 1,5 m aukštyje

	site1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-79	-77	-79	-82	-109	-106	-82	-109	-106	-83	-109	-107	-99	-123	-123
Taškas2	-76	-72	-76	-82	-108	-106	-82	-108	-106	-83	-108	-107	-99	-123	-123
Taškas3	-78	-80	-82	-83	-110	-107	-83	-110	-107	-84	-110	-108	-99	-123	-123
Taškas4	-73	-76	-78	-82	-107	-106	-82	-107	-106	-83	-108	-107	-99	-123	-123
Taškas5	-77	-87	-73	-83	-108	-107	-83	-108	-107	-85	-110	-109	-99	-123	-123
Taškas6	-74	-71	-80	-83	-108	-107	-83	-108	-107	-84	-109	-108	-99	-123	-123



5.10 pav. Signalų lygių kontroliniuose taškuose (1,5 m. aukštyje) diagrama

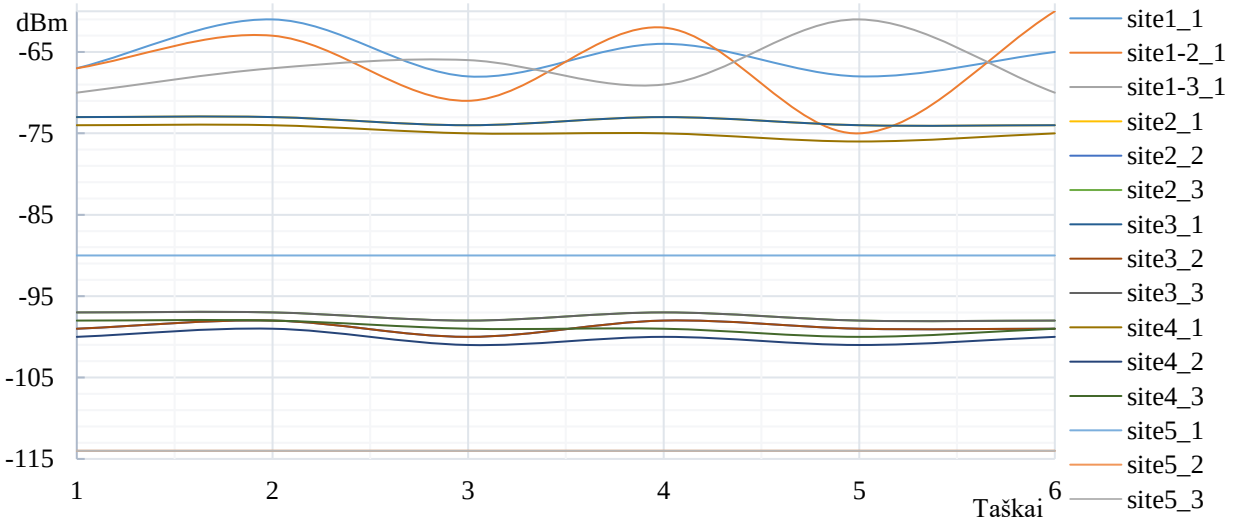
- signalo padengimas 5 m. aukštyje:



5.11 pav. Signalo padengimas 5 m. aukštyje

5.5 lentelė. Signalų lygis kontroliniuose taškuose 5 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-67	-67	-70	-73	-99	-97	-73	-99	-97	-74	-100	-98	-90	-114	-114
Taškas2	-61	-63	-67	-73	-98	-97	-73	-98	-97	-74	-99	-98	-90	-114	-114
Taškas3	-68	-71	-66	-74	-100	-98	-74	-100	-98	-75	-101	-99	-90	-114	-114
Taškas4	-64	-62	-69	-73	-98	-97	-73	-98	-97	-75	-100	-99	-90	-114	-114
Taškas5	-68	-75	-61	-74	-99	-98	-74	-99	-98	-76	-101	-100	-90	-114	-114
Taškas6	-65	-60	-70	-74	-99	-98	-74	-99	-98	-75	-100	-99	-90	-114	-114



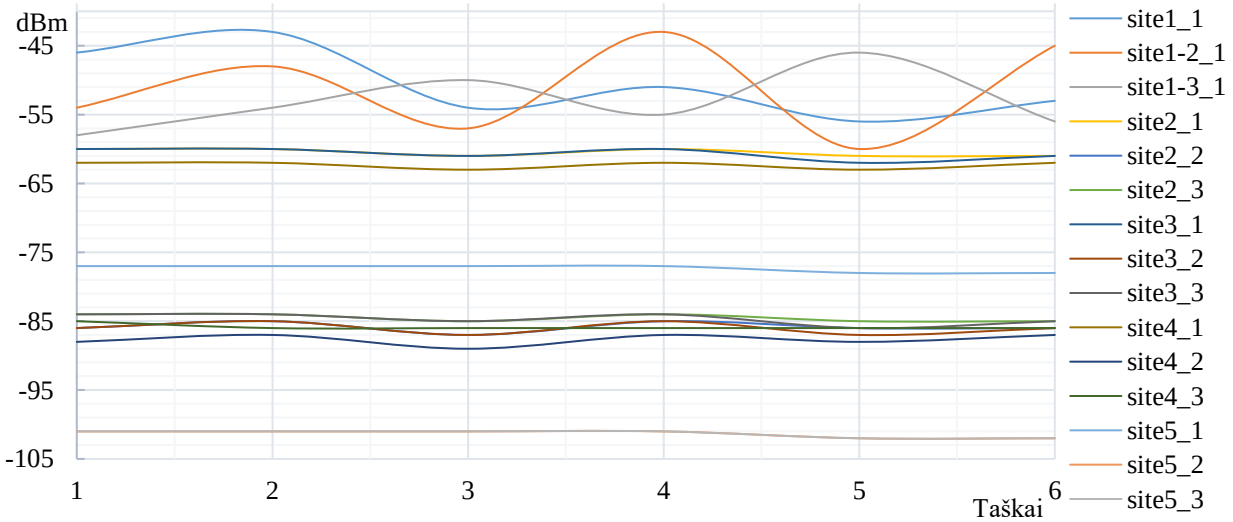
5.12 pav. Signalų lygių kontroliniuose taškuose (5 m. aukštyje) diagrama

- signalo padengimas 10 m. aukštyje:

5.13 pav. signalo padengimas 10 m. aukštyje

5.6 lentelė. Signalų lygis kontroliniuose taškuose 10 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-46	-54	-58	-60	-86	-84	-60	-86	-84	-62	-88	-85	-77	-101	-101
Taškas2	-43	-48	-54	-60	-85	-84	-60	-85	-84	-62	-87	-86	-77	-101	-101
Taškas3	-54	-57	-50	-61	-87	-85	-61	-87	-85	-63	-89	-86	-77	-101	-101
Taškas4	-51	-43	-55	-60	-85	-84	-60	-85	-84	-62	-87	-86	-77	-101	-101
Taškas5	-56	-60	-46	-61	-86	-85	-62	-87	-86	-63	-88	-86	-78	-102	-102
Taškas6	-53	-45	-56	-61	-86	-85	-61	-86	-85	-62	-87	-86	-78	-102	-102



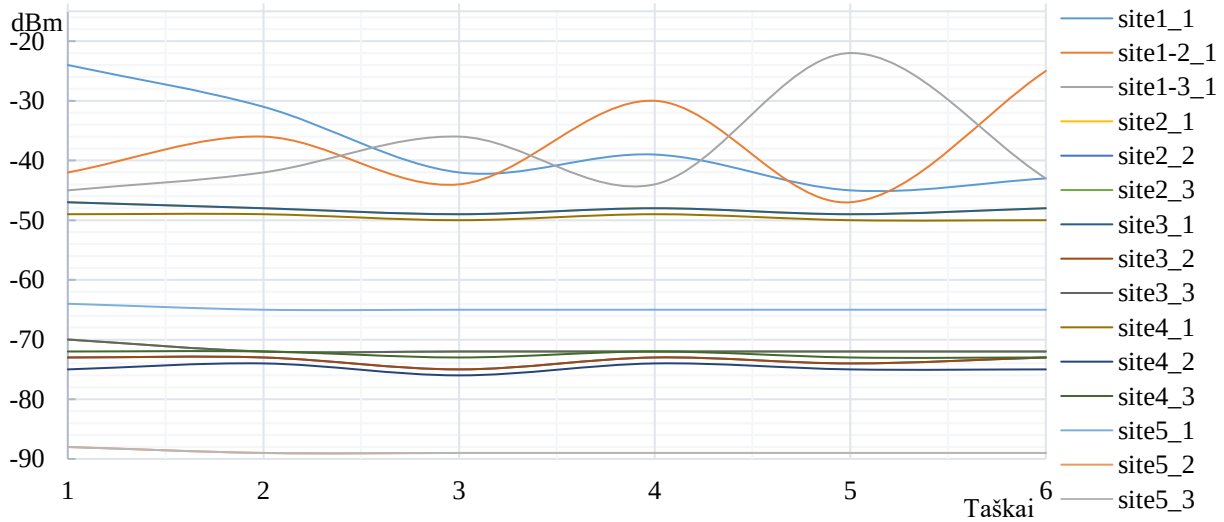
5.14 pav. Signalų lygių kontroliniuose taškuose (10 m. aukštyje) diagrama

- signalo padengimas 15 m. aukštyje:

5.15 pav. Signalo padengimas 15 m. aukštyje

5.7 lentelė. Signalų lygis kontroliniuose taškuose 15 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-24	-42	-45	-47	-73	-70	-47	-73	-70	-49	-75	-72	-64	-88	-88
Taškas2	-31	-36	-42	-48	-73	-72	-48	-73	-72	-49	-74	-72	-65	-89	-89
Taškas3	-42	-44	-36	-49	-75	-72	-49	-75	-72	-50	-76	-73	-65	-89	-89
Taškas4	-39	-30	-44	-48	-73	-72	-48	-73	-72	-49	-74	-72	-65	-89	-89
Taškas5	-45	-47	-22	-49	-74	-72	-49	-74	-72	-50	-75	-73	-65	-89	-89
Taškas6	-43	-25	-43	-48	-73	-72	-48	-73	-72	-50	-75	-73	-65	-89	-89



5.16 pav. Signalų lygių kontroliniuose taškuose (15 m. aukštyje) diagrama

Toliau modeliuojamas 1800 MHz dažnio signalų padengimas. Parinkti tokie bazinių stočių siųstuvų parametrai:

- siųstuvo galia: 33 dBm;
- antenos stiprinimas: 16,4 dBi;
- antenos spinduliavimo kampas: 90°.

Nekeičiant IMSI gaudyklių antenų išdėstymo, o tik minimaliai pakoregavus siųstuvų galias (žiūrėti 5.8 lentelėę), buvo gautas optimaliausias signalo padengimas visuose aukščiuose: 1,5 m., 5 m., 10 m. ir 15 m.

5.8 lentelė. IMSI gaudyklių duomenys

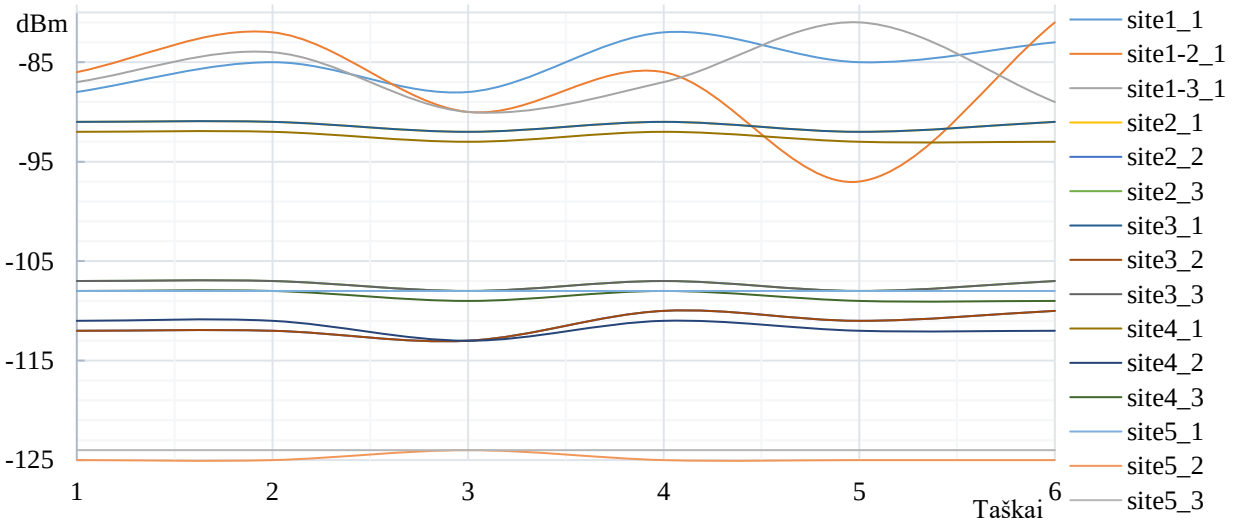
Sektorius	Platuma	Ilguma	Azimutas, °	Palink. kamp., °	Aukštis, m	Siųstuvo galia, dBm	Antenos stiprinimas, dBi
site1-1_1	54° 54' 38,54"	24° 12' 20,44"	353	6,5	17	12	16,4
site1-2_1	54° 54' 43,79"	24° 12' 23,26"	205	3	16	11	16,4
site1-3_1	54° 54' 43,26"	24° 12' 15,03"	135	3,5	16	11	16,4

- Signalo padengimas 1,5 m. aukštyje:

5.17 pav. Signalo padengimas 1,5 m. aukštyje

5.9 lentelė. Signalų lygis kontroliniuose taškuose 1,5 m aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-88	-86	-87	-91	-112	-107	-91	-112	-107	-92	-111	-108	-108	-125	-124
Taškas2	-85	-82	-84	-91	-112	-107	-91	-112	-107	-92	-111	-108	-108	-125	-124
Taškas3	-88	-90	-90	-92	-113	-108	-92	-113	-108	-93	-113	-109	-108	-124	-124
Taškas4	-82	-86	-87	-91	-110	-107	-91	-110	-107	-92	-111	-108	-108	-125	-124
Taškas5	-85	-97	-81	-92	-111	-108	-92	-111	-108	-93	-112	-109	-108	-125	-124
Taškas6	-83	-81	-89	-91	-110	-107	-91	-110	-107	-93	-112	-109	-108	-125	-124



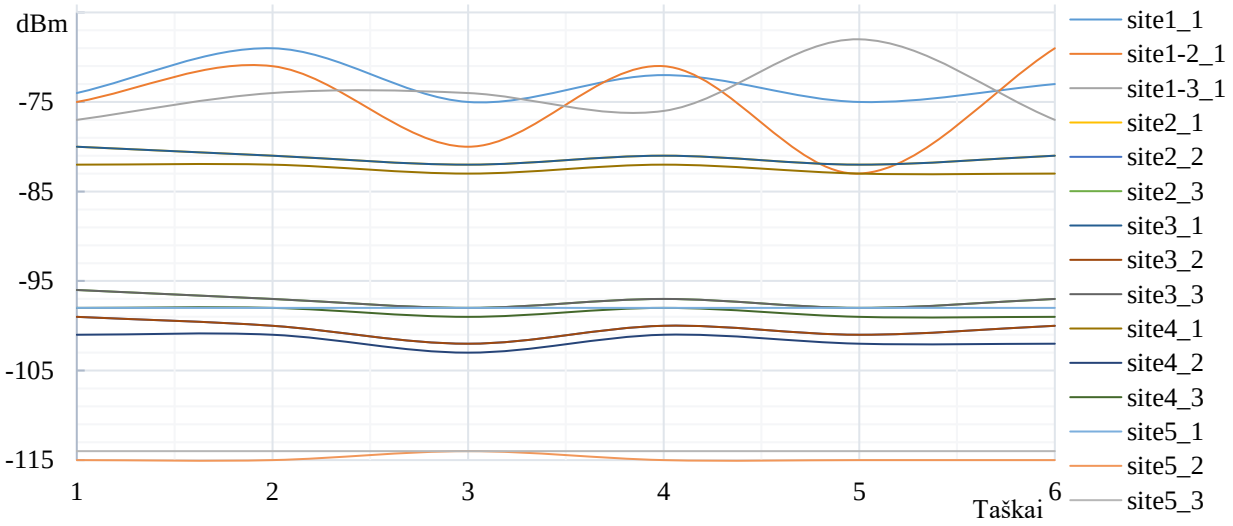
5.18 pav. Signalų lygių kontroliniuose taškuose (1,5 m. aukštyje) diagrama

- Signalo padengimas 5 m. aukštyje:

5.19 pav. Signalo padengimas 5 m. aukštyje

5.10 lentelė. Signalų lygis kontroliniuose taškuose 5 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-74	-75	-77	-80	-99	-96	-80	-99	-96	-82	-101	-98	-98	-115	-114
Taškas2	-69	-71	-74	-81	-100	-97	-81	-100	-97	-82	-101	-98	-98	-115	-114
Taškas3	-75	-80	-74	-82	-102	-98	-82	-102	-98	-83	-103	-99	-98	-114	-114
Taškas4	-72	-71	-76	-81	-100	-97	-81	-100	-97	-82	-101	-98	-98	-115	-114
Taškas5	-75	-83	-68	-82	-101	-98	-82	-101	-98	-83	-102	-99	-98	-115	-114
Taškas6	-73	-69	-77	-81	-100	-97	-81	-100	-97	-83	-102	-99	-98	-115	-114



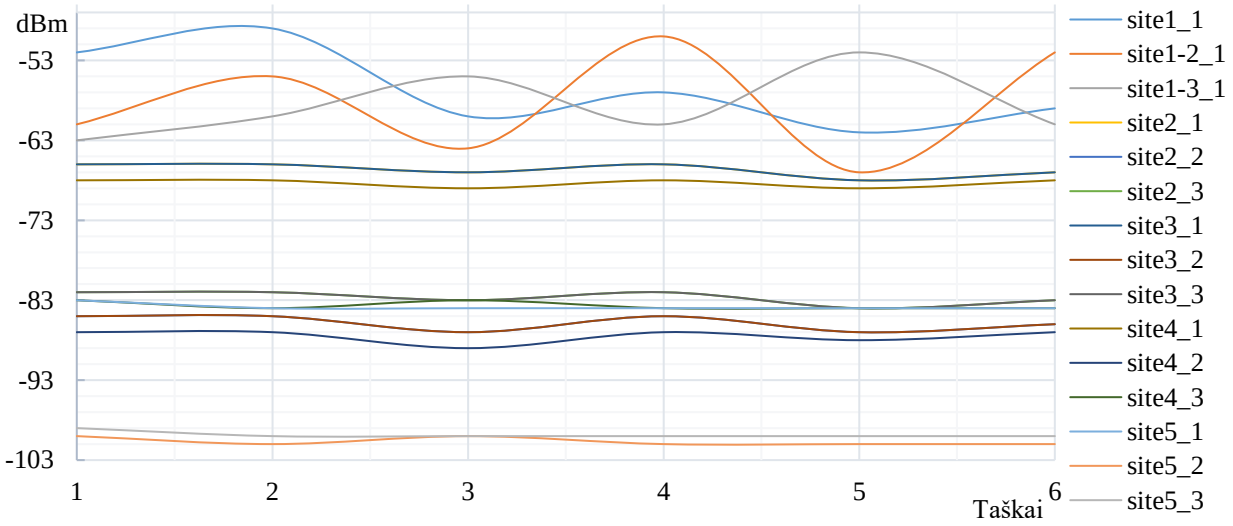
5.20 pav. Signalų lygių kontroliniuose taškuose (5 m. aukštyje) diagrama

- Signalo padengimas 10 m. aukštyje:

5.21 pav. Signalo padengimas 10 m. aukštyje

5.11 lentelė. Signalų lygis kontroliniuose taškuose 10 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2 _1	site2 _2	site2 _3	site3 _1	site3 _2	site3 _3	site4 _1	site4 _2	site4 _3	site5 _1	site5 _2	site5 _3
Taškas1	-52	-61	-63	-66	-85	-82	-66	-85	-82	-68	-87	-83	-83	-100	-99
Taškas2	-49	-55	-60	-66	-85	-82	-66	-85	-82	-68	-87	-84	-84	-101	-100
Taškas3	-60	-64	-55	-67	-87	-83	-67	-87	-83	-69	-89	-83	-84	-100	-100
Taškas4	-57	-50	-61	-66	-85	-82	-66	-85	-82	-68	-87	-84	-84	-101	-100
Taškas5	-62	-67	-52	-68	-87	-84	-68	-87	-84	-69	-88	-84	-84	-101	-100
Taškas6	-59	-52	-61	-67	-86	-83	-67	-86	-83	-68	-87	-84	-84	-101	-100



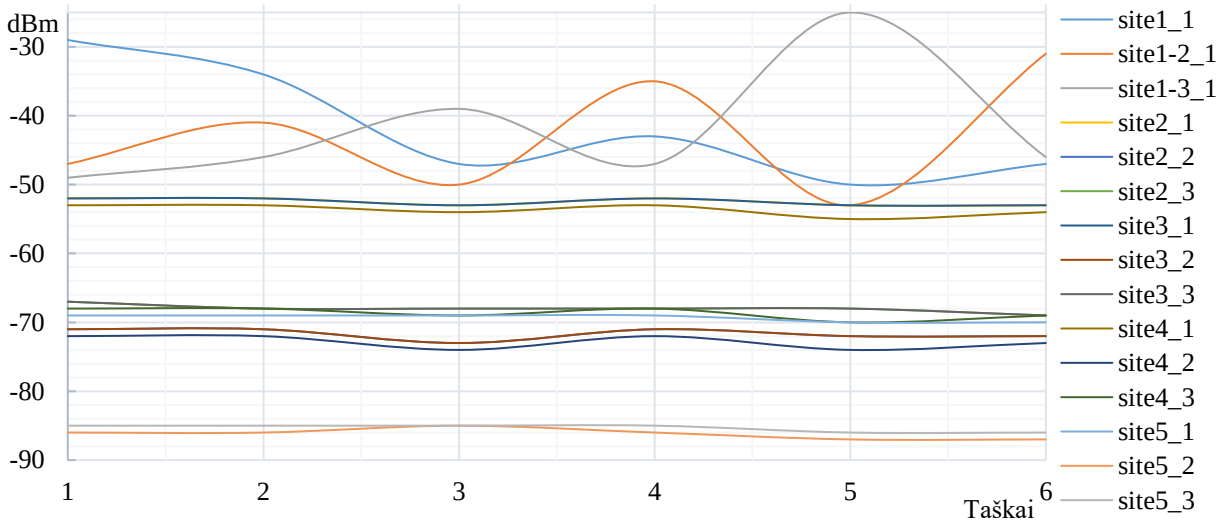
5.22 pav. Signalų lygių kontroliniuose taškuose (10 m. aukštyje) diagrama

- Signalo padengimas 15 m. aukštyje:

5.23 pav. Signalo padengimas 15 m. aukštyje

5.12 lentelė. Signalų lygis kontroliniuose taškuose 15 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2 _1	site2 _2	site2 _3	site3 _1	site3 _2	site3 _3	site4 _1	site4 _2	site4 _3	site5 _1	site5 _2	site5 _3
Taškas1	-29	-47	-49	-52	-71	-67	-52	-71	-67	-53	-72	-68	-69	-86	-85
Taškas2	-34	-41	-46	-52	-71	-68	-52	-71	-68	-53	-72	-68	-69	-86	-85
Taškas3	-47	-50	-39	-53	-73	-68	-53	-73	-68	-54	-74	-69	-69	-85	-85
Taškas4	-43	-35	-47	-52	-71	-68	-52	-71	-68	-53	-72	-68	-69	-86	-85
Taškas5	-50	-53	-25	-53	-72	-68	-53	-72	-68	-55	-74	-70	-70	-87	-86
Taškas6	-47	-31	-46	-53	-72	-69	-53	-72	-69	-54	-73	-69	-70	-87	-86



5.24 pav. Signalų lygių kontroliniuose taškuose (15 m. aukštyje) diagrama

5.1.2. UMTS

Sumodeliavus GSM technologijos signalo padengimą pereita prie UMTS. Pradėta nuo 900 MHz dažnio. Parinkti tokie bazinių stočių siųstuvų parametrai:

- siųstuvo galia: 43 dBm;
- antenos stiprinimas: 17,2 dBi;
- antenos spinduliavimo kampas: 90°.

Optimaliausi IMSI gaudyklių parametrai rasti pasinaudojus 5.1 poskyryje aprašytu algoritmu. Tik IMSI gaudyklių siųstuvų ir antenų skaičius bei išdėstymas teritorijoje nebuvo keičiamas. Galutiniai IMSI gaudyklių parametrai pateikiami 5.13 lentelėje.

5.13 lentelė. IMSI gaudyklių duomenys

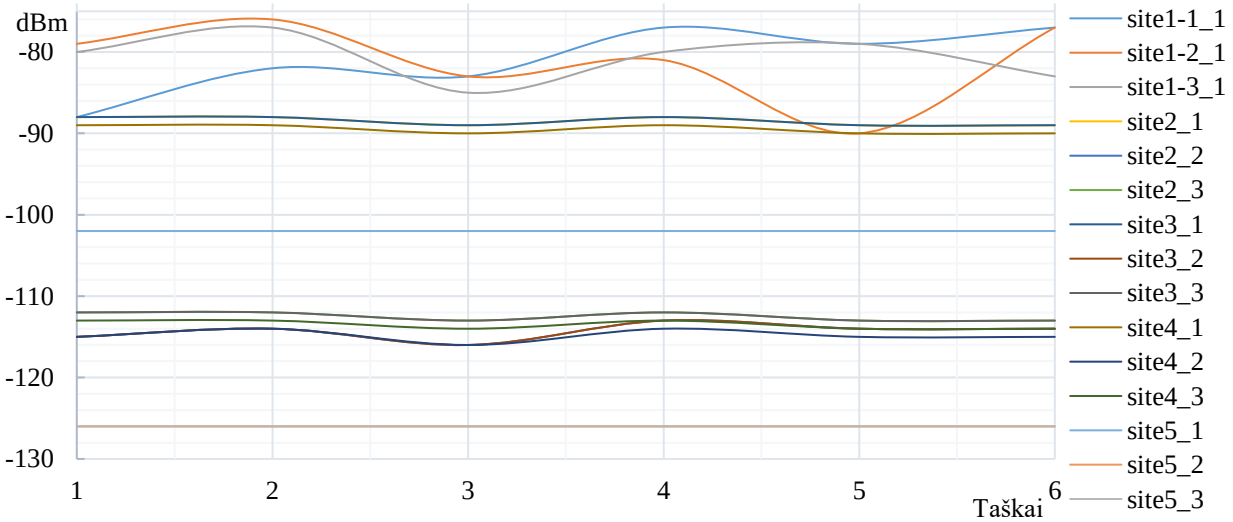
Sektorius	Platuma	Ilguma	Azimutas, °	Palink. kamp., °	Aukštis, m	Siųstuvo galia, dBm	Antenos stiprinimas, dBi
site1-1_1	54° 54' 38,54"	24° 12' 20,44"	353	6,5	17	6	17,2
site1-2_1	54° 54' 43,79"	24° 12' 23,26"	205	3	16	6	17,2
site1-3_1	54° 54' 43,26"	24° 12' 15,03"	135	3,5	16	5,5	17,2

- Signalo padengimas 1,5 m. aukštyje:

5.25 pav. Signalo padengimas 1,5 m. aukštyje

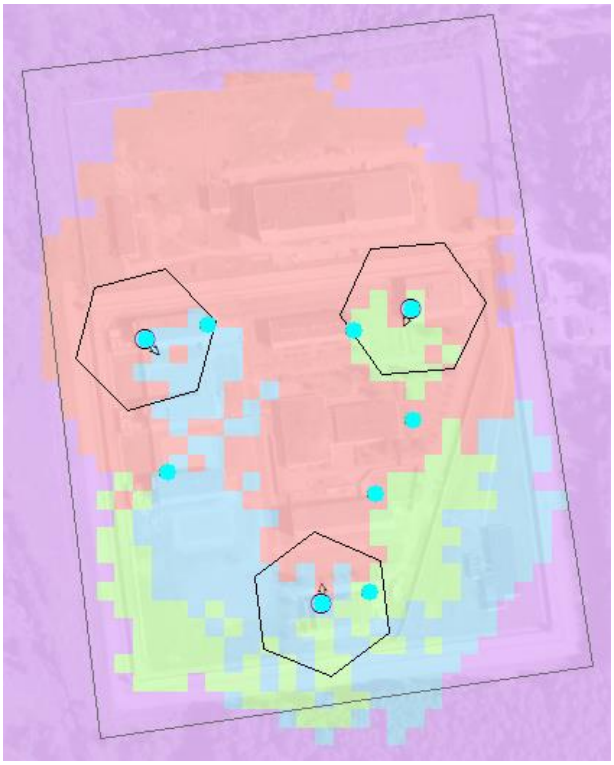
5.14 lentelė. Signalų lygis kontroliniuose taškuose 1,5 m aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-88	-79	-80	-88	-115	-112	-88	-115	-112	-89	-115	-113	-102	-126	-126
Taškas2	-82	-76	-77	-88	-114	-112	-88	-114	-112	-89	-114	-113	-102	-126	-126
Taškas3	-83	-83	-85	-89	-116	-113	-89	-116	-113	-90	-116	-114	-102	-126	-126
Taškas4	-77	-81	-80	-88	-113	-112	-88	-113	-112	-89	-114	-113	-102	-126	-126
Taškas5	-79	-90	-79	-89	-114	-113	-89	-114	-113	-90	-115	-114	-102	-126	-126
Taškas6	-77	-77	-83	-89	-114	-113	-89	-114	-113	-90	-115	-114	-102	-126	-126



5.26 pav. Signalų lygių kontroliniuose taškuose (1,5 m. aukštyje) diagrama

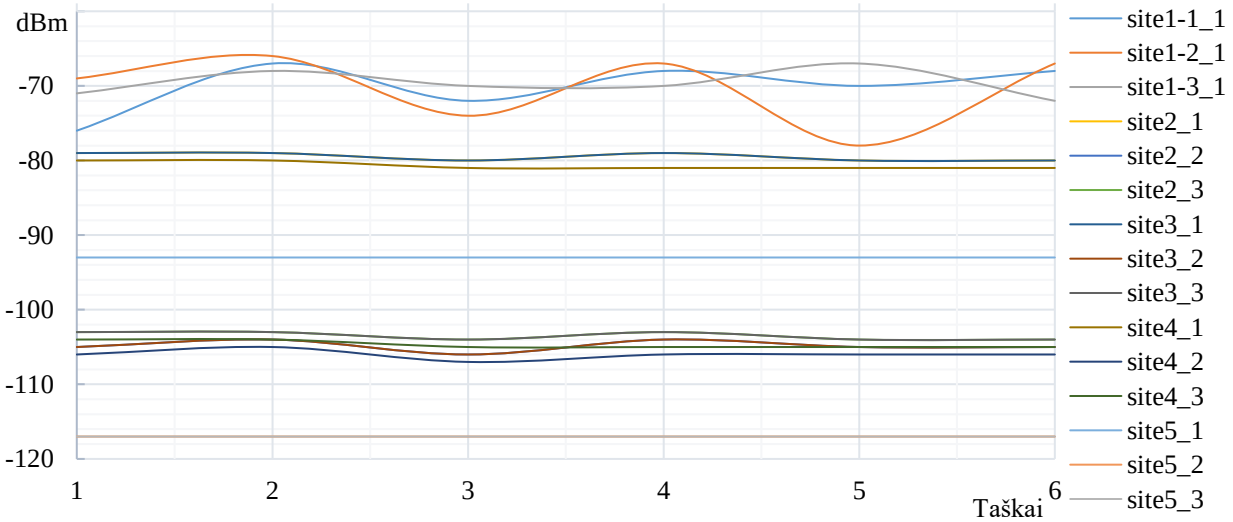
- Signalo padengimas 5 m. aukštyje:



5.27 pav. Signalo padengimas 5 m. aukštyje

5.15 lentelė. Signalų lygis kontroliniuose taškuose 5 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-76	-69	-71	-79	-105	-103	-79	-105	-103	-80	-106	-104	-93	-117	-117
Taškas2	-67	-66	-68	-79	-104	-103	-79	-104	-103	-80	-105	-104	-93	-117	-117
Taškas3	-72	-74	-70	-80	-106	-104	-80	-106	-104	-81	-107	-105	-93	-117	-117
Taškas4	-68	-67	-70	-79	-104	-103	-79	-104	-103	-81	-106	-105	-93	-117	-117
Taškas5	-70	-78	-67	-80	-105	-104	-80	-105	-104	-81	-106	-105	-93	-117	-117
Taškas6	-68	-67	-72	-80	-105	-104	-80	-105	-104	-81	-106	-105	-93	-117	-117



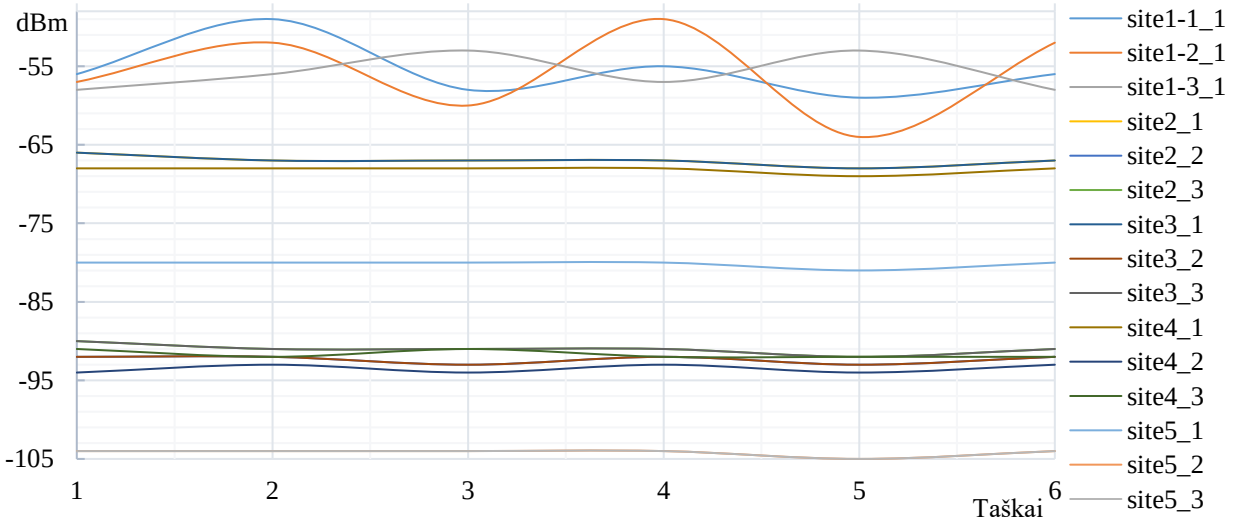
5.28 pav. Signalų lygių kontroliniuose taškuose (5 m. aukštyje) diagrama

- Signalo padengimas 10 m. aukštyje:

5.29 pav. Signalo padengimas 10 m. aukštyje

5.16 lentelė. Signalų lygis kontroliniuose taškuose 10 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-56	-57	-58	-66	-92	-90	-66	-92	-90	-68	-94	-91	-80	-104	-104
Taškas2	-49	-52	-56	-67	-92	-91	-67	-92	-91	-68	-93	-92	-80	-104	-104
Taškas3	-58	-60	-53	-67	-93	-91	-67	-93	-91	-68	-94	-91	-80	-104	-104
Taškas4	-55	-49	-57	-67	-92	-91	-67	-92	-91	-68	-93	-92	-80	-104	-104
Taškas5	-59	-64	-53	-68	-93	-92	-68	-93	-92	-69	-94	-92	-81	-105	-105
Taškas6	-56	-52	-58	-67	-92	-91	-67	-92	-91	-68	-93	-92	-80	-104	-104



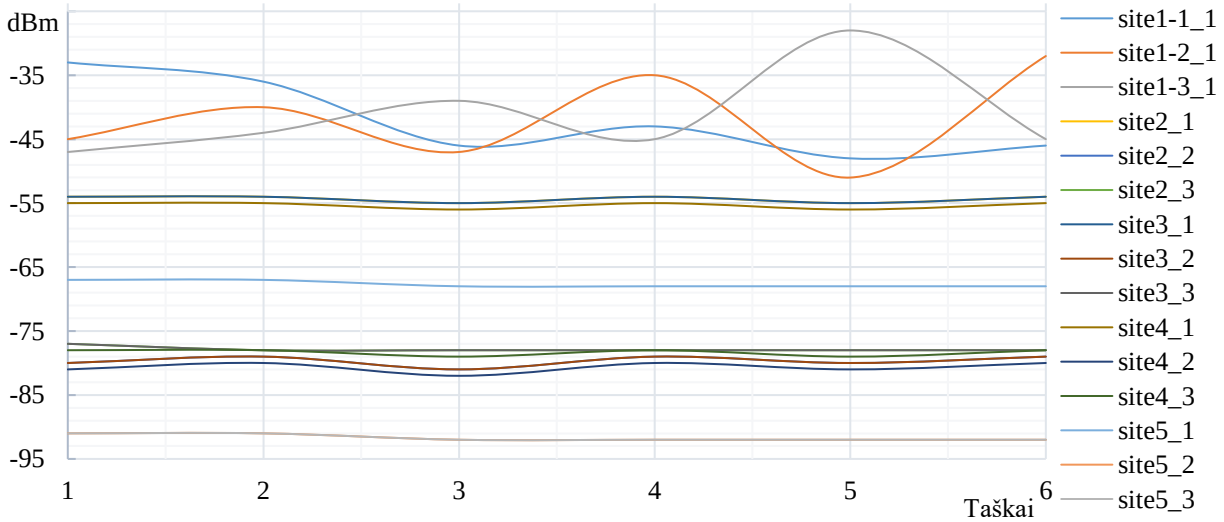
5.30 pav. Signalų lygių kontroliniuose taškuose (10 m. aukštyje) diagrama

- Signalo padengimas 15 m. aukštyje:

5.31 pav. Signalo padengimas 15 m. aukštyje

5.17 lentelė. Signalų lygis kontroliniuose taškuose 15 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-33	-45	-47	-54	-80	-77	-54	-80	-77	-55	-81	-78	-67	-91	-91
Taškas2	-36	-40	-44	-54	-79	-78	-54	-79	-78	-55	-80	-78	-67	-91	-91
Taškas3	-46	-47	-39	-55	-81	-78	-55	-81	-78	-56	-82	-79	-68	-92	-92
Taškas4	-43	-35	-45	-54	-79	-78	-54	-79	-78	-55	-80	-78	-68	-92	-92
Taškas5	-48	-51	-28	-55	-80	-78	-55	-80	-78	-56	-81	-79	-68	-92	-92
Taškas6	-46	-32	-45	-54	-79	-78	-54	-79	-78	-55	-80	-78	-68	-92	-92



5.32 pav. Signalų lygių kontroliniuose taškuose (15 m. aukštyje) diagrama

Toliau modeliuojamas 2100 MHz dažnio signalų padengimas. Parinkti tokie bazinių stočių siųstuvų parametrai:

- siųstuvo galia: 43 dBm;
- antenos stiprinimas: 16,4 dBi;
- antenos spinduliavimo kampas: 90°.

Minimaliai pakoregavus IMSI gaudyklių siųstuvų galias, buvo gautas geriausias signalo padengimas visuose aukščiuose: 1,5 m., 5 m., 10 m. ir 15 m.

5.18 lentelė. IMSI gaudyklių duomenys

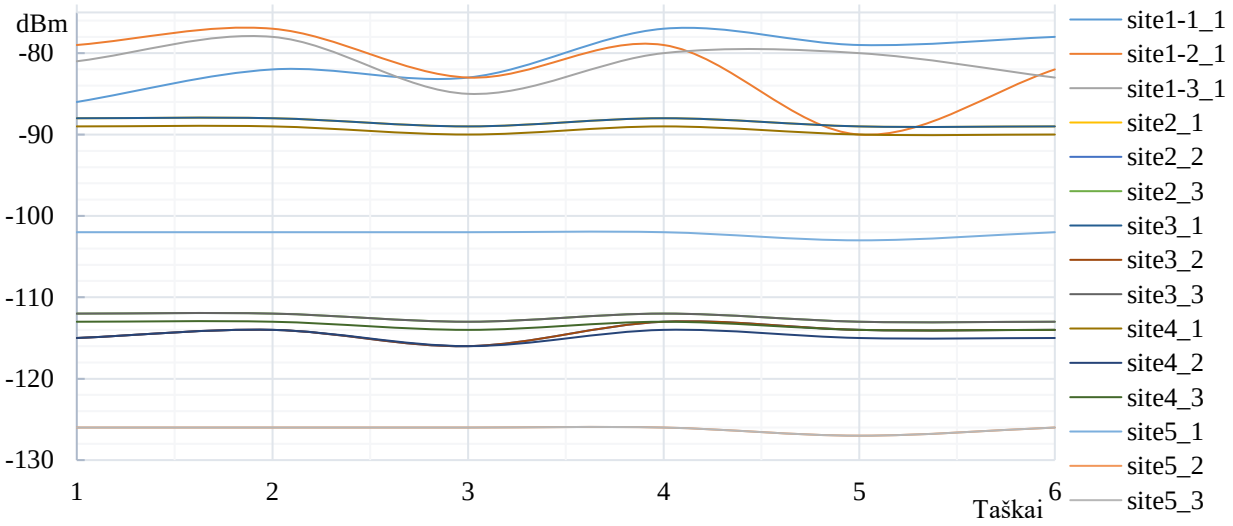
Sektorius	Platuma	Ilguma	Azimutas, °	Palink. kamp., °	Aukštis, m	Siųstuvo galia, dBm	Antenos stiprinimas, dBi
site1_1	54° 54' 38,54"	24° 12' 20,44"	353	6,5	17	5,3	16,4
site1-2_1	54° 54' 43,79"	24° 12' 23,26"	205	3	16	5,3	16,4
site1-3_1	54° 54' 43,26"	24° 12' 15,03"	135	3,5	16	4,7	16,4

- Signalo padengimas 1,5 m. aukštyje:

5.33 pav. Signalo padengimas 1,5 m. aukštyje

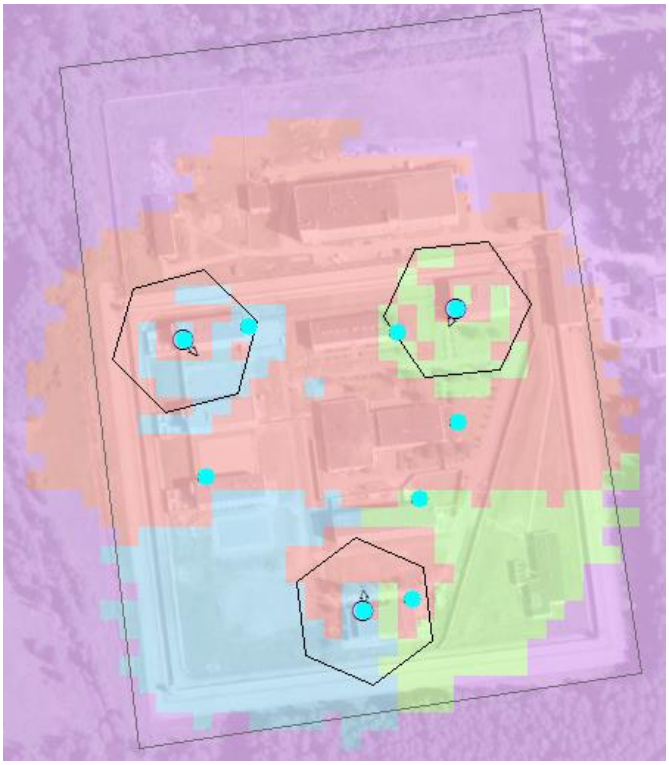
5.19 lentelė. Signalų lygis kontroliniuose taškuose 1,5 m aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-86	-79	-81	-88	-115	-112	-88	-115	-112	-89	-115	-113	-102	-126	-126
Taškas2	-82	-77	-78	-88	-114	-112	-88	-114	-112	-89	-114	-113	-102	-126	-126
Taškas3	-83	-83	-85	-89	-116	-113	-89	-116	-113	-90	-116	-114	-102	-126	-126
Taškas4	-77	-79	-80	-88	-113	-112	-88	-113	-112	-89	-114	-113	-102	-126	-126
Taškas5	-79	-90	-80	-89	-114	-113	-89	-114	-113	-90	-115	-114	-103	-127	-127
Taškas6	-78	-82	-83	-89	-114	-113	-89	-114	-113	-90	-115	-114	-102	-126	-126



5.34 pav. Signalų lygių kontroliniuose taškuose (1,5 m. aukštyje) diagrama

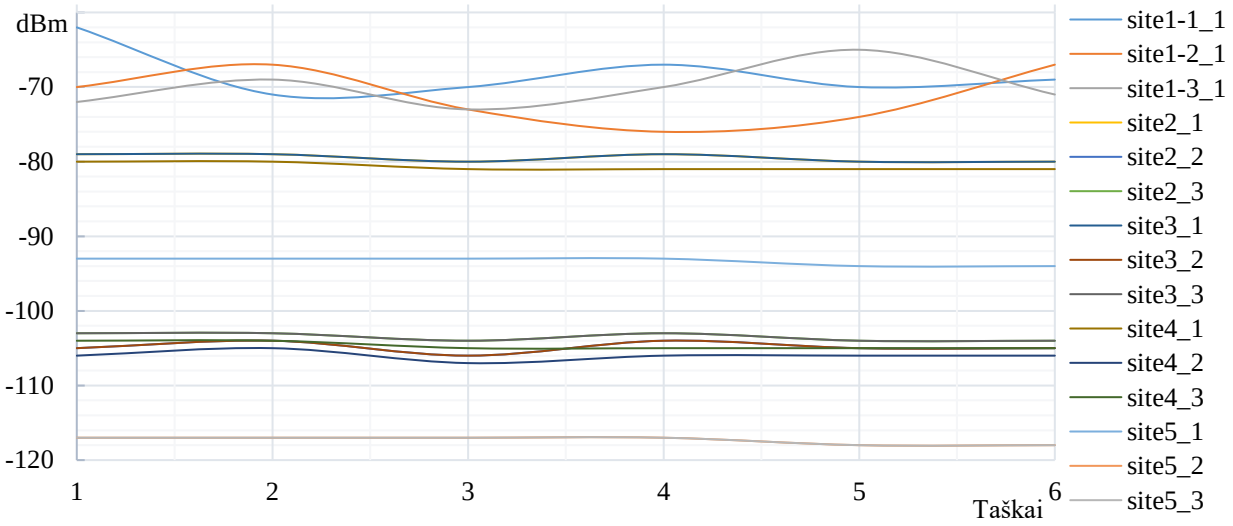
- Signalo padengimas 5 m. aukštyje:



5.35 pav. Signalo padengimas 5 m. aukštyje

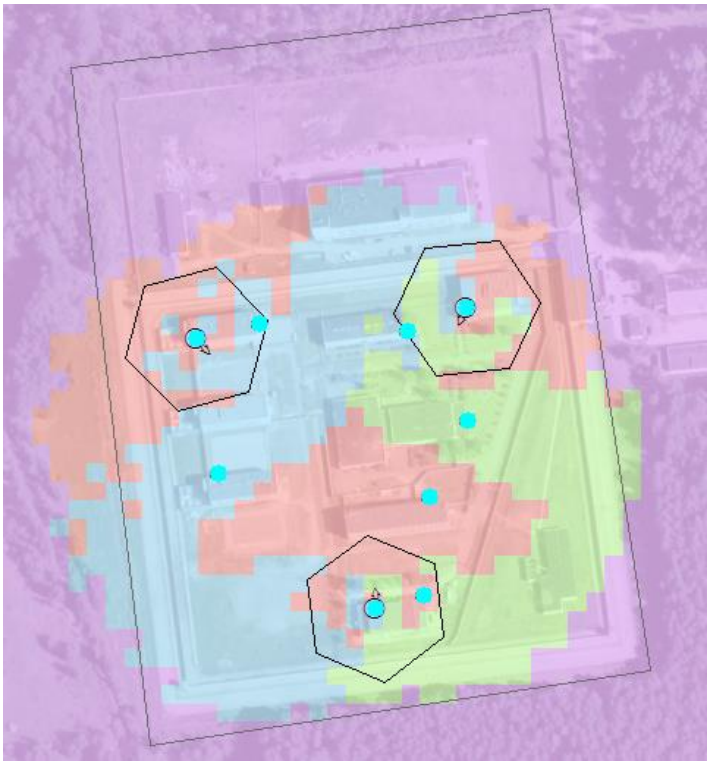
5.20 lentelė. Signalų lygis kontroliniuose taškuose 5 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-62	-70	-72	-79	-105	-103	-79	-105	-103	-80	-106	-104	-93	-117	-117
Taškas2	-71	-67	-69	-79	-104	-103	-79	-104	-103	-80	-105	-104	-93	-117	-117
Taškas3	-70	-73	-73	-80	-106	-104	-80	-106	-104	-81	-107	-105	-93	-117	-117
Taškas4	-67	-76	-70	-79	-104	-103	-79	-104	-103	-81	-106	-105	-93	-117	-117
Taškas5	-70	-74	-65	-80	-105	-104	-80	-105	-104	-81	-106	-105	-94	-118	-118
Taškas6	-69	-67	-71	-80	-105	-104	-80	-105	-104	-81	-106	-105	-94	-118	-118



5.36 pav. Signalų lygių kontroliniuose taškuose (5 m. aukštyje) diagrama

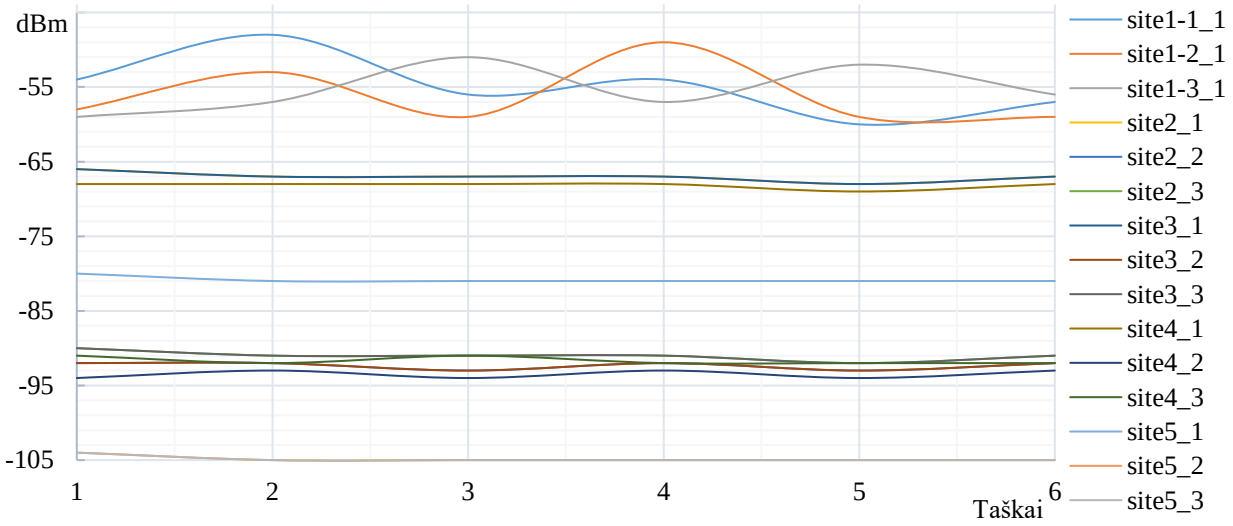
- Signalo padengimas 10 m. aukštyje:



5.37 pav. Signalo padengimas 10 m. aukštyje

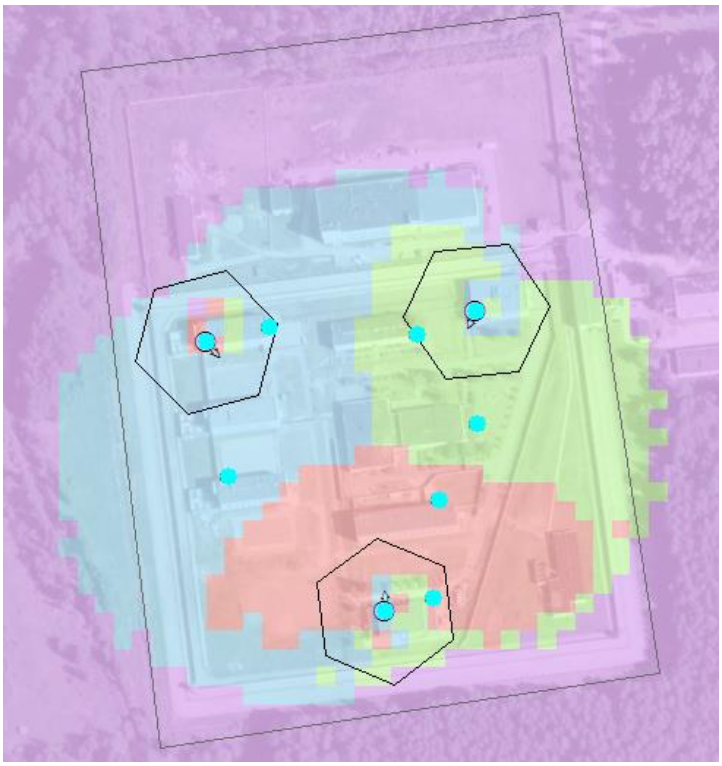
5.21 lentelė. Signalų lygis kontroliniuose taškuose 10 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-54	-58	-59	-66	-92	-90	-66	-92	-90	-68	-94	-91	-80	-104	-104
Taškas2	-48	-53	-57	-67	-92	-91	-67	-92	-91	-68	-93	-92	-81	-105	-105
Taškas3	-56	-59	-51	-67	-93	-91	-67	-93	-91	-68	-94	-91	-81	-105	-105
Taškas4	-54	-49	-57	-67	-92	-91	-67	-92	-91	-68	-93	-92	-81	-105	-105
Taškas5	-60	-59	-52	-68	-93	-92	-68	-93	-92	-69	-94	-92	-81	-105	-105
Taškas6	-57	-59	-56	-67	-92	-91	-67	-92	-91	-68	-93	-92	-81	-105	-105



5.38 pav. Signalų lygių kontroliniuose taškuose (10 m. aukštyje) diagrama

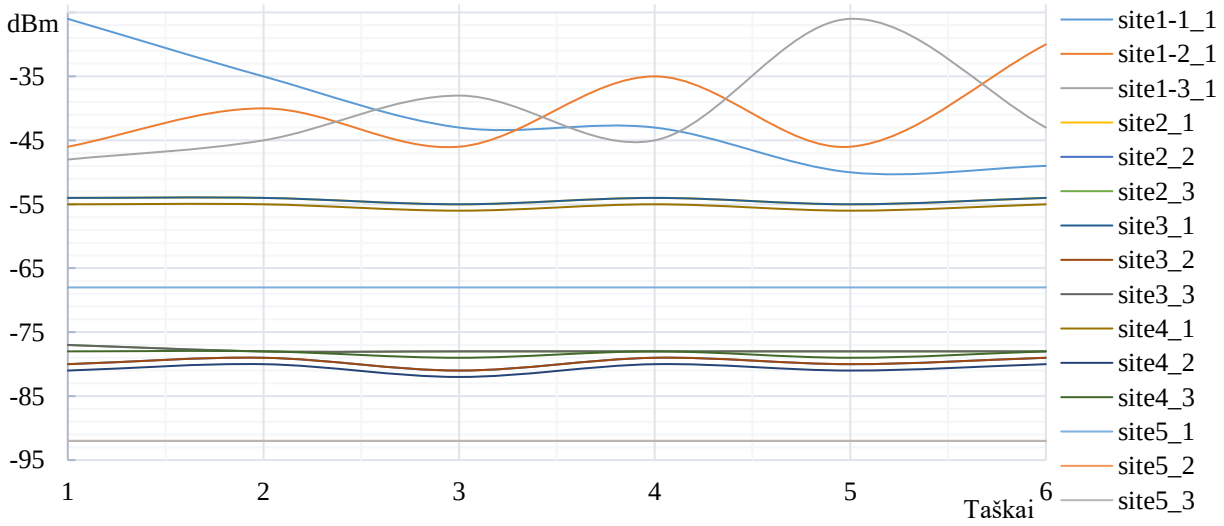
- Signalo padengimas 15 m. aukštyje:



5.39 pav. Signalo padengimas 15 m. aukštyje

5.22 lentelė. Signalų lygis kontroliniuose taškuose 15 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-26	-46	-48	-54	-80	-77	-54	-80	-77	-55	-81	-78	-68	-92	-92
Taškas2	-35	-40	-45	-54	-79	-78	-54	-79	-78	-55	-80	-78	-68	-92	-92
Taškas3	-43	-46	-38	-55	-81	-78	-55	-81	-78	-56	-82	-79	-68	-92	-92
Taškas4	-43	-35	-45	-54	-79	-78	-54	-79	-78	-55	-80	-78	-68	-92	-92
Taškas5	-50	-46	-26	-55	-80	-78	-55	-80	-78	-56	-81	-79	-68	-92	-92
Taškas6	-49	-30	-43	-54	-79	-78	-54	-79	-78	-55	-80	-78	-68	-92	-92



5.40 pav. Signalų lygių kontroliniuose taškuose (15 m. aukštyje) diagrama

5.1.3. LTE

Nors dar nėra daug komercinių IMSI gaudyklių, kurių gamintojai deklaruoja, kad jos veikia LTE technologijoje, tačiau vis didėjantis LTE naudojimas ir technologijoje esančios saugumo spragos įtakos tokių įrenginių pasiūlos didėjimą ateityje. Dėl šios priežasties aktualus yra ir LTE signalo padengimo skaičiavimas. Modeliavimas pradėtas nuo 800 MHz dažnio. Parinkti tokie bazinių stočių siųstuvų parametrai:

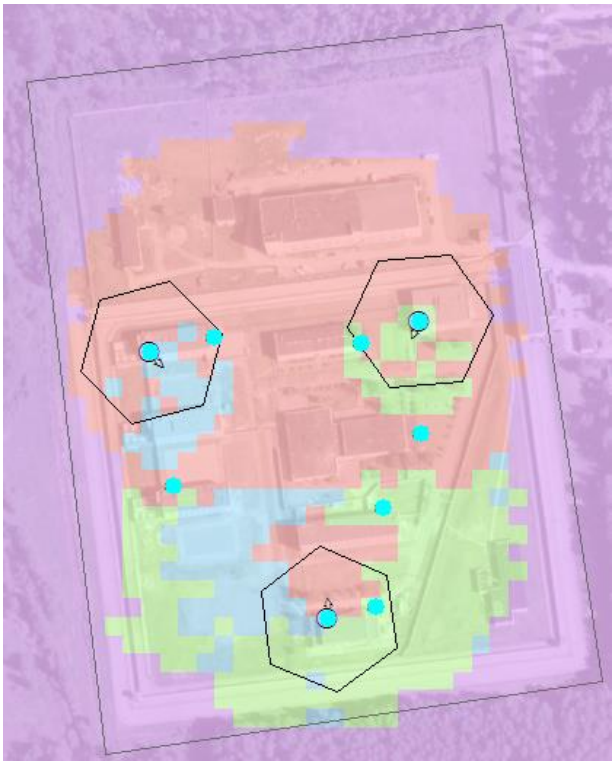
- siųstuvo galia: 43 dBm;
- antenos stiprinimas: 17,2 dBi;
- antenos spinduliavimo kampas: 90°.

Optimaliausi IMSI gaudyklių parametrai rasti pasinaudojus 5.1 poskyryje aprašytu algoritmu. Tik IMSI gaudyklių siųstuvų ir antenų skaičius bei išdėstymas teritorijoje nebuvo keičiamas. Galutiniai IMSI gaudyklių parametrai pateikiami 5.23 lentelėje.

5.23 lentelė. IMSI gaudyklių duomenys

Sektorius	Platuma	Ilguma	Azimutas, °	Palink. kamp., °	Aukštis, m	Siųstuvo galia, dBm	Antenos stiprinimas, dBi
site1_1	54° 54' 38,54"	24° 12' 20,44"	353	6,5	17	6	17,2
site1-2_1	54° 54' 43,79"	24° 12' 23,26"	205	3	16	6	17,2
site1-3_1	54° 54' 43,26"	24° 12' 15,03"	135	3,5	16	5,7	17,2

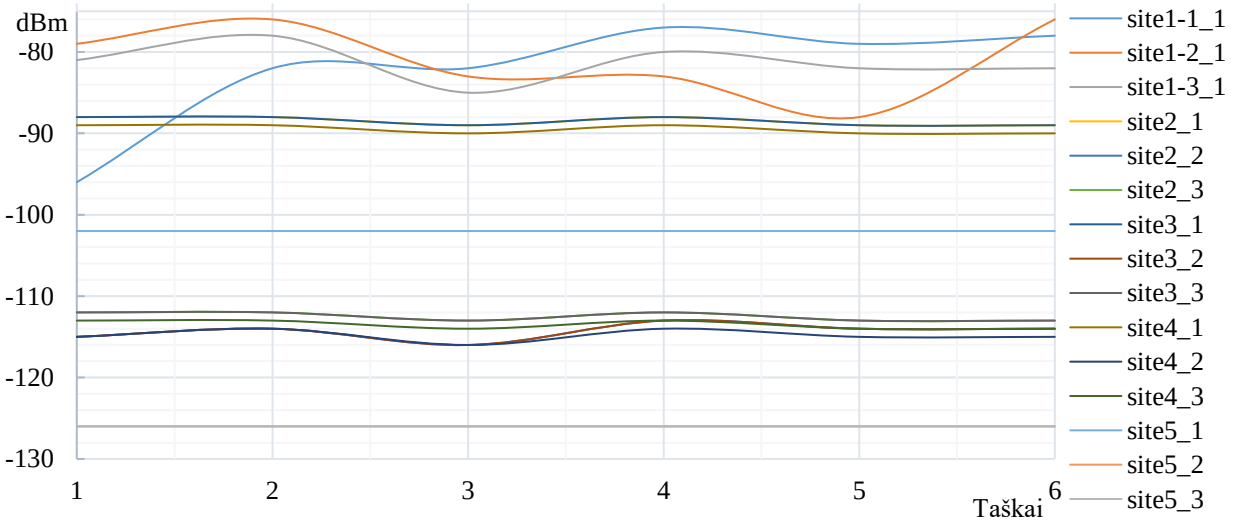
- Signalo padengimas 1,5 m. aukštyje:



5.41 pav. Signalo padengimas 1,5 m. aukštyje

5.24 lentelė. Signalų lygis kontroliniuose taškuose 1,5 m aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-96	-79	-81	-88	-115	-112	-88	-115	-112	-89	-115	-113	-102	-126	-126
Taškas2	-82	-76	-78	-88	-114	-112	-88	-114	-112	-89	-114	-113	-102	-126	-126
Taškas3	-82	-83	-85	-89	-116	-113	-89	-116	-113	-90	-116	-114	-102	-126	-126
Taškas4	-77	-83	-80	-88	-113	-112	-88	-113	-112	-89	-114	-113	-102	-126	-126
Taškas5	-79	-88	-82	-89	-114	-113	-89	-114	-113	-90	-115	-114	-102	-126	-126
Taškas6	-78	-76	-82	-89	-114	-113	-89	-114	-113	-90	-115	-114	-102	-126	-126



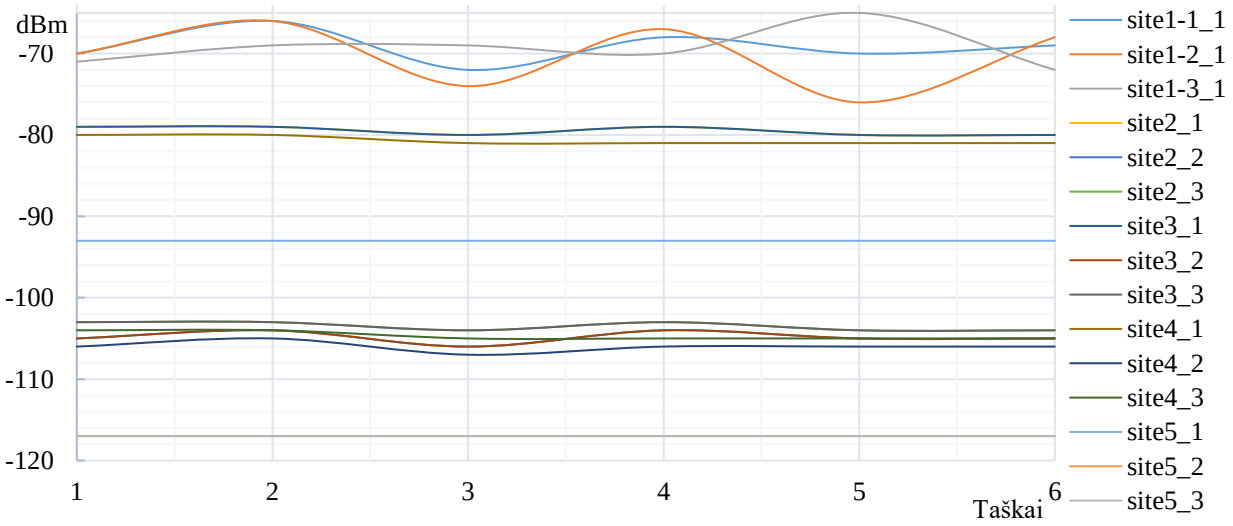
5.42 pav. Signalų lygių kontroliniuose taškuose (1,5 m. aukštyje) diagrama

- Signalo padengimas 5 m. aukštyje:

5.43 pav. Signalo padengimas 5 m. aukštyje

5.25 lentelė. Signalų lygis kontroliniuose taškuose 5 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-70	-70	-71	-79	-105	-103	-79	-105	-103	-80	-106	-104	-93	-117	-117
Taškas2	-66	-66	-69	-79	-104	-103	-79	-104	-103	-80	-105	-104	-93	-117	-117
Taškas3	-72	-74	-69	-80	-106	-104	-80	-106	-104	-81	-107	-105	-93	-117	-117
Taškas4	-68	-67	-70	-79	-104	-103	-79	-104	-103	-81	-106	-105	-93	-117	-117
Taškas5	-70	-76	-65	-80	-105	-104	-80	-105	-104	-81	-106	-105	-93	-117	-117
Taškas6	-69	-68	-72	-80	-105	-104	-80	-105	-104	-81	-106	-105	-93	-117	-117



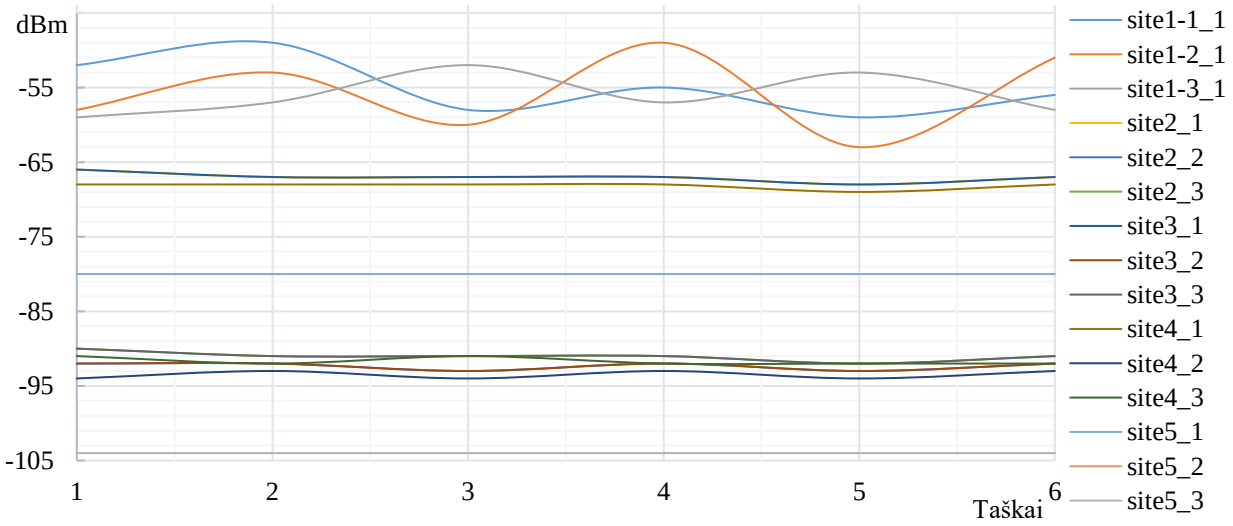
5.44 pav. Signalų lygių kontroliniuose taškuose (5 m. aukštyje) diagrama

- Signalo padengimas 10 m. aukštyje:

5.45 pav. Signalo padengimas 10 m. aukštyje

5.26 lentelė. Signalų lygis kontroliniuose taškuose 10 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-52	-58	-59	-66	-92	-90	-66	-92	-90	-68	-94	-91	-80	-104	-104
Taškas2	-49	-53	-57	-67	-92	-91	-67	-92	-91	-68	-93	-92	-80	-104	-104
Taškas3	-58	-60	-52	-67	-93	-91	-67	-93	-91	-68	-94	-91	-80	-104	-104
Taškas4	-55	-49	-57	-67	-92	-91	-67	-92	-91	-68	-93	-92	-80	-104	-104
Taškas5	-59	-63	-53	-68	-93	-92	-68	-93	-92	-69	-94	-92	-80	-104	-104
Taškas6	-56	-51	-58	-67	-92	-91	-67	-92	-91	-68	-93	-92	-80	-104	-104



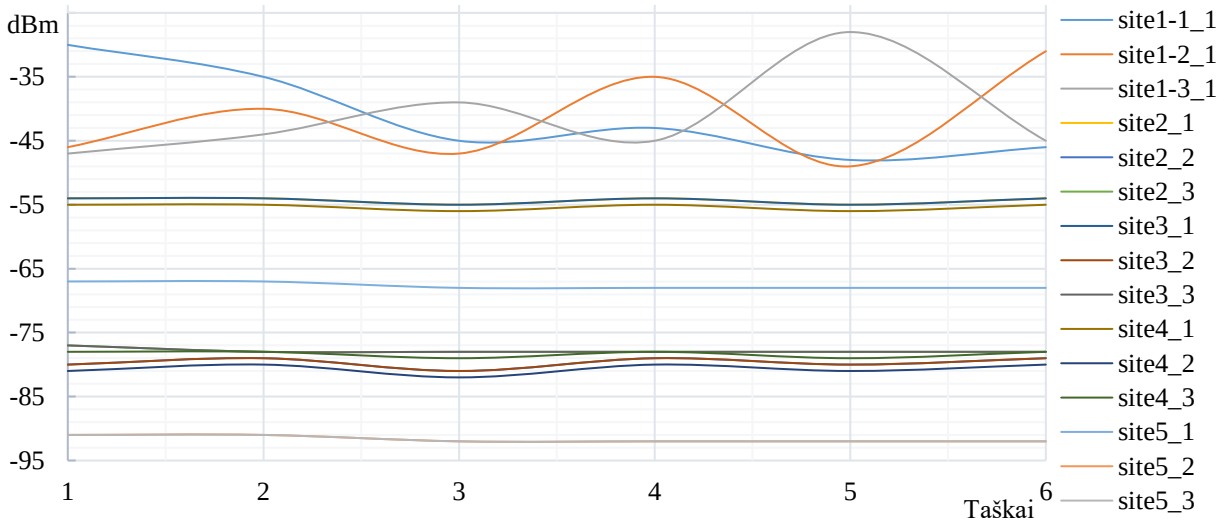
5.46 pav. Signalų lygių kontroliniuose taškuose (10 m. aukštyje) diagrama

- Signalo padengimas 15 m. aukštyje:

5.47 pav. Signalo padengimas 15 m. aukštyje

5.27 lentelė. Signalų lygis kontroliniuose taškuose 15 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-30	-46	-47	-54	-80	-77	-54	-80	-77	-55	-81	-78	-67	-91	-91
Taškas2	-35	-40	-44	-54	-79	-78	-54	-79	-78	-55	-80	-78	-67	-91	-91
Taškas3	-45	-47	-39	-55	-81	-78	-55	-81	-78	-56	-82	-79	-68	-92	-92
Taškas4	-43	-35	-45	-54	-79	-78	-54	-79	-78	-55	-80	-78	-68	-92	-92
Taškas5	-48	-49	-28	-55	-80	-78	-55	-80	-78	-56	-81	-79	-68	-92	-92
Taškas6	-46	-31	-45	-54	-79	-78	-54	-79	-78	-55	-80	-78	-68	-92	-92



5.48 pav. Signalų lygių kontroliniuose taškuose (15 m. aukštyje) diagrama

Toliau modeliuojamas 1800 MHz dažnio signalų padengimas. Parinkti tokie bazinių stočių siųstuvų parametrai:

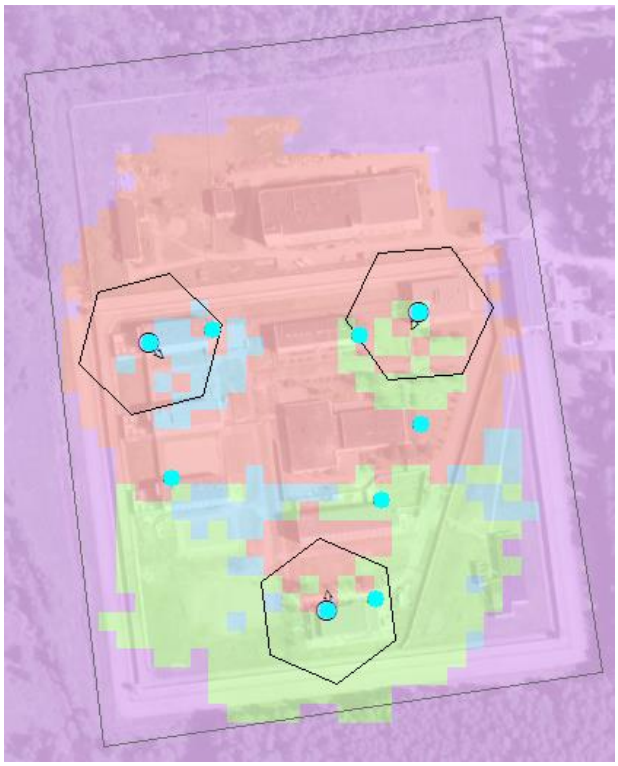
- siųstuvo galia: 43 dBm;
- antenos stiprinimas: 16,4 dBi;
- antenos spinduliavimo kampas: 90°.

Minimaliai pakoregavus IMSI gaudyklių siųstuvų galias, buvo gautas optimalus signalo padengimas visuose aukščiuose: 1,5 m., 5 m., 10 m. ir 15 m.

5.28 lentelė. IMSI gaudyklių duomenys

Sektorius	Platuma	Ilguma	Azimutas, °	Palink. kamp., °	Aukštis, m	Siųstuvo galia, dBm	Antenos stiprinimas, dBi
site1_1	54° 54' 38,54"	24° 12' 20,44"	353	6,5	17	5,1	16,4
site1-2_1	54° 54' 43,79"	24° 12' 23,26"	205	3	16	5,1	16,4
site1-3_1	54° 54' 43,26"	24° 12' 15,03"	135	3,5	16	4,6	16,4

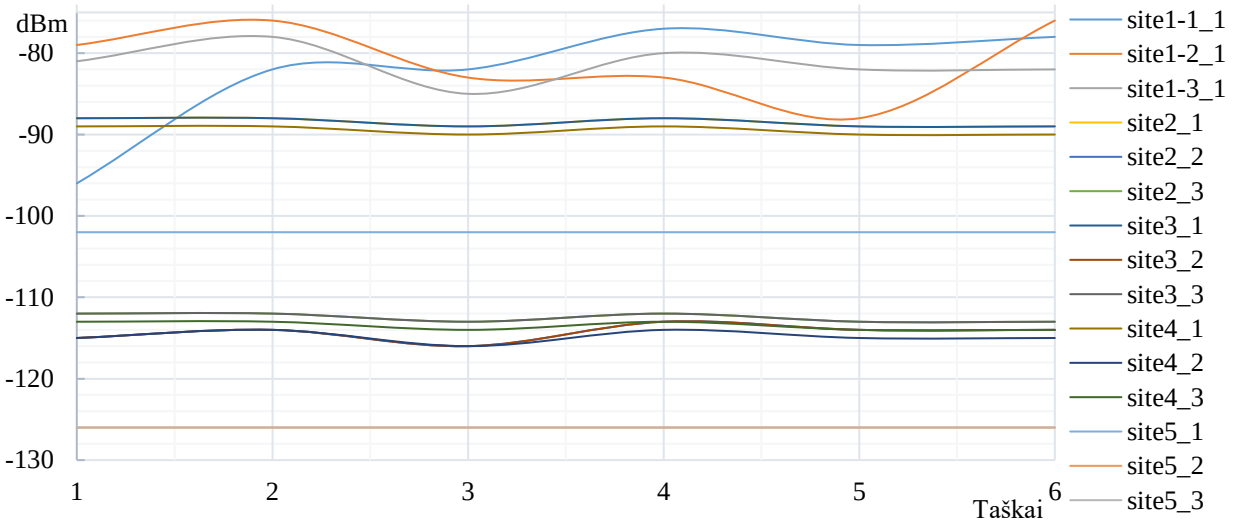
- Signalo padengimas 1,5 m. aukštyje:



5.49 pav. Signalo padengimas 1,5 m. aukštyje

5.29 lentelė. Signalų lygis kontroliniuose taškuose 1,5 m aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-96	-79	-81	-88	-115	-112	-88	-115	-112	-89	-115	-113	-102	-126	-126
Taškas2	-82	-76	-78	-88	-114	-112	-88	-114	-112	-89	-114	-113	-102	-126	-126
Taškas3	-82	-83	-85	-89	-116	-113	-89	-116	-113	-90	-116	-114	-102	-126	-126
Taškas4	-77	-83	-80	-88	-113	-112	-88	-113	-112	-89	-114	-113	-102	-126	-126
Taškas5	-79	-88	-82	-89	-114	-113	-89	-114	-113	-90	-115	-114	-102	-126	-126
Taškas6	-78	-76	-82	-89	-114	-113	-89	-114	-113	-90	-115	-114	-102	-126	-126



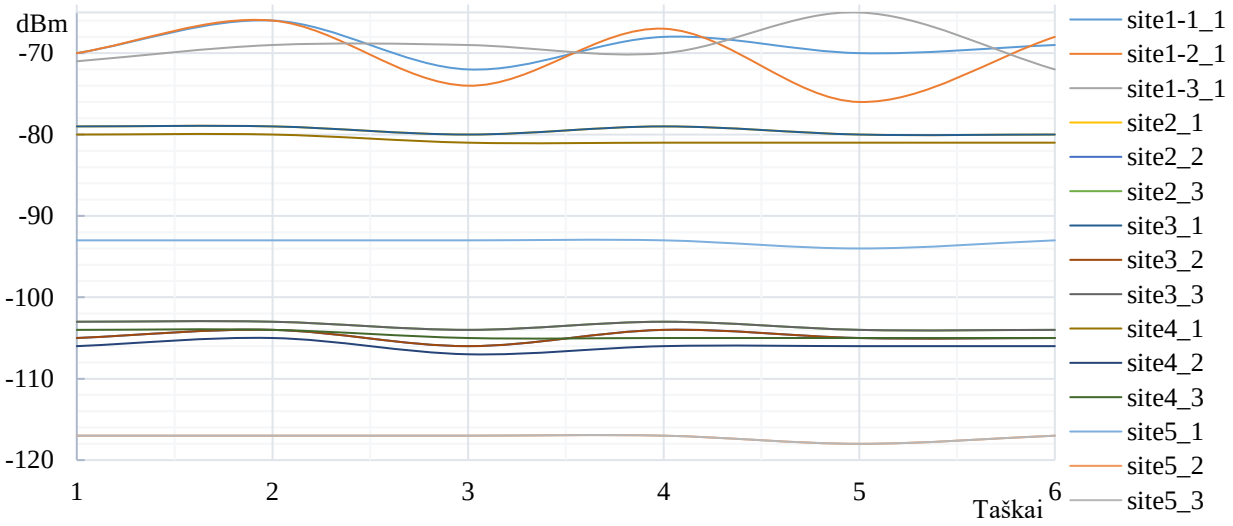
5.50 pav. Signalų lygių kontroliniuose taškuose (1,5 m. aukštyje) diagrama

- Signalo padengimas 5 m. aukštyje:

5.51 pav. Signalo padengimas 5 m. aukštyje

5.30 lentelė. Signalų lygis kontroliniuose taškuose 5 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-70	-70	-71	-79	-105	-103	-79	-105	-103	-80	-106	-104	-93	-117	-117
Taškas2	-66	-66	-69	-79	-104	-103	-79	-104	-103	-80	-105	-104	-93	-117	-117
Taškas3	-72	-74	-69	-80	-106	-104	-80	-106	-104	-81	-107	-105	-93	-117	-117
Taškas4	-68	-67	-70	-79	-104	-103	-79	-104	-103	-81	-106	-105	-93	-117	-117
Taškas5	-70	-76	-65	-80	-105	-104	-80	-105	-104	-81	-106	-105	-94	-118	-118
Taškas6	-69	-68	-72	-80	-105	-104	-80	-105	-104	-81	-106	-105	-93	-117	-117



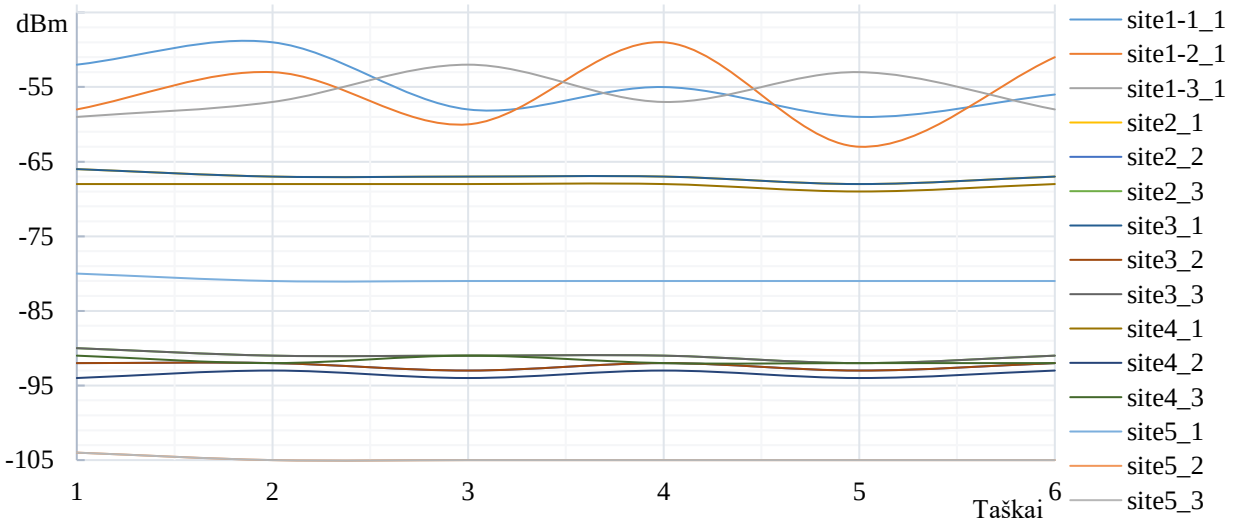
5.52 pav. Signalų lygių kontroliniuose taškuose (5 m. aukštyje) diagrama

- Signalo padengimas 10 m. aukštyje:

5.53 pav. Signalo padengimas 10 m. aukštyje

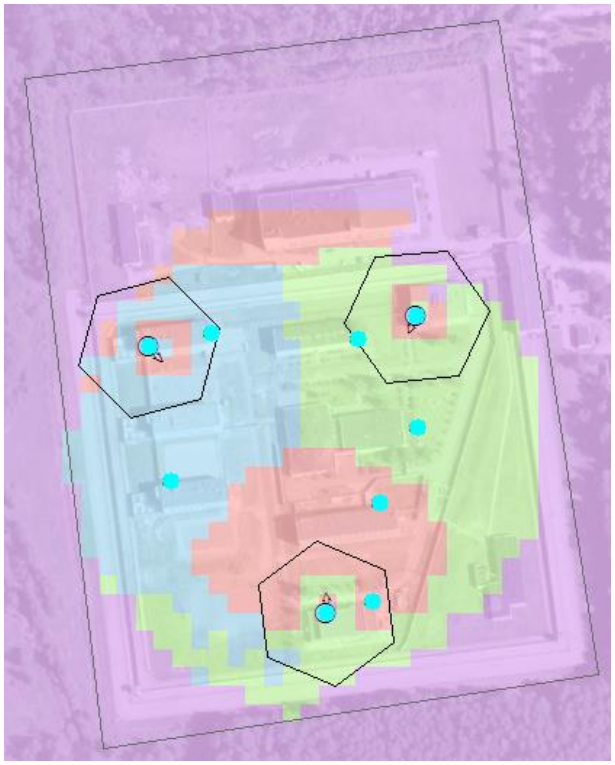
5.31 lentelė. Signalų lygis kontroliniuose taškuose 10 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-52	-58	-59	-66	-92	-90	-66	-92	-90	-68	-94	-91	-80	-104	-104
Taškas2	-49	-53	-57	-67	-92	-91	-67	-92	-91	-68	-93	-92	-81	-105	-105
Taškas3	-58	-60	-52	-67	-93	-91	-67	-93	-91	-68	-94	-91	-81	-105	-105
Taškas4	-55	-49	-57	-67	-92	-91	-67	-92	-91	-68	-93	-92	-81	-105	-105
Taškas5	-59	-63	-53	-68	-93	-92	-68	-93	-92	-69	-94	-92	-81	-105	-105
Taškas6	-56	-51	-58	-67	-92	-91	-67	-92	-91	-68	-93	-92	-81	-105	-105



5.54 pav. Signalų lygių kontroliniuose taškuose (10 m. aukštyje) diagrama

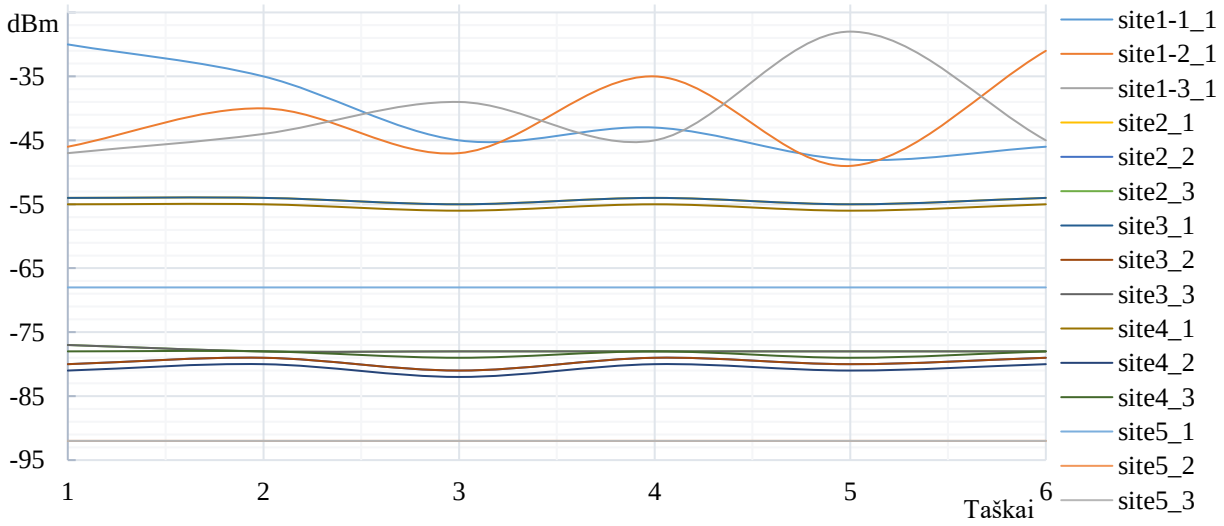
- Signalo padengimas 15 m. aukštyje:



5.55 pav. Signalo padengimas 15 m. aukštyje

5.32 lentelė. Signalų lygis kontroliniuose taškuose 15 m. aukštyje

	site 1-1_1	site 1-2_1	site 1-3_1	site2_1	site2_2	site2_3	site3_1	site3_2	site3_3	site4_1	site4_2	site4_3	site5_1	site5_2	site5_3
Taškas1	-30	-46	-47	-54	-80	-77	-54	-80	-77	-55	-81	-78	-68	-92	-92
Taškas2	-35	-40	-44	-54	-79	-78	-54	-79	-78	-55	-80	-78	-68	-92	-92
Taškas3	-45	-47	-39	-55	-81	-78	-55	-81	-78	-56	-82	-79	-68	-92	-92
Taškas4	-43	-35	-45	-54	-79	-78	-54	-79	-78	-55	-80	-78	-68	-92	-92
Taškas5	-48	-49	-28	-55	-80	-78	-55	-80	-78	-56	-81	-79	-68	-92	-92
Taškas6	-46	-31	-45	-54	-79	-78	-54	-79	-78	-55	-80	-78	-68	-92	-92



5.56 pav. Signalų lygių kontroliniuose taškuose (15 m. aukštyje) diagrama

5.2. IMSI gaudyklių atpažinimo požymiai

IMSI gaudyklių projektavimo ir gaminimo specifika nuo pat jų išradimo bei patentavimo pradžios buvo laikoma komercine paslaptimi arba slepiama saugumo sumetimais, todėl nėra viešai prieinamos informacijos, kaip konkretūs IMSI gaudyklių modeliai veikia. Tačiau remiantis atliktais tyrimais ir sukurtais prototipais, tokiais kaip Chris Paget pademonstruotas *DEF CON* konferencijoje [7], galima išskirti keletą neįprasto IMSI gaudyklių elgesio pavyzdžių, pagal kuriuos nesunku jas atskirti nuo tikrų mobiliojo ryšio tinklo bazinių stočių [13].

Šie atpažinimo požymiai gali būti pastebėti vartotojo galinėje įrangoje įdiegtos programinės įrangos arba specializuotų įrenginių pagalba. Tokia programinė įranga bei įrenginiai vadinami „IMSI gaudyklių gaudyklėmis“ arba „IMSI gaudyklių detektoriais“. Tolimesniuose poskyriuose pateikiami minėti požymiai ir pasiūlymai, kaip būtų galima juos užmaskuoti.

5.2.1. Neįprasto dažnio naudojimas

Siekiant pagerinti skleidžiamo signalo kokybę arba sumažinti esančius trukdžius, IMSI gaudyklės gali būti perjungiamos į nenaudojamus dažnius, pavyzdžiui, mobiliojo ryšio tinklo

testavimo tikslams rezervuotus kanalus arba skirtingų mobiliojo ryšio operatorių naudojamų dažnių skiriamąją juostą. Šis metodas turi trūkumų, nes IMSI gaudyklę nustačius į minėtus dažnius, judriosios stotys gali prie jos nesijungti, kadangi prioritetu renkasi kaimyninių celių dažnius, kuriuos pateikia kiekviena bazinė stotis.

Požymio aptikimas:

Šis požymis gali būti aptiktas lyginant mobilaus ryšio operatoriaus bazinių stočių naudojamus dažnius judriosios stoties buvimo teritorijoje su valstybės atsakingos tarnybos suteiktais radijo dažnių leidimais. Praktiškai kiekvienos valstybės atsakingos tarnybos viešai pateikia šią informaciją. Informaciją apie Lietuvoje išduotus radijo ryšio dažnių leidimus pateikia Lietuvos Respublikos ryšių reguliavimo tarnyba [39].

Sprendimas:

a) prieš pradedant naudoti IMSI gaudyklę tam tikroje vietovėje, atlikti joje naudojamų radijo dažnių analizę, pagal mobiliojo ryšio tiekėjus, ir veiksmams naudoti atitinkamus dažnius. Įgyvendinimui reiktų programinėje įrangoje aprašyti atitinkamus funkcionalumus arba naudoti papildomą, radijo spektro analizavimui skirtą, įrangą;
b) IMSI gaudyklių, skirtų tam tikram regionui (-ams) ar valstybei (-ėms), programinėje įrangoje aprašyti, tose regionuose mobilaus ryšio tiekėjų naudojamus radijo dažnius, duomenims panaudojant valstybių atsakingų tarnybų išduotų leidimų duomenų bazę. Šio varianto trūkumas yra tai, kad informaciją tektų nuolat atnaujinti, nes leidimai dažniausiai būna riboto galiojimo ir vėliau gali būti perskirstyti.

5.2.2. Neįprastas celės numeris

Mobiliojo ryšio tinklo celių numeriai (CID) yra unikalūs. Jie identifikuoja kiekvieną bazinę stotį, o vietovės kodas (LAC) nurodo kokioje vietovėje ji stovi. Siekiant išvengti protokolo neatitikimo su tikromis mobiliojo ryšio tinklo bazinėmis stotimis ir nenorint išprovokuoti judriąją stotį atsiųsti buvimo vietos atnaujinimo užklausą, IMSI gaudyklės dažniausiai pateikia naują celės numerį, kuris toje vietovėje nebuvo naudojamas.

Požymio aptikimas:

Šis požymis gali būti aptiktas lyginant bazinių stočių celių numerius buvimo vietoje su registruotų bazinių stočių, celių bei vietovių kodų duomenų bazėmis. Šią informaciją gali pateikti

valstybių atsakingos institucijos. Lietuvos Respublikos ryšių reguliavimo tarnyba tokios informacijos paprastam vartotojui nesuteikia. Todėl, kaip alternatyvą, galima naudoti mažiau patikimas viešas duomenų bazes [40].

Sprendimas:

Naudoti korektiškus CID, kurie priskirti esamai vietovei pagal jos LAC.

5.2.3. Bazinės stoties galimybių ir tinklo parametrų neatitikimas

Mobiliojo ryšio operatoriaus bazinės stotys teikia ne tik skambučių ir SMS, bet ir įvairias papildomas paslaugas, pavyzdžiui, duomenų perdavimo. Kai kurias iš šių paslaugų yra sudėtinga realizuoti, todėl tik profesionalios ir ypač brangios IMSI gaudyklės gali palaikyti tokius protokolus. Be to, judriosios stotys išsaugo informaciją apie pagrindinius mobiliojo ryšio tinklo parametrus, įskaitant ribines reikšmes, operacijų atlikimo trukmes ir skirtojo laiko reikšmes. Pasak [13], skirtingų mobiliojo ryšio operatorių tinkluose šie parametrai gali būti skirtingi, tačiau vieno operatoriaus visose bazinėse stotyse jie būna vienodi. Standartinės IMSI gaudyklės gali nekorektiškai nukopijuoti šią informaciją arba nukopijuoti ne visą, nes reikalingas specifinis tinklo branduolio informacijos išgavimas.

Požymio aptikimas:

Šis požymis gali būti nustatytas lyginant aptiktos bazinės soties galimybes su duomenų bazėje registruotų bazinių stočių informacija, kaip ir 5.2.2 punkte aprašytu atveju. Jei bazinės stoties siūlomos paslaugos nesutampa su duomenų bazėje pateikiamu aprašymu, ji tampa įtartina. Taip pat, kaip ir pagrindinių tinklo parametrų neatitikimo atveju.

Sprendimas:

Naudoti profesionalias IMSI gaudykles, kurios galėtų korektiškai nuskaityti tinklo branduolio informaciją.

5.2.4. Radijo bangų blokavimas

Siekiant, kad judrioji stotis greičiau atsijungtų nuo mobiliojo ryšio tiekėjo bazinės stoties ir prisijungtų prie IMSI gaudyklės, gali būti užteršiamas arba slopinamas bazinės stoties siunčiamas signalas. Judriosios stoties ryšys su bazine stotimi bus sutrikdytas ir nepavykus prisijungti prie kaimyninių bazinių stočių, judrioji stotis atliks pilną aplinkinių bazinių stočių

paiešką ir tuomet prisijungs prie stipriausią signalą siunčiančios bazinės stoties – IMSI gaudyklės. Radijo ryšio blokatorius, taip pat naudojamas siekiant privesti judriąją stotį persijungti iš LTE ar UMTS technologijos į GSM, nes ji turi silpniausią apsaugą.

Požymio aptikimas:

Bazinių stočių signalų blokavimas gali būti aptiktas judriajai stočiai stebint triukšmo lygį atitinkamuose dažniuose, tai yra šiuo metu naudojamame bei kaimyninių bazinių stočių dažniuose.

Sprendimas:

Nenaudoti radijo ryšio blokatoriaus, tam kad judriojo stotis persijungtų į GSM technologiją, o ataką vykdyti UMTS bei LTE tinkluose.

2014 m. gruodį vykusioje *Chaos Computer* saugumo konferencijoje, Karsten Nohl nurodė UMTS tinklo saugumo spragas, kuriomis galima pasinaudoti SS7 telefoninių signalų protokolų pagalba [41]. Pasinaudojant globaliais SS7 tinklais, IMSI gaudyklė gali apsimesti kitos šalies mobiliojo ryšio tiekėju, prie kurio jungiasi judrioji stotis, ir gauti autentiškumo patvirtinimą iš judriosios stoties mobiliojo ryšio operatoriaus bei taip autentifikuoti save judriajai stočiai.

Prie LTE tinklo prisijungusius įrenginius (UE) galima priversti persijungti į žemesnes technologijas ar apriboti gaunamas paslaugas. Tai galima atlikti išnaudojant LTE tinkle naudojamų buvimo vietos užklausų TAU (angl. *tracking area update*) ir prisijungimo prie tinklo užklausų (angl. *attach request*) saugumo spragomis – šios užklausos nėra šifruojamos. Netikra LTE bazinė stotis eNodeB gali informuoti UE, kad jai nėra suteikta prieiga prie LTE tinklo arba perėmusi prisijungimo prie tinklo užklausą, gali ją pakoreguoti ir realiam mobiliojo ryšio tinklui nusiųsti tokią užklausą, kurioje nurodyta, kad UE nepalaiko nei vienos ryšio technologijos. Pastaruoju atveju tinklas atmes UE siųstą užklausą atsakydamas, kad jai nėra suteikiama prieiga prie tinklo. UE gavusi tokias instrukcijas, net nebandys jungtis prie kitos bazinės stoties, net jei ji ir yra pasiekiama ar skleidžia stipresnį signalą nei dabartinė. Tokiu atveju UE iš naujo pradėtų jungtis prie tinklo, tik atlikus jos pakartotinę leistį [42].

5.2.5. Šifravimo nebuvimas

Kaip aprašyta 4.2.1 punkte, IMSI gaudyklė gali laisvai nurodyti judriajai stočiai, veikiančiai GSM protokolu, naudoti A5/0 šifro režimą, tai yra nešifruoti siunčiamos informacijos.

Požymio aptikimas:

Atsižvelgiant į įvairių šifravimo standartų naudojimą skirtingų operatorių mobiliojo ryšio tinkluose, šifravimo nebuvimas nėra pakankama priežastis įtarti, jog mobilioji stotis prisijungė prie netikros bazinės stoties. Tačiau, jei judrioji stotis jau užmezgė šifruotą sesiją ir ryšio perdavimas staiga tapo nebešifruotas, tai galima įtarti, kad ji prisijungė prie IMSI gaudyklės.

Sprendimas:

Tokiu atveju, reikia išnaudoti A5/1, A5/2 bei A5/3 šifrų protokolų saugumo spragas, kurios leidžia realiu laiku dešifruoti siunčiamą informaciją ir toliau komunikuoti su tinklu naudojant numatytą šifro režimą. A5/1 šifrą galima dešifruoti panaudojant iš anksto paruoštas atvirkštinių maišos funkcijų lenteles, kuriuos yra laisvai prieinamos [43]. Naudojant šį metodą kompiuteris su 2 GB operatyviosios atminties ir 2 TB talpos kietuoju disku per maždaug dvi minutes gali išgauti ilgalaikį saugos raktą K_i [38]. Dėl rimtų saugumo spragų GSM asociacija 2006 m. uždraudė naudoti A5/2 šifrą ir šiuo metu jis nėra naudojamas GSM tinkluose [44]. Taip pat buvo pademonstruotos A5/3 algoritmo praktinės atakos, tačiau šis metodas reikalauja tobulinimo ir optimizavimo, nes proceso trukmė per ilga (beveik 2 val.) ir sėkmės tikimybė per maža (~50%), kad šį metodą būtų galima naudoti realaus laiko atakoms [45].

5.2.6. Kaimyninių celių informacijos trūkumas

Kaip aprašyta 4.2.1 punkte, IMSI gaudyklė gali pateikti tuščią arba nekorektišką kaimyninių celių sąrašą, tam kad judrioji stotis liktų prie jos prisijungusi.

Požymio aptikimas:

Šis požymis gali būti aptiktas stebint kaimyninių celių sąrašų pasiekiamumą ir autentiškumą. Taip pat įtartinus kaimyninių celių sąrašus galima aptikti tikrinant registruotų bazinių stočių, kurios yra buvimo vietovėje, duomenų bazių įrašus.

Sprendimas:

Judriajai stočiai reikia pateikti buvimo vietovėje esančių tikrų kaimyninių celių sąrašą, tačiau jį sudaryti taip, kad jame esančios celės būtų kuo toliau nuo judriosios stoties veikimo teritorijos ir jų skleidžiamo signalo stiprumas būtų kuo žemesnis, pavyzdžiui, už keleto kilometrų (miesto sąlygomis) esanti celė, kurią užstoja aukštas pastatas.

5.2.7. Informacijos srauto nukreipimas

Kuomet IMSI gaudyklė užmezga ryšį su judriąja stotimi ir mobiliojo ryšio operatoriaus tinklu (žr. 4.2.1 punktą), ji turi palaikyti komunikavimą su abejomis pusėmis. Standartinė IMSI gaudyklė nepalaiko nei išeinančio, nei įeinančio judriosios stoties ryšio [7]. Mobiliojo ryšio operatoriaus tinkle toks abonentas traktuojamas, kaip esantis ne ryšio zonoje arba išjungtas.

Požymio aptikimas:

Šis požymis gali būti aptiktas bandant skambinti iš judriosios stoties, kuri yra prisijungusi prie IMSI gaudyklės, tokiu atveju skambutis nepavyks. Taip pat galima skambinti ar siųsti SMS iš kito telefono. Tokiu atveju judrioji stotis nesulauks nei skambučio, nei SMS, nors visos indikacijos rodys, kad ji yra prisijungusi prie mobiliojo ryšio operatoriaus tinklo, kai tuo tarpu skambutį atliekantis asmuo bus informuotas, kad abonentas, kuriam skambinama, yra ne ryšio zonoje.

Sprendimas:

a) naudojant standartinę IMSI gaudyklę, galima prie jos prijungti kitą judriąją stotį su SIM kortele ir visus išeinančius skambučius, duomenis bei SMS žinutes nukreipti per ją. Šio metodo trūkumas – skambučių ar SMS gavėjai matys, ne įprastą judriosios stoties abonento numerį, o visai nepažįstamą. Sušvelninat šį akivaizdų trūkumą, IMSI gaudyklėje galima nustatyti, kad nebūtų rodomas abonento numeris;
b) taip pat galima visą srautą tiesiogiai nukreipti į kito tiekėjo, teikiančio ryšio tinklų paslaugas;
c) geriausias sprendimas yra naudoto profesionalią įrangą, gebančia atlikti tikrą tarpinį įsilaužimą ir komutuoti informacijos perdavimą abiem pusėm.

6. IŠVADOS

1. Atlikus radijo bangų sklidimo prognozavimo modelių analizę pastebėta, kad nėra universalaus modelio, todėl reikia kuo tiksliau ir detaliau įvertinti aplinkos sąlygas bei parametrus, tai leis pasirinkti geriausiai tinkantį modelį. Suprojektavus sistemą naudojant netinkamą modelį gali būti blokuojami ne visi norimi įrenginiai arba atvirkščiai – bus paveikti ir paprasti vartotojai esantys šalia blokuotinos teritorijos. Esant galimybei, patartina bangų sklidimą prognozuoti kombinuojant kelis modelius bei blokavimo sistemoje naudoti kintamos galios siųstuvus, kuriais būtų galima kompensuoti skaičiavimų netikslumus.
2. Palyginus šiuo metu naudojamus signalo blokavimo metodus galima teigti, kad signalo blokavimo triukšmu metodas yra efektyvus, tačiau nelankstus blokuojamų vartotojų pasirinkimo atžvilgiu ir papildomai teršia radijo eterį. Todėl patartina naudoti IMSI gaudyklę, kurios pagalba papildomai galima manipuliuoti perimto signalo turiniu ar atsakyti į siunčiamas užklausas.
3. Išanalizavus IMSI gaudyklės specifiką nustatyta, kad efektyvesniam jos veikimui reikia naudoti kuo realesnius tinklo parametrus, tokius kaip korektišką operatoriaus radijo dažnį, korektišką celės numerį, mobiliajai stočiai pateikti jos buvimo vietai priskiriamų, tačiau kuo toliau esančių kaimyninių celių numerius, GSM tinkle su judriąja stotimi komunikuoti neišjungus šifravimo.
4. Sumodeliavus GSM, UMTS ir LTE technologijų IMSI gaudyklių tinklą, kuris tenkina signalo padengimo sąlygas, pastebėta, kad beveik neįmanoma iš karto numatyti optimalios tinklo konfigūracijos, todėl tikslui pasiekti reikalingas iteracinis procesas, kurio metu koreguojamas tinklo elementų skaičius, jų išdėstymas bei nustatymai.

7. INFORMACIJOS ŠALTINIŲ SĄRAŠAS

1. Security Research Labs, *SnoopSnitch* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <https://opensource.srlabs.de/projects/snoopsnitch>.
2. SecUpwN, *AIMSICD Wiki Home* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą:< https://github.com/SecUpwN/Android-IMSI-Catcher-Detector/wiki>.
3. REHNA V. J., KEHKESHAN Jalall S., HASRSHA K. ir kt. *Cell Phone Detection and Jamming System for GSM - 900 MHz and 1800 MHz Frequency Bands* [interaktyvus] 2014. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.warse.org/pdfs/2014/icceitsp052014.pdf>.
4. JISRAWI, Ahmad; *GSM-900 Mobile JAMMER* [interaktyvus].[žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.qrz.ru/schemes/contribute/security/jammers/gsm-jammer.pdf>.
5. SHANTANU KRISHNA MAHATO, C.Vimala; *Cellular Signals Jamming System in 2G And 3G* [interaktyvus] 2014. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.ijareeie.com/upload/2014/apr14-specialissue3/44_R45_Shantanu.pdf>.
6. PIQUERAS JOVER, Roger; LACKEY, Joshua; RAGHAVAN, Arvind; *Enhancing the security of LTE networks against jamming attacks* [interaktyvus] 2014. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą:< http://jis.eurasipjournals.springeropen.com/articles/10.1186/1687-417X-2014-7>.
7. PAGET, Chris; *Practical Cellphone Spying* [interaktyvus].[žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <https://www.youtube.com/watch?v=fQSu9cBaojc>.
8. KOSTRZEWA, Adam; *Development of a man in the middle attack on the GSM Um-Interface* [interaktyvus] 2011. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.isti.tu-berlin.de/fileadmin/fg214/finished_theses/kostrzewa/diplom_kostrzewa.pdf>.
9. MEYER, Ulrike; WETZEL, Susanne; *A Man-in-the-Middle Attack on UMTS* [interaktyvus] 2004. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://ece.wpi.edu/~dchasaki/papers/mitm_umts.pdf>.
10. MJØLSNES, Stig F.; OLIMID, Ruxandra F.; *Easy 4G/LTE IMSI Catchers for Non-Programmers* [interaktyvus] 2017. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <https://arxiv.org/pdf/1702.04434.pdf>.
11. PIQUERAS JOVER, Roger; *LTE security, protocol exploits and location tracking experimentation with low-cost software radio* [interaktyvus] 2016. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą:< https://arxiv.org/pdf/1607.05171.pdf>.
12. GOLDE, Nico; REDON, Kevin; BORGAONKAR, Ravishankar; *Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunication* [interaktyvus] 2012. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą:< https://www.tu-berlin.de/fileadmin/fg214/Papers/femto_ndss12.pdf>.
13. DABROWSKI, Adrian; MULAZZANI, Martin ir kt. *IMSI-Catch Me If You Can: IMSI-Catcher-Catchers* [interaktyvus] 2014. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <https://www.sba-research.org/wp-content/uploads/publications/DabrowskiEtAl-IMSI-Catcher-Catcher-ACSAC2014.pdf>.
14. HARMAT, Bryan; STROUD, Jared; JOHNSON, Daryl ir kt. *The Security Implications of IMSI Catchers* [interaktyvus] 2015. [žiūrėta: 2017 gegužės 26 d.] Prieiga per internetą: <https://www.cis.upenn.edu/current-students/undergraduate/courses/documents/EAS499Honors-IMSICatchersandMobileSecurity-V18F-1.pdf>.

15. VAN DEN BROEK, Fabian; DE RUITER, Joeri; VERDULT, Roel; *Defeating IMSI Catchers* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.cs.ru.nl/~rverdult/Defeating_IMSI_Catchers-CCS_2015.pdf>.
16. SAUNDERS, Simon R.; ARAGO´ N-ZAVALA Alejandro; *Antennas and propagation for wireless communication systems*. Chichester : JohnWiley & Sons Ltd, 2007.
17. LUO, Meiling; *Indoor radio propagation modeling for system performance prediction* [interaktyvus] 2014. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <https://tel.archives-ouvertes.fr/tel-00937481/document>.
18. SEYBOLD, John S; *Introduktion to RF Propagation* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.asrr.org/attachments/195_Introduction%20to%20RF%20Propagation%20-%20John%20S.%20Seybold-2005.pdf>.
19. SHABBIR, Noman ir kt. *Comparison of radio propagation models for long term evolution (LTE) network* [interaktyvus] 2011. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <https://arxiv.org/ftp/arxiv/papers/1110/1110.1519.pdf>.
20. STROBEL, Daehyun; *IMSI Catcher*. [interaktyvus] 2007. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <https://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf>.
21. EHEDURU, Marcellinus; *Indoor Radio Measurement and Planning for UMTS/HSPDA with Antennas* [interaktyvus] 2013. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://dc.uwm.edu/cgi/viewcontent.cgi?article=1093&context=etd>.
22. KEŽIONIS, Algimantas; *Telekomunikacijų principai* [interaktyvus] 2010. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://rfk.ff.vu.lt/doc/tel_pagrindai.pdf>.
23. ŽILINSKAS, Mindaugas; *Taikomoji elektrodinamika* [interaktyvus] 2008. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://rfk.ff.vu.lt/doc/t_elektrodinamika.pdf>.
24. VILNIAUS UNIVERSITETAS; *GSM bazinių stočių išdėstymo planavimas žemėlapyje* [interaktyvus] 2009. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://rfk.ff.vu.lt/doc/rysiai_lab1.pdf>.
25. 3GPP; *TS 03.22. Functions related to Mobile Station (MS) in idle mode and group receive mode* [interaktyvus] 2002. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.etsi.org/deliver/etsi_ts/100900_100999/100930/08.07.00_60/ts_100930v080700p.pdf>.
26. 3GPP; *TS 05.08. Radio subsystem link control* [interaktyvus] 2005. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.etsi.org/deliver/etsi_ts/100900_100999/100911/08.23.00_60/ts_100911v082300p.pdf>.
27. 3GPP; *TS 25.304. User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode* [interaktyvus] 2017. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.etsi.org/deliver/etsi_ts/125300_125399/125304/14.00.00_60/ts_125304v140000p.pdf>.
28. 3GPP; *TS 36.304. User Equipment (UE) procedures in idle mode* [interaktyvus] 2017. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.etsi.org/deliver/etsi_ts/136300_136399/136304/14.02.00_60/ts_136304v140200p.pdf>.
29. 3GPP; *Specifications* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.3gpp.org/specifications/79-specification-numbering>.

30. NYBERG, Kaisa; *Cryptographic algorithms for UMTS* [interaktyvus] 2004. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://research.ics.aalto.fi/publications/bibdb2014/pdf/eccomas.pdf>.
31. HOWARD, Peter; *3G Security Overview* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.isrc.rhul.ac.uk/useca/OtherPublications/IIR-overview.pdf>.
32. VINTILĂ, Cristina-Elena; PATRICIU, Victor-Valeriu; BICA Ion; *Security Analysis of LTE Access Network* [interaktyvus] 2011. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <https://www.thinkmind.org/download.php?articleid=icn_2011_2_20_10330>.
33. PURKHIABANI Masoumeh; SALAHI Ahmad; *Enhanced Authentication and Key Agreement Procedure of next Generation 3GPP Mobile Networks* [interaktyvus] 2012. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.ijiee.org/papers/57-C099.pdf>.
34. CANADA, RADIO ADVISORY BOARD OF; *Use of Jammer and Disabler Devices for Blocking PCS, Cellular & Related Services* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.meshcode.ca/PROJECTS/telefire/MK_jamming_laws_canada_01pub3.pdf>.
35. Gamry Instruments; *The Faraday Cage: What is it? How does it work?* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www:gamry:com/application-notes/instrumentation/faraday-cage/>.
36. PELL, Stephanie K.; SOGHOIAN, Christopher; *our Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy* [interaktyvus] 2014. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2437678>.
37. MÜLLER, Günter; RANNENBERG, Kai; FEDERRATH, Hannes; *Protection in Mobile Communications* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <https://www.semanticscholar.org/paper/Protection-in-Mobile-Communications-M%C3%BCller-Rannenberg/4b1e10122a72bff60607a78030de718a8cc96fed/pdf>.
38. MEYER, Ulrike; WETZEL, Susanne; *On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://ece.wpi.edu/~dchasaki/papers/gsm_enc.pdf>.
39. LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBA*; Leidimai naudoti radijo dažnius (kanalus), kurių skaičius yra ribotas* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.rrt.lt/rrt/lt/verslui/istekliai/radijo-dazniai/leidimu-sk-ribotas.html>.
40. ENAIKOON; *Open Cell ID* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://opencellid.org/>.
41. KARSTEN, Nohl; *Mobile self-defense* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <https://www.youtube.com/watch?v=GeCkO0fWWqc>.
42. SHAIK, Altaf ir kt; *Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems* [interaktyvus] 2016. [žiūrėta: 2017 gegužės 26 d.]. <http://arxiv.org/pdf/1510.07563.pdf>.
43. SRLabs; *A5/1 Decryption* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <https://opensource.srlabs.de/projects/a51-decrypt/files>.

44. 3GPP; *Prohibiting A5/2 in mobile stations and other clarifications regarding A5 algorithm support* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_37/Docs/SP-070671.zip>.
45. DUNKELMAN, Orr; KELLER, Nathan; SHAMIR, Adi; *A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony* [interaktyvus]. [žiūrėta: 2017 gegužės 26 d.]. Prieiga per internetą: <https://eprint.iacr.org/2010/013.pdf>.