Kauno technologijos universitetas

Mechanikos inžinerijos ir dizaino fakultetas

Vieno sluoksnio bepiločių orlaivių spiečiaus pažeidžiamumo panaudojant ataką elektroninėje erdvėje tyrimas

Baigiamasis magistro projektas

Irmantas Lukša

Projekto autorius

Doc. Saulius Japertas

Vadovas

Kaunas, 2024

Kauno technologijos universitetas

Mechanikos inžinerijos ir dizaino fakultetas

Vieno sluoksnio bepiločių orlaivių spiečiaus pažeidžiamumo panaudojant ataką elektroninėje erdvėje tyrimas

Baigiamasis magistro projektas

Aeronautikos inžinerija (6211EX024)

Irmantas Lukša

Projekto autorius

Doc. Saulius Japertas

Vadovas

Prof. Laurencas Raslavičius

Recenzentas

Kaunas, 2024

Kauno technologijos universitetas

Mechanikos inžinerijos ir dizaino fakultetas

Irmantas Lukša

Vieno sluoksnio bepiločių orlaivių spiečiaus pažeidžiamumo panaudojant ataką elektroninėje erdvėje tyrimas

Akademinio sąžiningumo deklaracija

Patvirtinu, kad:

1. baigiamąjį projektą parengiau savarankiškai ir sąžiningai, nepažeisdama(s) kitų asmenų autoriaus ar kitų teisių, laikydamasi(s) Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo nuostatų, Kauno technologijos universiteto (toliau – Universitetas) intelektinės nuosavybės valdymo ir perdavimo nuostatų bei Universiteto akademinės etikos kodekse nustatytų etikos reikalavimų;

2. baigiamajame projekte visi pateikti duomenys ir tyrimų rezultatai yra teisingi ir gauti teisėtai, nei viena šio projekto dalis nėra plagijuota nuo jokių spausdintinių ar elektroninių šaltinių, visos baigiamojo projekto tekste pateiktos citatos ir nuorodos yra nurodytos literatūros sąraše;

3. įstatymų nenumatytų piniginių sumų už baigiamąjį projektą ar jo dalis niekam nesu mokėjęs (-usi);

4. suprantu, kad išaiškėjus nesąžiningumo ar kitų asmenų teisių pažeidimo faktui, man bus taikomos akademinės nuobaudos pagal Universitete galiojančią tvarką ir būsiu pašalinta(s) iš Universiteto, o baigiamasis projektas gali būti pateiktas Akademinės etikos ir procedūrų kontrolieriaus tarnybai nagrinėjant galimą akademinės etikos pažeidimą.

Irmantas Lukša

Patvirtinta elektroniniu būdu

Kaunas technologijos universitetas

Mechanikos inžinerijos ir dizaino fakultetas

Baigiamojo magistro projekto užduotis

Išduota studentui (-ei) – Irmantas Lukša

1. Projekto tema

Vieno sluoksnio bepiločių orlaivių spiečiaus pažeidžiamumo panaudojant ataką elektroninėje erdvėje tyrimas

(Lietuvių kalba)

Investigation of the Vulnerability of Single-Layer Drone Swarm to Cyber Attack

(Anglų kalba)

2. Projekto tikslas ir uždaviniai

Tikslas: sukurti įsilaužimo į vieno sluoksnio bepiločių orlaivių spiečiaus kontrolę modelį, kai įsilaužimo objektas apibrėžiamas kaip dinaminė sistema.

Uždaviniai:

1. Išnagrinėti bepiločių orlaivių kolizijų išvengimo bepiločių orlaivių spiečiuje metodus.
2. Nustatyti spiečiaus struktūrą, naudojamą kuriant modelį.
3. Nustatyti spiečiaus infekavimo kibernetinės atakos metu būdus.
4. Sudaryti lyderio bepiločių orlaivių spiečiuje identifikavimo algoritmą.
5. Sudaryti funkcinį atakos elektroninėje erdvėje modelį.

3. Pagrindiniai reikalavimai ir sąlygos

Pateikti tikslią BO spiečiaus struktūrą.
Pateikti įsilaužimo į BO spiečiaus kontrolę modelį.

4. Papildomi reikalavimai projektui, ataskaitai ir jos priedams

Netaikoma

Projekto autorius	Irmantas Lukša	2024-02-15
	(Vardas, Pavardė)	*(Data)*
Projekto vadovas	Doc. Saulius Japertas	2024-02-15
	(Vardas, Pavardė)	*(Data)*
Krypties studijų programų vadovas/	Prof. Artūras Keršys	2024-02-15
	(Vardas, Pavardė)	*(Data)*

Lukša, Irmantas. Vieno sluoksnio bepiločių orlaivių spiečiaus pažeidžiamumo panaudojant ataką elektroninėje erdvėje tyrimas. Magistro baigiamasis projektas / vadovas Doc. Saulius Japertas; Kauno technologijos universitetas, Mechanikos inžinerijos ir dizaino fakultetas.

Studijų kryptis ir sritis (studijų krypčių grupė): Aeronautikos inžinerija (E14), Inžinerijos mokslai.

Reikšminiai žodžiai: Bepiločių orlaivių spiečius; bepiločių orlaivių spiečiaus architektūra; bepiločių orlaivių spiečiaus pažeidžiamumas; ataka elektroninėje erdvėje; bepiločių orlaivių spiečiaus lyderis; bepiločių orlaivių spiečiaus agentai.

Kaunas, 2024. 62 p.

Santrauka

Baigiamajame magistro darbe siekta kuo išsamiau išanalizuoti galimybę pažeisti vieno sluoksnio bepiločių orlaivių spiečiaus kontrolę, panaudojant ataką elektroninėje erdvėje. Tyrimo objektas – bepiločių orlaivių spiečius, kuris susideda iš 10 agentų, t.y. 9 spiečiaus agentai ir vienas lyderis. Spiečius pilnai autonominis – neturi tiesioginio kontakto su žmogiškuoju veiksniu visos misijos metu.

Darbe išnagrinėta bepiločių orlaivių spiečiaus architektūra. Nustatyta kokiu būdu bepiločių orlaivių spiečiaus agentai nesusiduria ir išlaiko struktūrą. Norint nustatyti bepiločių orlaivių spiečiaus pažeidžiamumą, svarbu nustatyti visas galimas komunikacijas tarp spiečiaus agentų ir ryšių architektūrą. Pasirinkta išsamiau tirti *Ad-hock* ryšio architektūra.

Pasirinkta, kad tyrime bus naudojamas bepiločių orlaivių spiečius, kuris susideda iš 9 spiečiaus agentų ir 1 lyderio. Tokia konfigūracija naudojama dėl aiškaus valdymo algoritmų tikslumo ir pritaikomumo patikrinimo. Sudaryta keletas valdymo algoritmų naudojamų simuliacijų duomenims pavaizduoti. Valdymo algoritmų tikslumui patikrinti pateikta viena simuliacija be spiečiaus lyderio ir nustatyta, kad tokio algoritmo paklaida nesiekia 1 procento.

Remiantis STRIDE metodologija nustatytos saugumo grėsmės bepiločių orlaivių spiečiui FANET tinkle. 4 bepiločių orlaivių spiečiaus ryšio jungtys turi 6 galimas atakas elektroninėje erdvėje, o 2 mazgai – 6 grėsmes jiems patiems. Sudaryta programinė architektūra *Linux* programinės įrangos pagrindu ir atlikta kibernetinė ataka prieš menamą bepiločių orlaivių spiečiaus lyderį. Pastebėta, kad naudojant *DoS* ataką buvo kardinaliai pakeista menamo lyderio judėjimo trajektorija.

Remiantis moksliniais tyrimais nustatyta, kad bepiločių orlaivių spiečiai naudoja atvirą tinklą komunikacijai palaikyti. Sudarytas prisijungimo prie išskirstyto FANET tinklo metodo algoritmas, kuris paremtas lyderio pasirinkimu atvirame vienos ar daugiau dažnių juostų tinkle.

Sudarytas atakos elektroninėje erdvėje modelis, kurio pagrindas tikimybinės lygtys. Modelis pritaikytas neapibrėžtai valdymo sistemai ir remiasi pažeidžiamumo sąlygomis, kurios nustatomos, kai orlaivis užpuolikas prisijungia prie spiečiaus tinklo architektūros.

Lukša, Irmantas. Investigation of the Vulnerability of Single-Layer Drone Swarm to Cyber Attack. Masters's Final Degree Project / supervisor Assoc. Prof. Saulius Japertas; Faculty of Mechanical Engineering and Design, Kaunas University of Technology.

Study field and area (study field group): Aeronautical Engineering (E14), Engineering Science.

Keywords: UAV swarm; UAV architecture; vulnerability of UAV swarm; cyber-attack; UAV master; UAV slave; Master-Slave UAV model.

Kaunas, 2024. 62.

Summary

The purpose of the final master's thesis was to analyse in as much detail as possible the possibility of breaching the control of a single layer UAV swarm by using an electronic attack. The object of the study is an UAV swarm consisting of 10 agents, i.e. 9 slaves and one master. The swarm is fully autonomous - it has no direct contact with the human factor throughout the mission.

The architecture of the UAV swarm is analysed in this work. It has been determined in what way the UAV swarm agents do not collide and maintain the structure. To determine the vulnerability of an UAV swarm, it is important to identify all possible communications between swarm agents and the communication architecture. The *Ad-hock* communication architecture has been chosen to investigate in more detail.

It has been chosen to use an UAV swarm in the study which consists of 9 slaves and 1 master This configuration is used because of the clarity of the control algorithms and to test the accuracy and applicability. Several control algorithms have been developed to represent the simulation data. To test the accuracy of the control algorithms, one simulation without a swarm leader is presented and it is found that the precision of this algorithm is more than 99 %.

Based on the STRIDE methodology, security threats to UAV swarms in the FANET are identified. The 4 UAV swarm communication links have 6 potential threats in cyberspace and the 2 nodes have 6 threats to themselves. A software architecture based on Linux software has been developed and a cyber-attack against the assumed leader of the UAV swarm has been performed. It was noticed that the DoS attack radically changed the movement trajectory of the assumed leader.

Research has shown that UAV swarms use an open network to communicate. An algorithm for a distributed FANET connection method was developed based on the choice of a leader in an open network of one or more frequency bands.

An electronic attack model based on probability equations has been developed. The model is applied to an unspecified control system and is based on vulnerability conditions that are defined when the attacker aircraft connects to the swarm network architecture.

Turinys

Lentelių sąrašas

Paveikslų sąrašas

Santrumpų ir terminų sąrašas

Santrumpos:

BO – bepilotis orlaivis.

BOS – bepiločių orlaivių sistema.

GCS – antžeminė ryšio stotis.

GPS – globali padėties nustatymo sistema.

ROS – robotų valdymo operacinė sistema.

SOTA – naujausi technologijų pasiekimai.

WMN – tinklinis tinklo ryšys.

FANET – orlaivių belaidis tinklas *Ad-Hoc* tinkle.

VANET – transporto priemonių tinklas *Ad-Hoc* tinkle.

MANET – mobilusis *Ad-Hoc* tinklas.

P2P – vartotojas/vartotojas.

D2D – dronas/dronas.

D2GS – dronas/antžeminė stotis.

D2N – dronas/belaidis tinklas.

SAA – jutiklių duomenimis paremta sistema.

CA – susidūrimo vengimas.

GCA – antžeminė ryšio stotis.

Įvadas

Pastaraisiais metais bepiločių orlaivių plitimas sukėlė revoliuciją įvairiuose sektoriuose, įskaitant karines operacijas, nelaimių valdymą, tiksliąją žemdirbystę ir infrastruktūros tikrinimą. Bepiločių orlaivių spiečiai tapo perspektyvia sistema, padedančia vykdyti bendradarbiavimo ir keičiamo mastelio misijas, užtikrinančias didesnį veiksmingumą ir lankstumą. Šiuo metu didelis dėmesys skiriamas bepiločių orlaivių spiečiaus vystymui, įskaitant apsaugos nuo įsilaužimo priemones. Darbe pagrindinis dėmesys skiriamas ne atskirų bepiločių orlaivių saugumui, o spiečiaus, kaip kolektyvinio darinio, funkcionalumo pažeidimui. Sutrikdant ryšių ir koordinavimo mechanizmus, galima paveikti spiečių, todėl jis taps neveiksmingas siekiant numatytų misijos tikslų.

Vis dažniau naudojant bepiločių orlaivių spiečius kyla grėsmė jų vykdomų misijų saugumui. Pastebėta, kad atlikta sąlyginai daug tyrimų, kuriuose bandoma išsiaiškinti kaip apsaugoti spiečių, bet labai mažai tų, kurie tiria įsilaužimo galimybę. Įsilaužimo į bepiločių orlaivių spiečiaus kontrolę aktualumą galima traktuoti skirtingai: tai apsaugos priemonė, jei spiečiaus misijos objektas turi būti apsaugotas; tai apsaugos priemonė bepiločių orlaivių spiečiui. Jei žinomos įsilaužimo grėsmės tolimesnių tyrimu metu galima apsaugoti spiečių nuo nepageidaujamų pažeidimų. Tyrimo aktualumas grindžiamas tuo, kad daugiausia dėmesio skiriama elektroninėms atakoms, kuriomis siekiama ištirti pažeidžiamumą, būdingą vieno sluoksnio bepiločių orlaivių spiečių formavimosi sistemoms, ir taip atskleisti galimas silpnąsias vietas.

Darbo tikslas: sukurti įsilaužimo į vieno sluoksnio bepiločių orlaivių spiečiaus kontrolę modelį, kai įsilaužimo objektas apibrėžiamas kaip dinaminė sistema.

Tikslui pasiekti iškelti uždaviniai:
1. Išnagrinėti bepiločių orlaivių kolizijų išvengimo bepiločių orlaivių spiečiuje metodus.
2. Nustatyti spiečiaus struktūrą, naudojamą kuriant modelį.
3. Nustatyti spiečiaus infekavimo kibernetinės atakos metu būdus.
4. Sudaryti lyderio bepiločių orlaivių spiečiuje identifikavimo algoritmą.
5. Sudaryti funkcinį atakos elektroninėje erdvėje modelį.

Apibendrinant galima teigti, kad šiuo tyrimu siekiama sistemingai analizuojant įvairių atakų scenarijų poveikį spiečiaus darnai ir elgsenai, pateikti iššūkius su kuriais susiduriama vykdant bepiločių orlaivių spiečių misijas dinamiškoje ir potencialiai priešiškoje aplinkoje. Galiausiai, nustatant pažeidžiamumus, siekiama sukurti tvirtą pagrindą tolimesniems bepiločių orlaivių tyrimams, kad būtų galima atlaikyti elektroninius trikdžius ir priešiškas grėsmes.

1. Bepiločių orlaivių kolizijų išvengimo bepiločių orlaivių spiečiuje metodus

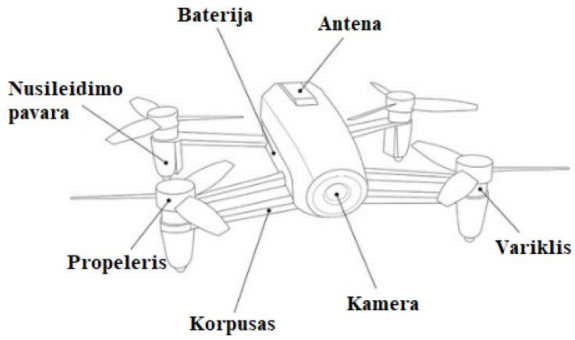
Skyriuje pateikta standartinių BO architektūra, komunikacija, susidūrimo vengimo metodai ir ryšio technologijos.

1.1. Standartinis BO

Nors nuo bepiločių orlaivių sukūrimo ir pirmojo panaudojimo praėjo beveik šimtmetis, jie tapo ypač populiarūs pastaraisiais metais. Nepriklausomai nuo paskirties BO struktūra susideda iš:

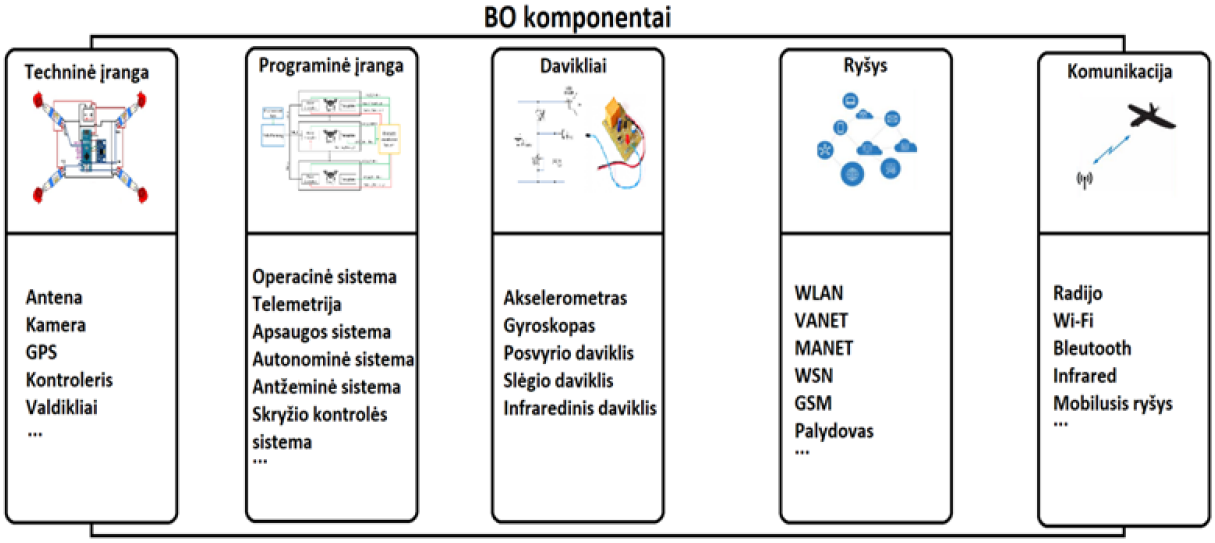
- mechaninės dalies;
- elektroninės dalies;
- kompiuterinės/programinės įrangos dalies;
- domenų perdavimo dalies;
- naudingo krovinio (stebėjimo įranga; ginkluotė ir pan.) gabenimo dalies.

Standartinio BO struktūra pateikta 1 pav.



1 pav. Kvandrakopterio komponentai

1 pav. pateikta standartinio kvadrakopterio architektūra. Be papildomo įrangos tokios kaip jutikliai, siųstuvai ir imtuvai, duomenų saugojimo įrenginių, vaizdo ar kitų stebėjimų įrangos, orlaivis susideda iš korpuso, kuriame talpinama baterija, inercinė navigacinė sistema, energijos skirstymo blokas, pasaulinės padėties nustatymo sistemos ir kitų valdiklių. Prie korpuso tvirtinami 4 varikliai su propeleriais, kurios tiesiogiai valdo greičio perdavimo kontroleris.



2 pav. BO įrangą sudarančių komponentų skirstymas

IEEE 802.11 – standartizuotos grupės ryšio protokolų rinkinys, skirtas vietiniam tinklo ryšiui palaikyti. Standartas ryšio sistemoje atsakingas iš kontrolės ir fizinio tinklo lygmens tinkamumą palaikymui. *Ad-hoc* – primatus dinaminis tinklas, kuris naudoja pažangias technologijas belaidžiam tinklui palaikyti. Susiejus *Ad-hoc* tinklą ir IEEE 802.11 standartą gaunama tinklo architektūra, kurioje visi ryšio komponentai gali judėti atsitiktinai, nepriklausomai ir pakaitomis vienas kito atžvilgiu. Toks komunikacijos tipas idealiai tinka BO spiečiui, nes parasta valdyti kolizijos reiškinį [49]. Galima išskirti 3 *Ad-hoc* tinklo subkategorijas tinkančias BO spiečiaus kontrolės architektūrai:

1. MANET (angl. „Mobile Ad-hoc Network“) – tinklo architektūros pliusas, kad BO orlaiviai gali judėti autonomiškai ir atsitiktinai. Kiekvienas orlaivis gali turėti savo valdymo protokolą, todėl kyla grėsmė saugumui ir dideli nuostoliai perduodat komunikacijos paketus [50].
2. VANET (angl. „Vehicular Ad-hoc network“) – belaidžių tinklų architektūra taikanti spontanišką valdymo modelį ir dažniausiai naudojama transporto priemonėms valdyti. Tinklo architektūros pliusas – lengva susieti valdymo sistemą su jutiklių informacija. Ryšys pažeidžiamas *Sybil* atakų, nes kiekvienas įrenginys apibrėžtas kaip mazgas, kuris su kitais sąveikoje dalyvaujančiais mazgais bendrauja nestandartizuotai. Prisijungus naudojant suklastotas tapatybes galima perimti spiečiaus kontrolę [51].
3. WSN (angl. „Wireless Sensor Networks“) – architektūros pagrindą sudaro ryšio palaikymas per antžeminę stotį, todėl išauga spiečiaus narių energijos sąnaudos. Dėl tiesioginės komunikacijos su antžemine stotimi ryšio architektūra tampa pažeidžiama pasiklausymo ir MITM atakoms [52].

1.2. BO architektūra ir komunikacijos tipai

Standartinio BO, skirto nesudėtingoms misijoms atlikti architektūra sudaro 3 esminiai komponentai [1,2]:

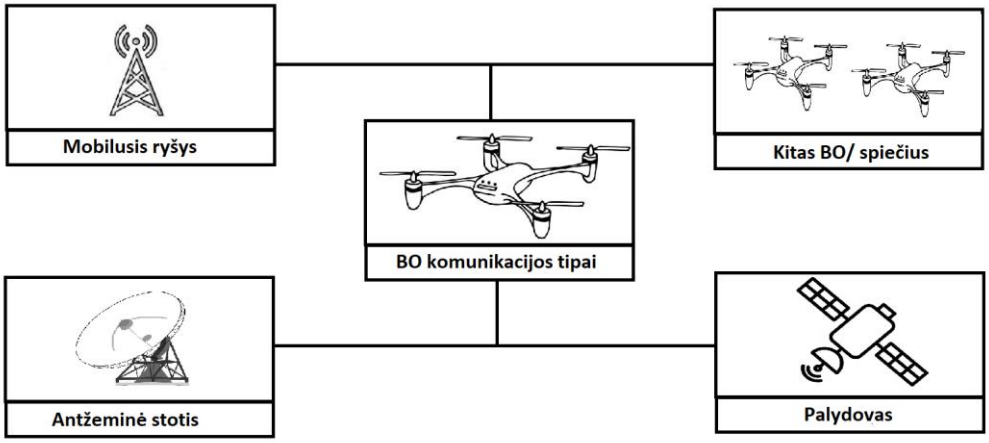
- Misijos duomenų valdiklis – kontroleris naudojantis programinę įrangą skirtą skrydžio parametrams ir duomenims analizuoti [1].
- Antžeminė ryšio stotis – naudojant ryšį oras-žemė BO valdymo operatorius perduoda komandas ryšio mazgams. Antžeminės stotys skiriasi nuo BO atliekamos misijos – priklausomai nuo bendravimo atstumo skiriasi antžeminių stočių ryšio perdavimo galia. Paprastai misijos atlikimo metu BO komunikuoja su keletu antžeminių stočių [1].
- Domenų perdavimo ryšiai – ryšiai, kurie kontroliuoja informacijos srautą tarp BO ir antžeminės ryšio stoties [2].

Reikalingus ryšio atstumus galima skirstyti:

1. Iki matomumo linijos ribų – galima ryšio palaikymui naudoti radijo bangas [2].
2. Už matomumo linijos ribų – paprastai naudojama palydovinę komunikacija[2].

4 pav. pateikta BO skirstymo pagal ryšio tipu iliustracija. Atlikus analizę pastebėta, kad komunikacijos ryšį galima suskirstyti į 4 pagrindinius tipus: dronas-mobilusis-ryšys (angl. „Drone-to-Network“, D2N), dronas-dronas (angl. „Drone-to-Drone“, D2D), dronas-antžeminė stotis (angl. „Drone-to-Ground Station“, D2GS), dronas-palydovas (angl. „Drone-to-Setellite“, D2S).

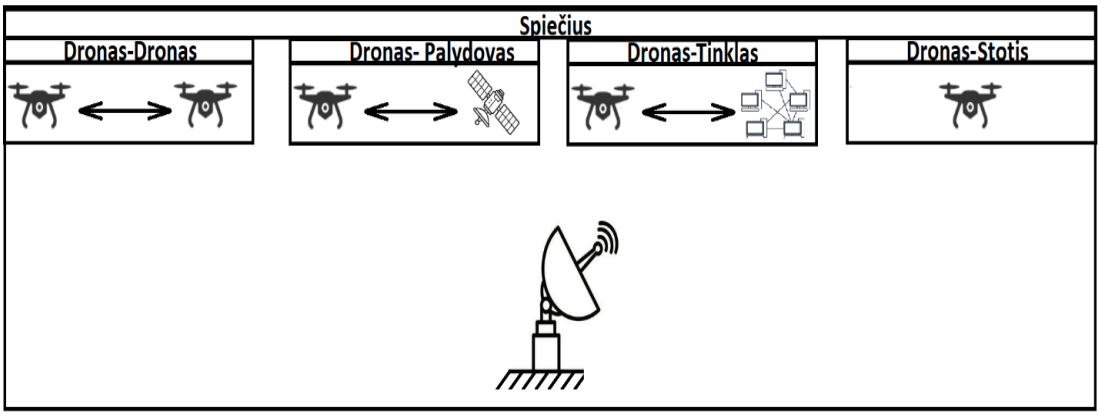
D2D – nestandartizuotas ryšio tipas. Kaip ir P2P tinklas, D2D pažeidžiamas angl. „Peer-toPeer“) atakomis tokiomis kaip *DDoS* (didelis kiekis autentifikavimo pranešimų per sąlyginai trumpą laiko tarpą), *Sybil* (neteisėtai prisijungiama prie ryšio) ar naudojant trikdymą (*Jamming*) [4,5].



3 pav. BO komunikacija

D2GS – standartizuotas ryšio tipas, nes naudojami standartiniai protokolai tokie kaip *Bluetooth* ir *Wi-Fi* ryšiui palaikyti. Net ir naudojant simetrinio rakto patvirtinimą užpuolikas dešifravęs autentifikavimą gali lengvai prisijungti prie sąlyginai viešo ir nesaugos tinklo. Paprasčiausiai įgyvendinamos atakos: pasiklausymas ir MITM [4,5].

D2N – Ryšys pasižymi saugumo lygio adaptavimu. Esant poreikiui, galima pasirinkti saugesni ryšį, pavyzdžiui, palydovinę komunikacija ir atvirkščiai – misijai nereikalaujant aukšto saugumo galima rinkti pigesnės eksploatacijos korinį ryšį (3 GHz, 4 GHz, LTE, 5 GHz dažniai) [4,5].



4 pav. BO komunikacija

D2S – Palydovinis ryšys yra laikomas patikimu ir saugiu. Pagrindinis ryšio pliusas tas, kad galima naudoti koordinačių perdavimą realiu laiku per GPS: pasaulinę padėties nustatymo sistemą, tačiau tokio tipo ryšys yra gana brangus, be to, reikalauja specialių priežiūros reikalavimų.

1.3. BO tipai

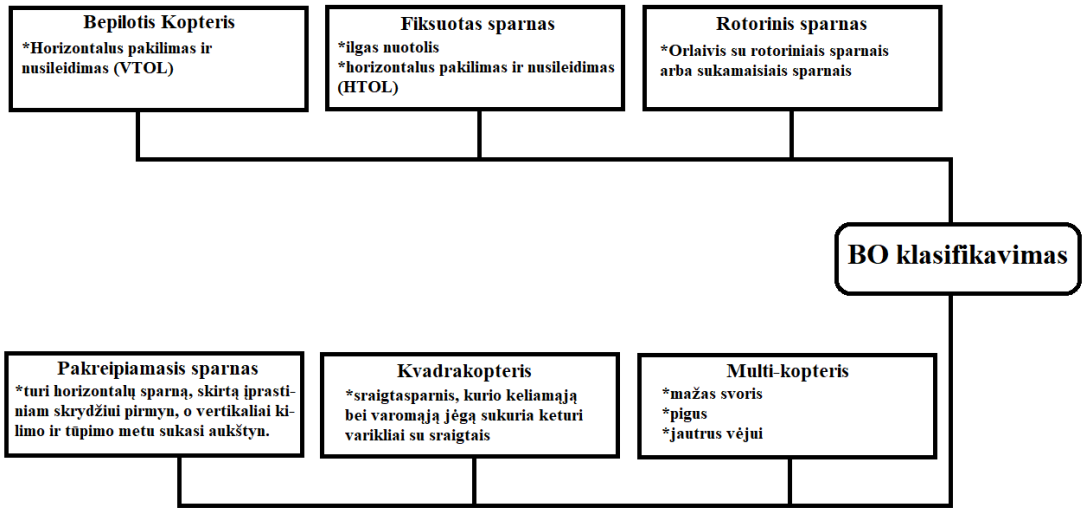
Šiame poskyryje išsamiai aprašomas skirtumas tarp dronų, bepiločių orlaivių (BO) ir bepiločių orlaivių sistemų (BOS). Klasifikacija pateikta 5 pav. ir 6 pav. Pastebėta, kad visi bepiločiai orlaiviai yra dronai, tačiau ne visi dronai yra bepiločiai orlaiviai.

Dronais paprastai vadinami orlaiviai, kurie valdomi nuotoliniu arba autonominiu būdu naudojant programiškai kontroliuojama iš anksto nustatyta misiją. Pagal naudojamus skraidymo mechanizmus dronai gali būti klasifikuojami taip[6]:

- daugiarotoriniai dronai – keliamąją jėga generuoja daugiau nei 2 fiksuoti žingsnio besisukantys rotoriaus sraigtai. Tokie orlaiviai pasižymi vertikaliu kilimu ir tūpimu, taip pat gali kyboti fiksuotame taške. Daugiarotorinių dronų trūkumas – didelis energijos suvartojimas, todėl misijos laikas ribotas [6,7];
- fiksuoto sparno bepiločiai orlaiviai – paprastai tokie dronai turi vieną fiksuotą sparną. Skrydis kaip lėktuvo – būtinas paskilimo ir nusileidimo takas. Fiksuoto sparno bepiločiai orlaiviai brangesni nei daugiarotoriniai ir negali kyboti fiksuotame taške, nes naudojama įeinančio srauto keliamoji jėga [6,7];
- paprastai tokie dronai turi vieną fiksuotą sparną. Skrydis kaip lėktuvo – būtinas paskilimo ir nusileidimo takas. Fiksuoto sparno bepiločiai orlaiviai brangesni nei daugiarotoriniai ir negali kyboti fiksuotame taške, nes naudojama įeinančio srauto keliamoji jėga.
- bepiločiai orlaiviai su hibridiniu sparnu – panašus į daugiarotorių tipą, todėl orlaivis gali greitai pasiekti taikinį, sklandydamas ore ir pakibti taške rotorių pagalba [7,8].

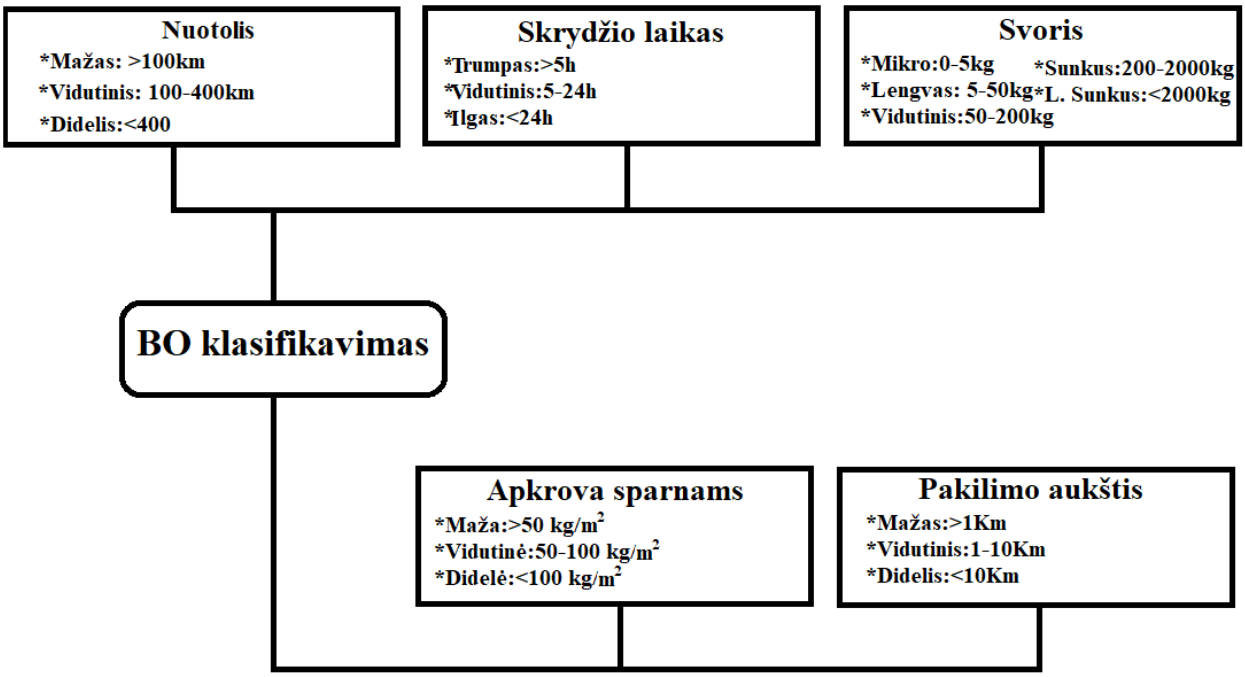
Bepilotis orlaivis – pilnai ar dailinai autonominis orlaivis. Pagrindiniai valdymo tipai :

- antžeminis pilotas valdo orlaivį nuotoliu;
- dalinai autonominis – skrydžio misija atliekama autonomiškai, bet esant būtinybei antžeminis pilotas gali koreguoti parametrus;
- pilnai autonominė misija be žmogaus įsikišimo.



5 pav. BO klasifikavimas pagal sparno tipą

Bepiločių orlaivių sistemos (BOS) – šiai grupei priklauso visi su skrydžio misija susieja komponentai: tiek bepiločiai orlaiviai, tiek dronai, tiek juos valdantys operatoriai. Bepilotis orlaivis yra viena iš BOS rūšių, nes jis reiškia valdomą transporto priemonę arba orlaivį.



6 pav. BO klasifikacija pagal skrydžio parametrus

Nuotoliniu būdu valdomi orlaiviai (RPA) – nuotoliniu būdu valdomas orlaivis. Priklausomai nuo misijos sudėtingumo reikalingi antžeminio piloto įgūdžiai. Trūkumas: kuo sudėtingesnė misija, tuo didesnė tikimybė atsirasti žmogiškajai klaidai.. Priklausomai nuo misijos sudėtingumo reikalingi antžeminio piloto įgūdžiai. Trūkumas: kuo sudėtingesnė misija, tuo didesnė tikimybė atsirasti žmogiškajai klaidai.

1.4. Susidūrimo vengimo metodai

Šiuolaikiniai BO turi kolizijos sistemą leidžiančią interpretuoti jutiklių duomenis tam, kad būtų išvengiama susidūrimo. Tam būtina kiekvienu laiko momentu žinoti tikslų kiekvieno BO išdėstymą erdvėje. Orlaivio apsaugai naudojami atpažinimo priemonės, kurios veikia radijo dažnio perdavimo pagalba.

Kadangi BO nuolat artimai kontaktuoja, labai svarbu išvengti bet kokio jų susidūrimo. Todėl moksliniame straipsnyje „Mažo aukščio bepiločių orlaivių teikiamos daiktų interneto paslaugos: Išsami apžvalga ir ateities perspektyvos.“ buvo aptarti keli bepiločių orlaivių saugos modeliavimo ir vertinimo metodai, kurie taikomi bepiločių orlaivių sistemoms (BOS). Autoriai pristatė metodą, leidžiantį interpretuojant atpažinimo jutiklių duomenis modeliuoti ir vertinti susidūrimo vengimo sistemą. Sistemos veikimas derinamas su federaline aviacijos administracija [9]. Kitą susidūrimo vengimo metodą pristatė Finlis Barfieldas [10]. Moksliniame straipsnyje siūlomas metodas paremtas autonominio kolizijos vengimo sistema. Rezultatai parodė, kad tokia sistema nepadarė jokios įtakos BO misijai. Liangas Yangas sudarė kolizijos vengimo algoritmą BO judantiems plokštumoje [11]. Algoritmas susideda iš 2 vengimo sistemų: individualus kolizijos išvengimas iki bendros formacijos judėjimo ir grupinis kolizijos išvengimas kai BO juda sąlyginai mažoje aplinkoje su dideliu kiekiu kliūčių trijų demencijų aplinkoje. Kitą metodą pristatė mokslinis straipsnis „Bepiločių orlaivių klasterių susidūrimų vengimas naudojant spiečiaus intelekto metodus“[12], jis pagrįstas bepiločio orlaivio 3D kelio planavimu, kurį sudaro kelio be susidūrimų paieška užgriozdintoje 3D aplinkoje remiantis trimis pagrindiniais apribojimais: geometriniais, fiziniais ir laiko.

Yra pateikti įvairūs susidūrimo su kliūtimi vengimo metodai, skirti įveikti bet kokią kliūtį, su kuria susiduria bepiločiai orlaiviai. Dėsnį, leidžiantį tiksliai nustatyti netoliese esančių objektų buvimo vietą BO, pristatė Adamas Brandtas ir Markas Coltonas [13]. Kvadrakopteriai yra tinkamesni naudoti patalpose dėl jų lankstaus veikimo mažose ir ribotose erdvėse. Moksliniame straipsnyje „Automatinis rankiniu būdu valdomų bepiločių orlaivių susidūrimo išvengimo metodai“ [14] pateiktas algoritmas, leidžiantis nuotoliniu būdu valdyti bepiločius orlaivius, naudojant automatinį kliūčių išvengimo sistemą.

1.5. BO maršrutų valdymas ir komunikacijos technologijos

Svarbu užtikrinti saugų bepiločių orlaivių maršrutą, kad būtų išvengta nelaimingų atsitikimų, žalos ir sužalojimų. Norint tai padaryti reikia atsižvelgti į grėsmes, rizikas ir vietovę, taip pat į bepiločių orlaivių apribojimus. Tikimybinės autonominių bepiločių orlaivių tinklų kelio planavimo strategijos buvo stebimos taikant vietovėje esančias kliūtis [15]. Moksliniame straipsnyje „Daugiatikslis bepiločių orlaivių maršruto parinkimas“ [16] taikytas grafų teorija pagrįstas metodas daugiaobjektyviam maršruto planavimui, kad būtų laikomasi reikiamų saugos reikalavimų.

MTC (angl. „Machine Type Communication“) apibūdina duomenų perdavimą tarp dviejų subjektų nedalyvaujant žmogui. MTC įrenginių tarpusavio ryšiui palaikyti, per tinklą arba internetą, reikia pasirinkti tinkamą prieigos tinklą. Šie prieigos tinklai naudoja pažangius ryšio modelius, dėl kurių net mažame aukštyje skraidantys BO taps išmanesni [53]. Ryšio kategorijos:

1. Plačiajuostis ryšis – užtikrina didelę aprėptį. Naudojama: interneto tinkle, pavyzdžiui, *LTE*; ryšyje *Wimax*); palydoviniame ryšyje, pavyzdžiui *SATCOM* [53].
2. Trumpojo nuotoliu ryšys – naudojamas trumpo atstumo ryšiui palaikyti. Naudojama: *Zigbee* ir *Bluetooth* ryšiuose [53].

Techninių specifikacijų grupės paslaugos ir sistemos aspektai nurodo tris smulkaus duomenų perdavimo aspektus MTC technologijoje: 1) tinklas perduodamas informaciją palaiko minimalius nuostolius; 2) MTC abonentas gali būti prijungtas arba atjungtas nuo tinklo; 3) MTC tinklo įrenginys laisvai konfigūruojamas pagal poreikį [27].

Daiktų internetas apibūdina įrenginius su jutikliais, galimybę apdoroti informacija, naudojant programinę įrangą. Daiktų internetas apibūdina ryšio tinklą, kuriame du ar daugiau įrenginių keičiasi informacijos paketais. Telekomunikacijų technologijų pažanga leidžia valdyti dideliame aukštyje skrendančius bepiločius orlaivius iš didelio atstumo. 4G LTE ir 5G sistemos gali užtikrinti patikimą mobilųjį ryšį su bepiločiais orlaiviais, skirtais duomenims rinkti, apdoroti ir analizuoti. Dėl šio priežasties reikalingas patikimas ryšio palaikymas ir greitas duomenų paketų perdavimas. Daiktų internetas kartu su pažangia 5G sistema gali užtikrinti nepertraukiamą, tikslią ir patikimą BO misijos vykdymą [54].

BO panaudojimas auga paslaugų tiekimo sferoje. Pavyzdžiui, *Google* realizavo nedidelės aprėpties korinio ryšio technologiją *SkyBender*. BO siunčia ir priima signalus naudojant aukšto dažnio radijo signalus taip veikdami kaip aukšto lygio ryšio retransliavimo platforma ir užtikrinanti 5G ryšį. Rezultatai parodė, kad tokia platforma pasiekė iki 40 kartų didesnį perdavimo greitį nei 4G korinio ryšio tinklas [55].

Bevielis interneto ryšys: naujausi nuotolinio skraidančių transporto priemonių valdymo per bevielį ryšį pasiekimai leido valdyti bepiločius orlaivius net už regimosios matomumo linijos ribų. Be abejo,

viena iš galimybių suteikiančių šią funkciją bepiločiams orlaiviams yra korinio ryšio tinklų taikymas. Celė – tai geografinė teritorija, kurią aprėpia viena korinio ryšio tinklo bazinė stotis. Norint užtikrinti kokybišką ryšio tinklą, reikia naudoti persidengiančias bazines stotis. BO judant dinaminėje aplinkoje, bevielis interneto ryšys puikiai tinka komunikacijos palaikymui, nes celės užtikrina misijos teritorijos radijo ryšio aprėptį. Naudojant keletą fiksuotos vietos siųstuvų galima išplėsti ryšio aprėptį. Keli BS užtikrina natūralų dubliavimą taip, kad jei vienas ryšys yra prastas, kitas ryšys gali susilpnėjimą kompensuoti. Populiariausios korinio ryšio technologijos: globalinio ryšio sistema (GSM), universalioji ryšio sistema arba 3G, LTE arba 4G ir 5G.

Daugumoje civilinių bepiločių orlaivių ryšiui naudojamos pramoninės, mokslinės ir medicininės (ISM) dažnių juostos. Šių dažnių juostų transmisijos galia yra griežtai ribota, todėl skrydžio aprėptis yra ribota. Siekiant išvengti dažnių juostos pločio ir aprėpties apribojimų galima ryšiui naudoti korinio ryšio tinklus. Taip yra todėl, kad korinio ryšio tinklai gali užtikrinti plačią aprėptį ir didelį pralaidumą, ryšio įrenginiai yra nedideli, sunaudoja nedaug energijos ir yra masinės gamybos, o tai gali pagreitinti jų naudojimą praktiniame bepiločių orlaivių įgyvendinime.

Lauko bandymų eksperimente [17] analizuojamos 3G mažų bepiločių orlaivių kaip belaidžių retransliatorių, padedančių veikti korinio ryšio tinklui, taikymo galimybės, siekiant užtikrinti tinklo ryšį įprastomis sąlygomis nepasiekiamose teritorijose. Šio eksperimento rezultatai padidino interneto pralaidumo ir sumažino ryšio paketų perdavimo uždelsimą. Be to, palyginus mažus BO perdavimo našumą su alternatyviais apkrovos balansavimo ir statinio perdavimo metodais, galima teigti, kad vidutinis pralaidumas ir paslaugų kokybė yra geresni už esamus metodus.

WiMAX – bevielis plačiajuostis ryšys, kuris sparčiai perduoda duomenis radijo ryšiu. Lyginant *WiMax* su *Wi-Fi* pastebėta, kad *WiMax* ryšio palaikymas pigesnis, o aprėptis didesnė. Priklausomai nuo dažnių juostos, ši technologija taiko dažnio arba laiko dalijimo dalijimosi dupleksų konfigūracijas. Optimaliomis sąlygomis WiMax pasiekia iki 75 Mbps duomenų perdavimo greitį[18].

Rahmanas [18] mano, kad bepiločiu orlaiviu pagrįsta gelbėjimo sistema yra perspektyvus sprendimas gelbstint gyvybes kalnų aplinkoje. Atsižvelgiant į tinklo reikalavimus darbe aptariami esamų belaidžio ryšio technologijų iššūkiai, kad būtų galima užtikrinti bepiločių orlaivių ryšį ir nustatoma, kad *WiMAX* yra tinkama technologija šiai nepalankiai aplinkai. Priežastys, kodėl pasirinkta *WiMAX*, yra šios: 1) lankstumo, t. y. ji palaiko P2P ir tinklines sistemas; 2) paslaugų diferencijavimo, t. y. ji taiko skirtingus valdymo metodus pagal duomenų srauto tipus; 3) didesnio saugumo, t. y. joje įdiegti keli šifravimo, autentifikavimo ir saugumo metodai; 4) didesnio pralaidumo; 5) plačios aprėpties; 6) mobilumo, t. y. ji leidžia užmegzti ryšį iki 120 km/val. greičiu; 7) paprasto įdiegimo ir mažos kainos.

Kai bepiločiai orlaiviai dėl atstumo ar aplinkos kliūčių yra už tiesioginio ryšio ribų, ryšiui palaikyti naudojami palydoviniai ryšiai [20]. *BLoS* – tai technologijos arba sistemos, kurios išplečia belaidžio ryšio sistemų veikimo spindulį už šios ribos. Be to, vykdant bepiločių orlaivių operacijas palydovinis ryšys turi būti nuolat, kad būtų užtikrintas misijai svarbus ryšys.

Skinnemoenas [21] nurodė, kad SATCOM turi būti arba pačiame bepiločiame orlaivyje, arba kaip retransliatorius per žemę. Jis pateikia pagrindinius uždavinius, susijusius su SATCOM taikymu tiesioginiam nuotraukų ir vaizdo ryšiui per BO sistemą. Siūloma išspręsti keletą iššūkių (dažnių juostos pločio ribojimas ir perdavimo nuostoliai) susijusių su kritinės svarbos bepiločių orlaivių operacijomis. Be to, tyrime kalbama apie bepiločių orlaivių vaizdų perdavimo sistemą, pagrįstą palydovine retransliacija. Straipsnyje aptariamos pagrindinės specifikacijos, tokios kaip bepiločio

orlaivio ryšio perdavimo galia, vaizdo perdavimo sparta ir palydovo siuntimo žemyn galia. Lyginant bepiločių orlaivių oro duomenų perdavimą su palydoviniu duomenų perdavimu, nurodoma, kad palydovinė retransliacija užtikrina didesnį perdangos nuotolį, kai yra stabilus belaidžio kanalo veikimas ir užtikrina vaizdo perdavimą dideliu atstumu su gera vaizdo kokybe.

Wi-Fi – belaidžio ryšio technologija, apimanti standartų rinkinį, kuris naudoja radijo bangas, kad būtų užtikrinama interneto prieiga. Naudojamos 2,4, 3,6, 5 ir 60 GHz dažnių juostos [22]. Ši technologija naudojama skrydžio valdymui ir realaus laiko duomenims, pavyzdžiui, nuotraukų ir vaizdo perdavimui tarp BO ir ant žemės esančių įrenginių. [23] atliktas tyrimas sukūrė BO *Wi-Fi* prototipų sistemą, kurioje BO siunčia *Wi-Fi* signalą į avarines zonas. Naudojant kryptines antenas ir jų krypties valdymo mechanizmus galima padidint *Wi-Fi* signalo sklidimą iki 25km (optimaliomis sąlygomis), nors paprastai signalas sklidai iki 100m. Šis prototipas patvirtina galimybę sukurti *Wi-Fi* paslaugą naudojant lanksčią BO platformą. Lauko eksperimentuose sprendžiama antenų konfigūravimo BO pagrindu veikiančiuose tinkluose problematiką. Ji praneša apie belaidžio ryšio nuo BO iki antžeminės stoties našumo matavimą, naudojant gauto signalo stiprumo indikacija (RSSI), atstumą, neapdoroto ryšio sluoksnio pralaidumą ir antžeminės stoties aukštį. Šis eksperimentas palygina 32 vienu metu veikiančių BO ir antžeminių konfigūracijų porų veikimą ir daro išvadą, kad norint pasiekti didžiausią pralaidumą tiek BO, tiek antžeminė stotis turėtų naudoti horizontaliai išdėstytas įvairiakryptes antenas. 802.11a belaidžių ryšių taikymo BO ir antžeminės stoties rezultatai rodo, kad tai naudinga BO tinkle.

Bluetooth yra trumpo nuotolio ryšio protokolas, paprastai naudojama nesudėtingoms konfigūracijoms. Ryšiui palaikyti naudojama ISM dažnių spektro juosta (2,4GHz). Perdavimo greitis skirstomas į kategorijas: klasikinis iki 1Mbps, o naudojant pažangesnį BLE metodą iki 24Mbps [24]. Protokolas taikomas *Ad-hoc* tinkle ar periferinių ryšių palaikymui.

Zigbee – aukšto lygio protokolų rinkinys, naudojantis mažos galios siųstuvus. Ryšys naudojamas BO dėl mažos kainos, ilgo akumuliatoriaus tarnavimo laiko ir saugaus duomenų palaikymo. Mažo energijos suvartojimo funkcija užtikrina ilgesnį tarnavimo laiką, o tinklinis tinklas (*Mesh-Network*) užtikrina aukštą patikimumą ir didesnį diapazoną. ISM radijo dažnių juostos yra radijo spektro dalys, tarptautiniu mastu rezervuotos pramonės, mokslo ir medicinos reikmėms, išskyrus taikymą telekomunikacijų srityje. Ryšiui palaikyti naudojama ISM dažnių spektro juosta (2,4GHz) arba 9.15MHz dažnį nesudėtingoms komunikacijoms palaikyti. Duomenų perdavimo greitis optimaliomis sąlygomis siekia iki 250 kbps. *Zigbee* naudoja siaurajuosčius kanalus (5MHz) pločio. Protokolas puikiai tinka jutiklių duomenis analizuoti ir perduoti [25].

2. BO susidūrimo išvengimo spiečiuje matematiniai algoritmai

Skyriuje pasiūlytas metodas BO spiečiaus susidūrimo išvengimui. Klasteriai veikia susidūrimo išvengimo režimu su kitais klasteriais, jiems tenka papildoma užduotis išlaikyti saugų atstumą nuo kito klasterio narių ir iki minimumo sumažinti nuokrypį nuo pradinės judėjimo linijos pasiekus norimą saugų atstumą. Susidūrimo išvengimą sudaro 2 etapai: individualus kolizijos išvengimas ir grupinis kolizijos išvengimas.

2.1. Judėjimo lygtys

Judėjimo lygtis galima užrašyti išskaidant transporto priemonės greitį į tris komponentus.

$$\dot{x}=V\cos\theta\cos\Psi; \tag{2.1.1}$$

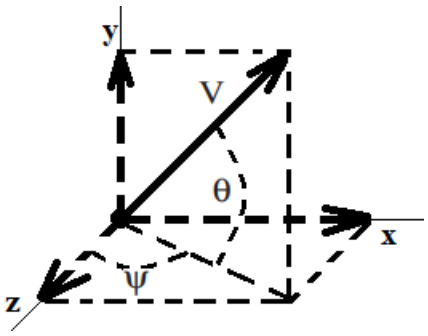
$$\dot{y}=V\cos\theta\sin\Psi; \tag{2.1.2}$$

$$\dot{z}=V\sin\theta. \tag{2.1.3}$$

, čia:

$$\dot{\Psi}=\frac{n_y}{V\cos\theta}; \tag{2.1.4}$$

$$\dot{\theta}=\frac{n_x}{V}. \tag{2.1.5}$$



7 pav. BO judėjimo erdvėje geometrija

7 pav. pateikta BO judėjimo erdvėje geometrija. Reikalingo kampo paieška panaši į menamo taško paieškas, kuris atitinka sekančio judėjimo taško koordinates. Esama ir reikiamo kampo skirtumas yra tiesiogiai proporcinga trajektorijos pokyčiui. Atitinkamos lygtys yra:

$$n_y=k\Delta\Psi; \tag{2.1.6}$$

$$n_x=k\Delta\theta; \tag{2.1.7}$$

$$\Delta\Psi=\Psi_{reikalingas}-\Psi; \tag{2.1.8}$$

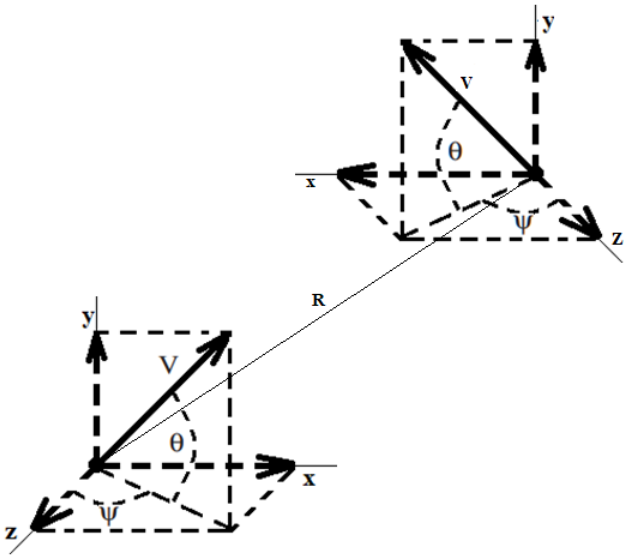
$$\Delta\theta=\theta_{reikalingas}-\theta; \tag{2.1.9}$$

, čia k yra pagreičio konstanta, o $\Psi_{reikalingas}$ ir $\theta_{reikalingas}$ yra pasirinkta kryptis ir posvyrio kampas naudojant judėjimo lygtis.

$$\Delta\Psi_{reikalingas} = \sum w_n \left(\Psi_{reikalingas_n} - \Psi\right); \quad (2.1.10)$$

$$\Delta\theta_{reikalingas} = \sum w_n \left(\theta_{reikalingas_n} - \Psi\right). \quad (2.1.11)$$

Lygties svoriai w_n keičiami remiantis judėjimo elgesiu.



8 pav. Dviejų BO susijusi geometrija

8pav. pateiktas dviejų susijusių BO geometrija. Tolimesniuose išraiškose taikoma ši sąsaja.

2.2. Sanglauda

Sanglauda – šis spiečiaus parametras leidžia BO grupės nariams išlikti pakankamai arti vienas kito. Sanglaudos taisyklė apibrėžiama kaip išėjimo greičio vektorius, kuris leidžia BO pereiti prie kitų BO jutiklių diapazone ir taip išvengiant susidūrimo.

Tarkime, spiečiuje yra n_i orlaivių, kurie yra i-tojo BO jutiklių matomumo lauke ir koordinatės (X_{Si}; Y_{Si}; Z_{Si}) yra centras visų n_i orlaivių. Siekiant įgyvendinti sanglaudos taisyklę, i-tasis BO turi persekioti centrą nepaliekant jo už jutiklių ribų. Norimas krypties kampas ir posvyrio kampas sanglaudai pateikti kaip:

$$\Psi_{Si} = \arctan\left(\frac{Y_{Si} - Y_i}{X_{Si} - X_i}\right); \quad (2.2.1)$$

$$\theta_{Si} = \arctan\left(\frac{Z_{Si} - Z_i}{\sqrt{(X_{Si} - X_i)^2 + (Y_{Si} - Y_i)^2}}\right). \quad (2.2.2)$$

2.3. Sekimas

Sekimas – dėl šio elgesio kiekvienas BO seka vieną iš dviejų BO, iš kurių vienas yra artimiausias BO, o kitas yra atsitiktinai parinktas BO. Tegul (X_{Ni}; Y_{Ni}; Z_{Ni}) yra BO, esančios arčiausiai i-tojo BO, (X_{Ri}; Y_{Ri}; Z_{Ri}) yra bet kurio atsitiktinai pasirinkto BO koordinatės ir (X_i; Y_i; Z_i) yra i-tojo BO koordinatės. Norint įgyvendinti šią taisyklę, norima kryptis Ψ_{Fi} ir nuolydžio kampas θ_{Fi} gaunami taip:

$$\Psi_{Ri} = \arctan\left(\frac{Y_{Ri} - Y_i}{X_{Ri} - X_i}\right); \quad (2.3.1)$$

$$\theta_{Ni} = \arctan\left(\frac{Z_{Ri} - Z_i}{\sqrt{(X_{Ri} - X_i)^2 + (Y_{Ri} - Y_i)^2}}\right); \quad (2.3.2)$$

$$\Psi_{Ni} = \arctan\left(\frac{Y_{Ni} - Y_i}{X_{Ni} - X_i}\right); \quad (2.3.3)$$

$$\theta_{Ni} = \arctan\left(\frac{Z_{Ri} - Z_i}{\sqrt{(X_{Ni} - X_i)^2 + (Y_{Ni} - Y_i)^2}}\right); \quad (2.3.4)$$

$$\Psi_{Fi} = \frac{\Psi_{Ri} + \Psi_{Ni}}{2}; \quad (2.3.5)$$

$$\theta_{Fi} = \frac{\theta_{Ri} + \theta_{Ni}}{2}. \quad (2.3.6)$$

2.4. Grįžimas

Grįžimas – elgsena leidžia BO judėti link signalo šaltinio. Grįžimo koordinatės apibrėžtos kaip (X_{Gi}; Y_{Gi}; Z_{Gi}). Norimą nukreipimo kryptį ir žingsnio kampus nurodo:

$$\Psi_{Gi} = \arctan\left(\frac{Y_{Gi} - Y_i}{X_{Gi} - X_i}\right); \quad (2.4.1)$$

$$\theta_{Gi} = \arctan\left(\frac{Z_{Si} - Z_i}{\sqrt{(X_{Gi} - X_i)^2 + (Y_{Gi} - Y_i)^2}}\right). \quad (2.4.2)$$

2.5. Išsklaidymas

Išsklaidymas – judėjimas paremtas BO grupės narių minimalaus atstumo palaikymu. Jo išvesties kampas yra toks, kad BO nutolsta nuo kitų BO, kurie yra per arti jo. Tegul BO centras i-tojo BO d_{min}. diapazone yra (X_{Ci}; Y_{Ci}; Z_{Ci}). Norima dispersijos kryptis ir žingsnio kampai pateikiami pagal:

$$\Psi_{Ii} = \arctan\left(\frac{Y_i - Y_{Ci}}{X_{Ci} - X_i}\right); \quad (2.5.1)$$

$$\theta_{Ii} = \arctan\left(\frac{Z_{Si} - Z_i}{\sqrt{(X_{Ci} - X_i)^2 + (Y_{Ci} - Y_i)^2}}\right). \quad (2.5.2)$$

2.6. Lygiavimas

Lygiavimas – elgesys, reikalingas tam, kad būtų sukurta tam tikra BO spiečiaus judėjimo tvarka ir padėtų grupei judėti kaip visumai. Lygiavimas yra grupinės formacijos etapas, kurio metu žinomas kiekvieno n_i BO greitis, kad nei vienas BO neišsiskirtų iš formacijos judėjimo. Reikalinga išlygiavimo kryptis ir žingsnio kampai pateikiami pagal:

$$\Psi_{Li} = \left(\frac{1}{n_i}\right)\sum_{j=1}^{n_i} \Psi_j; \quad (2.6.1)$$

$$\theta_{Li}=\left(\frac{1}{n_i}\right)\sum_{j=1}^{n_i}\theta_j. \quad (2.6.2)$$

2.7. Grupinis kolizijos išvengimas

Grupinis kolizijos išvengimas – pilnai susiformavusio spiečiaus judėjimas nesusiduriant. w_{GSi} – lygties koeficientas, skirtas išlaikyti visus BO atitinkamai nutolusios vienos nuo kito po kiekvieno manevro. Grupės susidūrimo vengimo principas gali būti įgyvendinamas naudojant toliau pateiktas lygtis, pagal kurias apskaičiuojamas i-tojo BO vengimo taisyklės svoris:

$$w_{GSi}=\begin{cases}1, & \text{jei } \left(P_i-C_{p_i}\right)\le\rho_{GKI}\\ 0, & \text{jei } P_i-C_{p_i})\ge\rho_{GKI}\\ 0, & \text{visa jei atvėjis kitas}\end{cases}. \quad (2.7.1)$$

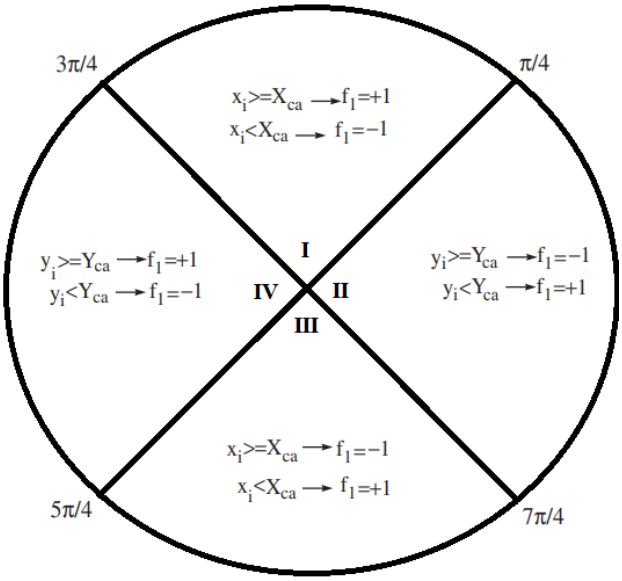
Pageidaujamas i-tojo bepiločio orlaivio kurso išvengimo kampas nustatomas:

$$\Psi_{GSi}=f_i\left(\frac{\pi}{2}\right)+\Psi_i; \quad (2.7.2)$$

, čia posūkio kryptis f_i, reikalinga išvengti susidūrimų horizontalioje plokštumoje, nustatoma pagal 2.7.3 formulę, kur (X_{GS}; Y_{GS}; Z_{GS}) koordinatės yra spiečiaus bepiločių orlaivių centras.

$$f_i=\begin{cases}1, \text{ kai } \left(\frac{\pi}{4}<\Psi_i\le\frac{3\pi}{4}\right) \text{ ir tenkinama sąlyga, kad } x_i\ge X_{GS}\\ -1, \text{ kai } \left(\frac{\pi}{4}\le\Psi_i\le\frac{3\pi}{4}\right) \text{ ir tenkinama sąlyga, kad } x_i<X_{GS}\\ -1, \text{ kai } \left(\frac{5\pi}{4}<\Psi_i\le\frac{7\pi}{4}\right) \text{ ir tenkinama sąlyga, kad } x_i\ge X_{GS}\\ 1, \text{ kai } \left(\frac{5\pi}{4}\le\Psi_i<\frac{7\pi}{4}\right) \text{ ir tenkinama sąlyga, kad } x_i<X_{GS}\\ 1, \text{ kai } \left(\frac{3\pi}{4}<\Psi_i\le\frac{5\pi}{4}\right) \text{ ir tenkinama sąlyga, kad } y_i\ge Y_{GS}\\ -1, \text{ kai } \left(\frac{3\pi}{4}\le\Psi_i<\frac{5\pi}{4}\right) \text{ ir tenkinama sąlyga, kad } y_i<Y_{GS}\\ -1, \text{ kai } \left(\frac{7\pi}{4}<\Psi_i\le\frac{\pi}{4}\right) \text{ ir tenkinama sąlyga, kad } y_i\ge Y_{GS}\\ 1, \text{ kai } \left(\frac{7\pi}{4}\le\Psi_i\le\frac{\pi}{4}\right) \text{ ir tenkinama sąlyga, kad } y_i<Y_{GS}\end{cases}. \quad (2.7.3)$$

2.7.3 formulės taisyklę galima paaiškinti taip: Siekiant išvengti susidūrimo, abu bepiločiai orlaiviai turi judėti normaliai lyginant su pradine kryptimi, kad atstumas tarp jų padidėtų. 9 pav. pateiktas loginis kolizijos išvengimo skirstymas. Atliekant manevrą BO tikriną sritis pakaitomis pradedant nuo srities į kurią nukreiptas to BO greitis.



9 pav. Loginis kolizijos išvengimo erdvės skirstymas

Jei greičio vektoriau kryptis II ir IV srityse, tai BO lygina x koordinates. Kitu atveju (I ir III sritys) – y koordinates.

Reikalinga posvyrio ir posūkio kampai randami:

$$\theta_{GSi} = f_2\left(\frac{\pi}{2}\right) + \theta_i ; \tag{2.7.3}$$

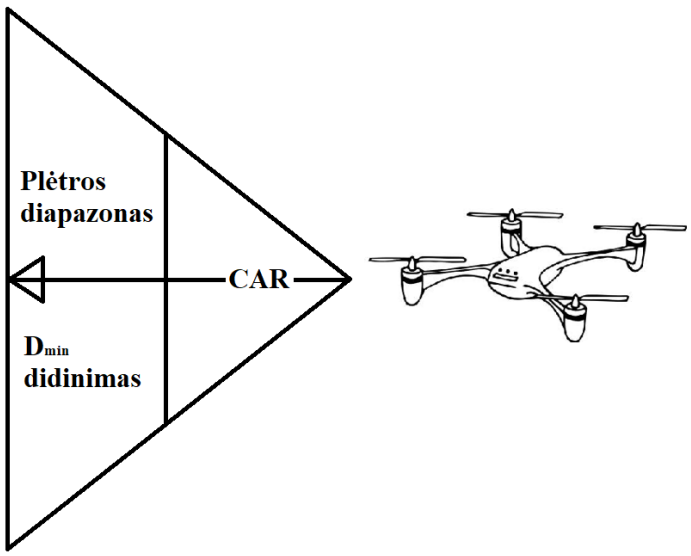
, čia:

$$f_2 = \begin{cases} 1, \text{ jei tenkinama sąlyga } z_i \geq Z_{GS} \\ -1, \text{ jei tenkinama sąlyga } z_i < Z_{GS} \end{cases}. \tag{2.7.4}$$

Siekiant išvengti dviejų BO vienodų sprendimų, jie pasirenkami lyginant bepiločio orlaivio padėtį (x_i; y_i; z_i), su kito bepiločio orlaivio centru (X_{GS}; Y_{GS}; Z_{GS}). Dėl to posūkio kryptis f_1 ir f_2 gali būti skirtinga, todėl kyla konfliktų ir vienas ar daugiau bepiločių orlaivių, vykdydami susidūrimo vengimo veiksmus, gali nutolti nuo grupės. Šioje schemoje posūkio kryptis nustatoma atsižvelgiant į centrą (X_{GSi}; Y_{GSi}; Z_{GSi}),o ne į atskiras padėtis (x_i; y_i; z_i), todėl visoms grupės BO suteikiama vienoda posūkio kryptis f_1 ir f_2, taip išvengiant konflikto.

2.8. Individualus susidūrimo vengimas

Individualus susidūrimo vengimas labai panašus kaip ir grupinio susidūrimo vengimas, tik lygčių koeficientai skiriasi. Individuliam susidūrimo išvengimui siūlomas jutiklių panaudojimas, kurių grafinis diapazonų vaizdas pateiktas 10 pav. Mažiausias leistinas atstumas tarp dviejų BO d_{min} grupėje yra nustatytas kaip:



10 pav. Individualaus susidūrimo mažinimas remiantis jutikliais

$$d_{min}=\begin{cases} d_1, \text{ jei } \left(P_i\text{-}C_{p_i}\right)\leq\rho_{ICA} \\ d_2, \text{ jei } \left(P_i\text{-}C_{p_i}\right)\geq\rho_{ICA} \\ d_1>d_2 \end{cases}. \quad (2.8.1)$$

Vengimo taisyklės svoris, kurso kampas ir posūkio kryptis, vengimo nuolydžio kampas ir kryptis nustatomi taip pat kaip ir grupiniam susidūrimui pagal 2.7.1 – 2.7.4 formules. Aptikus svetimus bepiločius orlaivius plėtros jutiklio veikimo zonoje, d_{min} padidinamas nuo d_2 iki d_1, kad visa grupė išsiplėstų ir svetimas bepilotis orlaivis galėtų praskristi pro šią grupę. O kai svetimas BO patenka į susidūrimo išvengimo diapazoną, imamasi susidūrimo išvengimo veiksmų. Šiuo atveju, priešingai nei susidūrimo vengimo pagal grupes atveju, w_c sumažinamas, kad būtų galima lengvai plėstis.

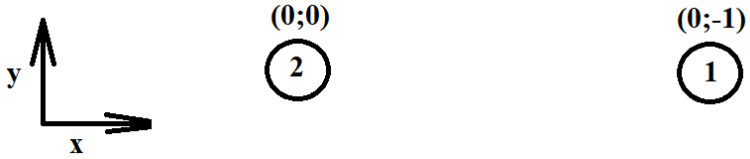
3. Tyrime naudojamo spiečiaus struktūra

Laisvai pasirinkta, kad BO spiečių sudaro 10 orlaivių. 9 agentai ir 1 lyderis . Spiečius juda 2D erdvėje. Toliau skyriuje pateikiama tokio spiečiaus veikimo logika.

3.1. Spiečiaus formavimasis

Spiečiaus formavimasis susideda iš 3 pagrindinių žingsnių: formacijos, judančios formacijos ir susidūrimo vengimo.

1. Formacija – procesas, kurio metu komponentas iš ten kur yra, atsiduria ten kur turi būti.



11 pav. Formacijos pavyzdys

11 pav. pavaizduotas formacijos pavyzdys. Tarkim, komponentas 1 turi atsidurti ten kur yra komponentas 2. Tai:

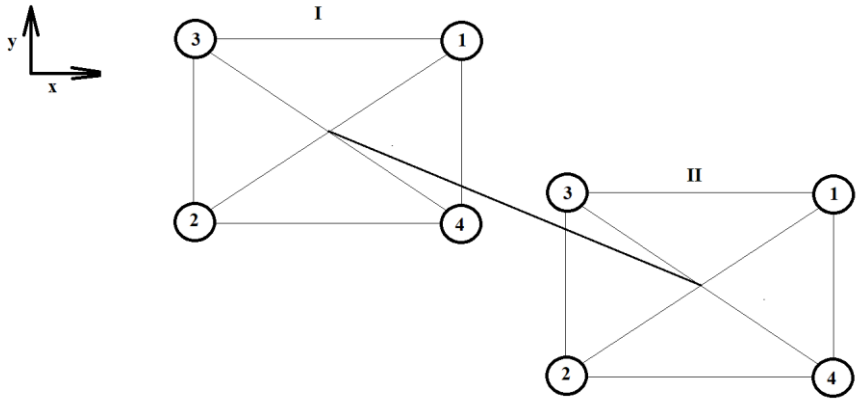
$$Pos_{esama} - Pos_{būsima}; \quad (3.1.1)$$

, arba

$$(-1{:}0)_{esama} - (Pos_x; Pos_y); \quad (3.1.1)$$

, kur $(Pos_x; Pos_y)=(0;0)$;

2. Grupinė formacija – procesas, kurio metu grupė komponentų iš ten kur yra, atsiduria ten kur turi būti.



12 pav. Grupinės formacijos pavyzdys

12 pav. pavaizduotas grupinės formacijos pavyzdys. Tarkime, kad grupė I, kuri susideda iš 4 komponentų, turi atsidurti ten kur yra grupė II. Iš esmės, grupės I centras juda link grupės II centro.

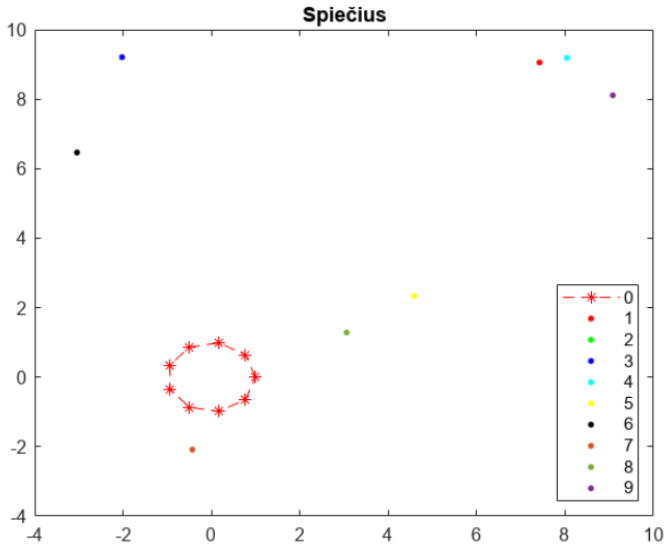
Tam išvedamas dydis K_c – formacijos koeficientas, kuris parodo kaip arti turi būti komponentai, kad jie judėtu kaip grupė.

3. Susidūrimo išvengimas – procesas, kurio metu komponentai nekerta vienas kito trajektorijos, tuo pačiu laiko momentu.

Proceso loginė seka aprašyta 2 skyriuje.

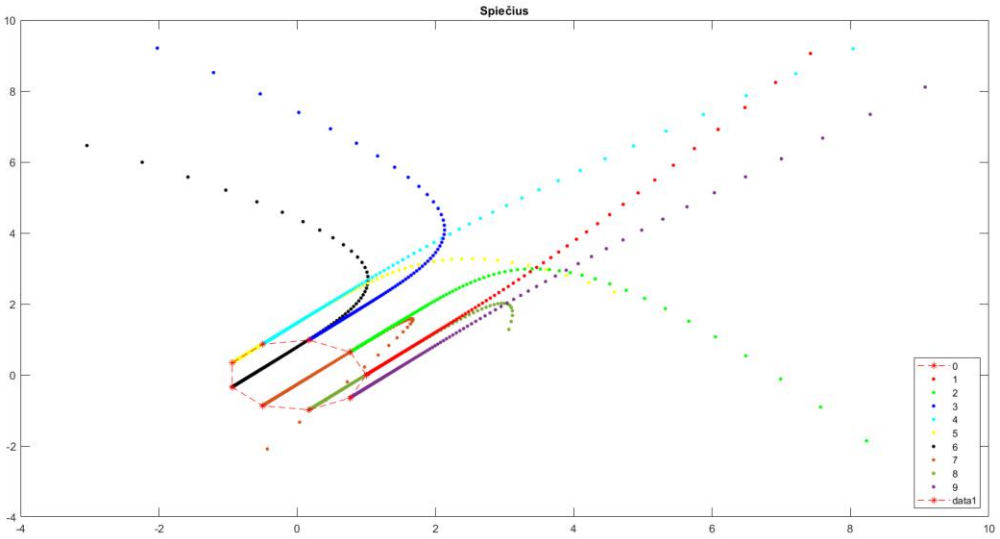
3.2. Spiečiaus struktūros realizavimas *Matlab* programinėje aplinkoje

Realizacijos logikai pateikti naudojami tik 9 BO, be lyderio. Lyderio įtaka spiečiaus kontrolei bus aptarta tolimesniuose skyriuose.



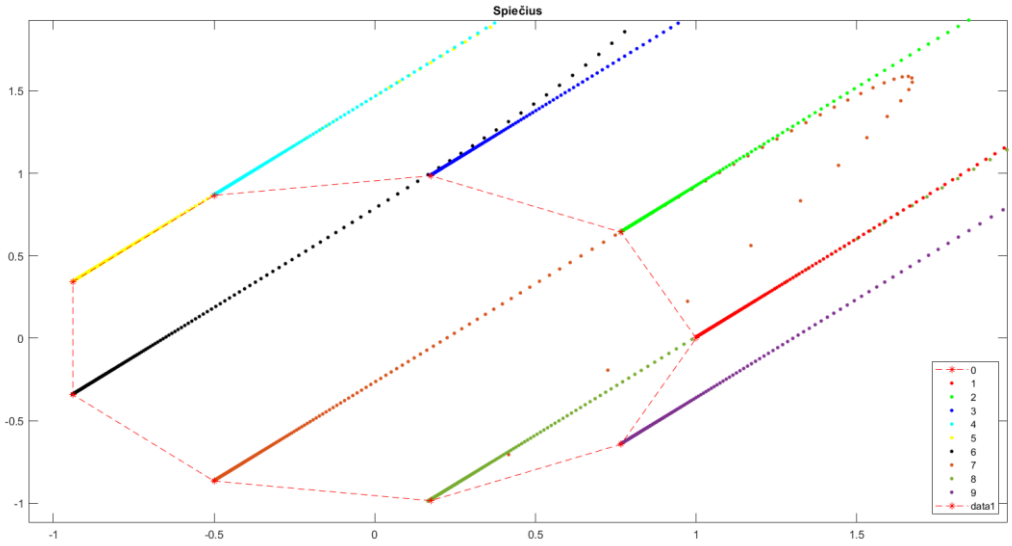
13 pav. Spiečiaus pradinis išsidėstymas

13 pav. Pateiktas spiečiaus pradinis išsidėstymas. Jį sudaro 9 orlaiviai išdėstyti atsitiktinėje erdvėje ([-4:10];[-4:10]). Žvaigždutėmis pažymėtas 9 kraštinių daugiakampis – tikslas kuriame turi atsidurti visi 9 BO.



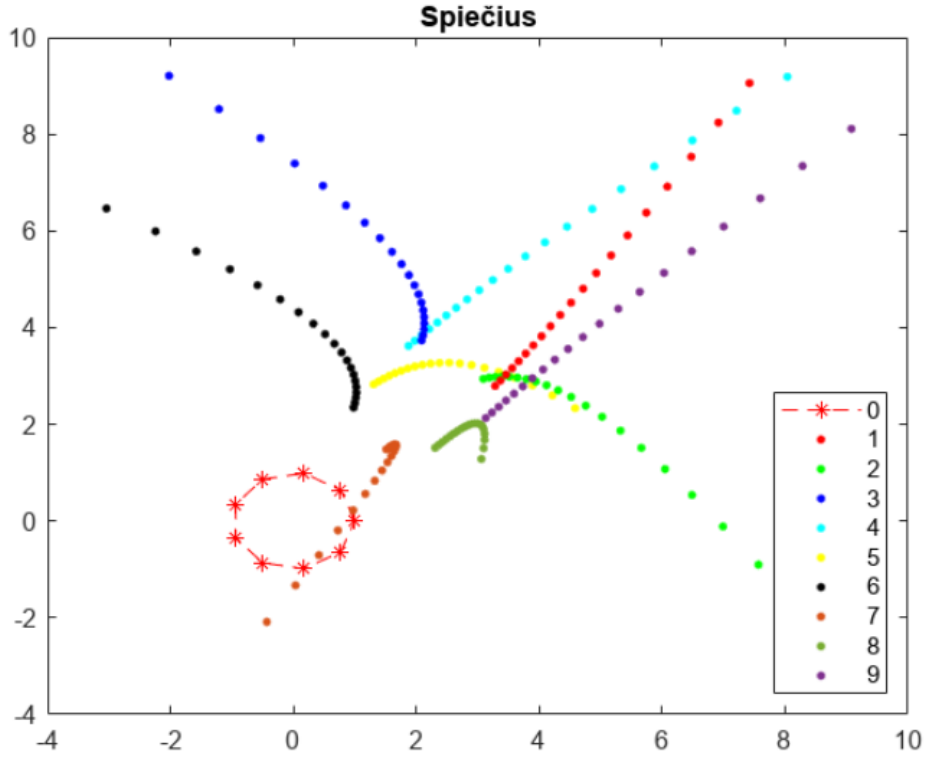
14 pav. Skaičiavimų rezultatai

14 pav. pavaizduoti skaičiavimų rezultatai *Matlab* programinėje įrangoje, naudojant 2 ir 3.1 skyrių logika. Galima teikti, kad tokia logika tinkama, nes BO pasiekė savo tikslą.



15 pav. Tikslas

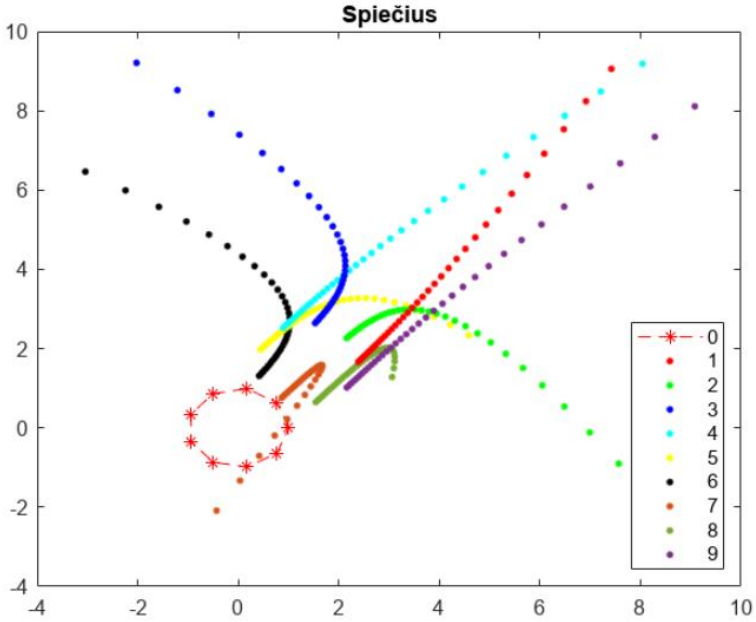
15 pav. pateiktas skaičiavimų rezultatų tikslo vaizdas. 9 BO atsitiktinai paskirstyti erdvėje (*randi([-5,10],9,2)* pasiekė tikslą (*t = linspace(0,1,10);x = cos(t.*2*pi); y = sin(t.*2*pi))* nenukrypdami. Nuokrypis iki 1%. Tikslūs skaičiavimo rezultatai pateikti 2 priede.



16 pav. Susidūrimo išvengimas

16 pav. pateiktas susidūrimo išvengimo vaizdas. 9 BO susitinka glaustoje erdvėje. Jų trajektorijos kertasi, bet skirtingu laiko momentu. Agentų greičiai iki formacijos skirtingi, toliau nuo menamo

formacijos taško esantys orlaiviai juda didesniu greičiu (didesni tarpai tarp simuliacijos taškų), po formacijos – greitis vienodas, jei judama tiesia linija.



17 pav. Grupinis formacijos koeficientas

17 pav. pateiktas grupinio formavimosi koeficiento įtaka 9 BO judėjimui. Šis reiškinys parodo, kaip BO išvengia susidūrimo kai erdvė tampa glausta ir jų trajektorijos kertasi. Galima nenaudoti grupinės formacijos prieš pasiekiant tikslą, bet tada sunkiau pavaizduoti susidūrimo išvengimą, t.y. užduoties vykdymo tikslumui grupinis formacijos koeficientas įtakos neturi.

3.3. Pilnai autonominis spiečius

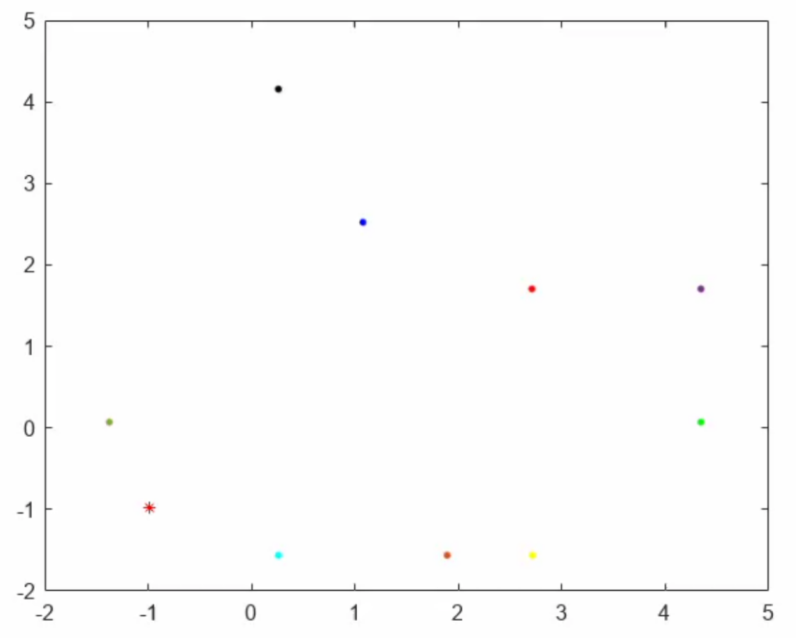
Dabartiniai autonominiai BO spiečiai taiko *Master-Slave* modelį. Taikant *Master-Slave* modelį, BO spiečiaus lyderis gauna vieną ar daugiau užklausų ir generuoja užduotis, kurias vykdo agentai. Paprastai lyderis kontroliuoja pavaldžiųjų subjektų skaičių ir kiekvieno pavaldžiojo subjekto atliekamus veiksmus. Agentas veikia nepriklausomai nuo kitų agentų.

3.4. Pilnai autonominio spiečiaus kontrolė

Pilnai autonominio spiečiaus kontrolės raliavimui pasirinkta naudoti panašią logiką, kaip ir 3.2 poskyryje. Siekiant pateikti kuo geresnį vaizdavimo aiškumą, grafikų legenda pateikta atskirai 18 pav.

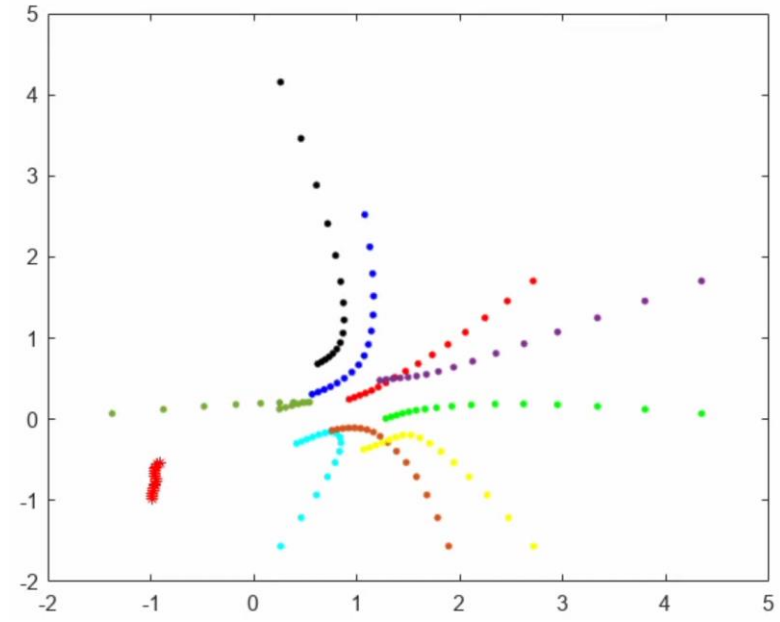
18 pav. Legenda

Spiečių sudaro 10 BO iš kurių vienas yra lyderis. Pirminis spiečiaus išsidėstymas pasirinktas naudojant atsitiktines funkcijas. Tokio BO spiečiaus pradinis vaizdas pateiktas 19 pav.



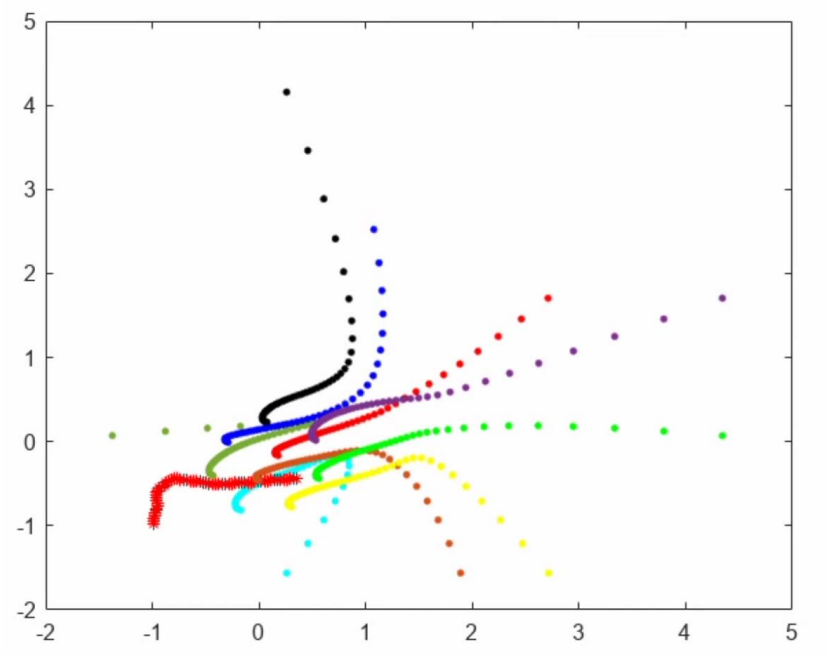
19 pav. Spiečiaus pradinė padėtis

20 pav. pateikta pirminė spiečiaus formacija. BO lyderis juda atsitiktinai. BO agentai pirmiausia susiformuoja į pirminę formaciją, siekiant išvengti susidūrimo. Toliau agentai seka lyderį. Spiečiaus agentai susiformuoja kiek įmanoma greičiau, kad spiečiaus lyderis nenutoltu nuo likusio BO spiečiaus.



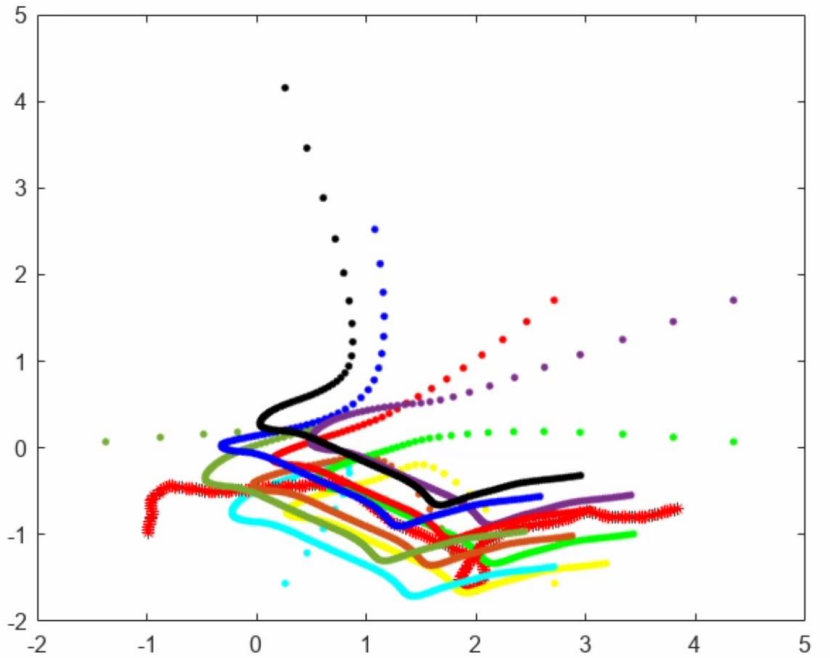
20 pav. Spiečiaus formacija

21 pav. pateiktas spiečiaus posūkis, kuriame dalyvauja visi agentai sekdami lyderį Agentai taiko susidūrimo vengimo vienas nuo kito metodą, o lyderis laikosi 1,5 menamo atstumo nuo kiekvieno agento.



21 pav. Posūkis

22 pav. pateikta imituota spiečiaus užduotis. Užduotis – spiečius juda 8 sekundes nesusidurdamas. 8 sekundės pasirinktos dėl vaizdavimo aiškumo. Visą užduotą judėjimo laiką agentai ir lyderis juda kaip bendras vienetas, lyderis diktuoja trajektorija, agentai ją seka.

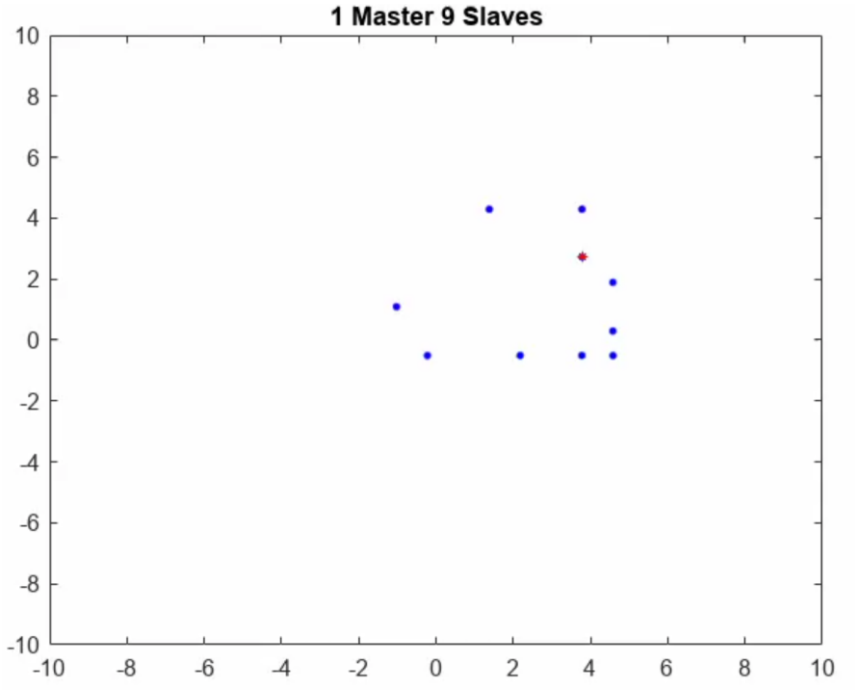


22 pav. Imituota užduotis

BO nesusidūrė, agentai seka lyderį, posūkiai atliekami naudojant susidūrimo vengimą, todėl galima teikti, kad *Master-Slave* spiečiaus kontrolė realizuota. Tikslios judėjimo koordinatės nepateiktos, nes spiečiaus judėjimas paremtas 3.2 poskyrio logika.

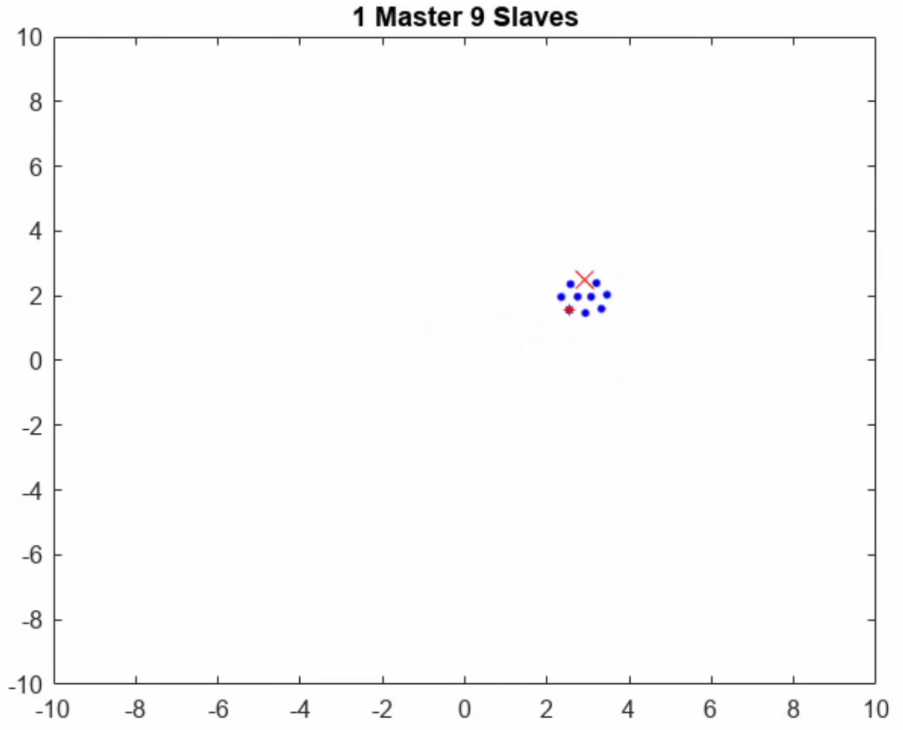
3.5. BO spiečiaus lyderio pakeitimas, kai imituojama potenciali ataka

Poskyryje pateiktas scenarijus, kai nulaužiamas spiečiaus lyderis, o atsitiktinis agentas perima jo funkcijas ir kontrolę.



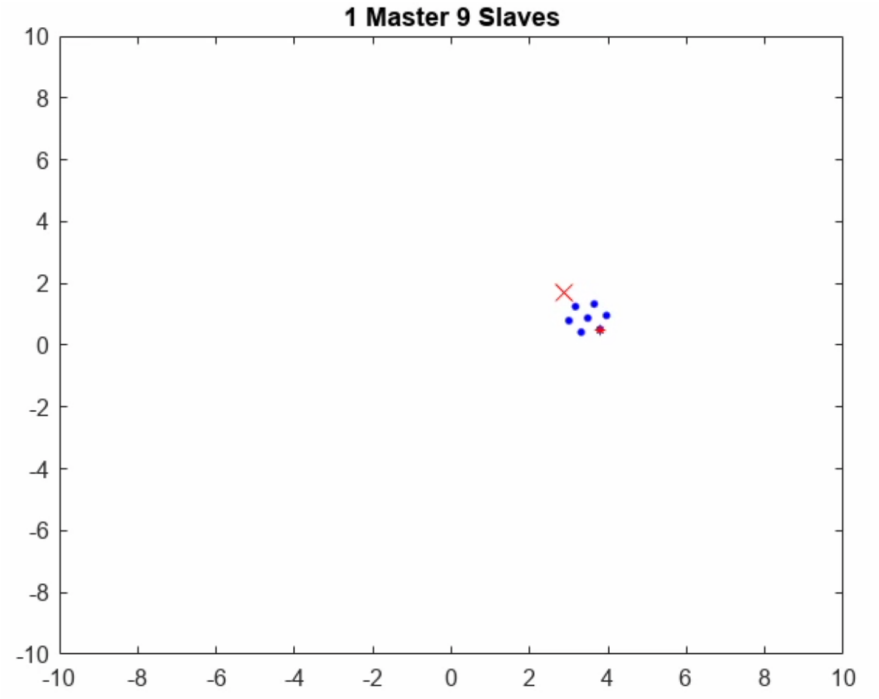
23 pav. Pirminis išsidėstymas

23 pav. pateiktas pirminis spiečiaus išsidėstymas, kurį sudaro 9 agentai ir 1 BO spiečiaus lyderis. Spiečiaus užduotis tokia pat kaip 3.4 poskyryje.



24 pav. Imituojamas pirmi lyderio nulaužimas

24 pav. pavaizduotas pirmo lyderio nulaužimas. Spiečius sumažėja 1 vienetu, o lyderio funkcijas perima kitas, atsitiktinis agentas. Spiečius juda toliau ir tęsia užduotį.



25 pav. Imituojamas antro lyderio nulaužimas

25 pav. pateiktas imituojamas antro lyderio nulaužimo vaizdas. Persiskirstymo užduotimis seka tokia pat kaip ir pirmo lyderio nulaužomo atveju. Lyginat 24 pav. ir 25 pav. matoma, kad spiečius persiformuoja priklausomai nuo likusių orlaivių skaičiaus.

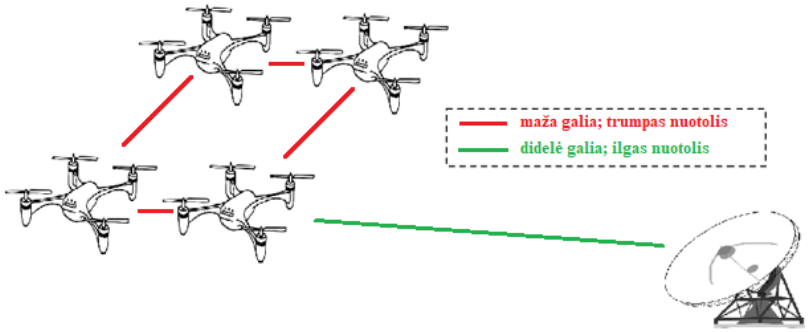
Spiečius visą simuliacijos laiką judėjo nesusidurdamas ir sekdamas lyderį nepriklausomai, kuris agentas yra BO spiečiaus lyderis. Net ir pasikeitus lyderiui spiečiui išlaiko formacijos reikalavimus, persiformavimas vyksta be strigimų, todėl galima teikti, kad toks lyderio pakeitimas misijos atlikimo eigoje yra teisingas.

4. BO spiečiaus infekavimo būdai

Skyriuje daugiausia dėmesio skiriama FANET (angl. „flying ad-hoc network“). Siekiama pateikti BO spiečiaus kontrolės grėsmes ir jų klasifikavimus.

4.1. FANET

Tarkim, spiečių sudaro 10 magistralinių BO. Magistraliniai BO – turi didesnį ryšio pralaidumą, didesnius skaičiavimo pajėgumus ir didesnę belaidžio ryšio aprėptį nei kiti misijos BO. Tokiu atveju, kiekvienas spiečiaus agentas gali būti lyderis. Architektūra pateikta 27pav.

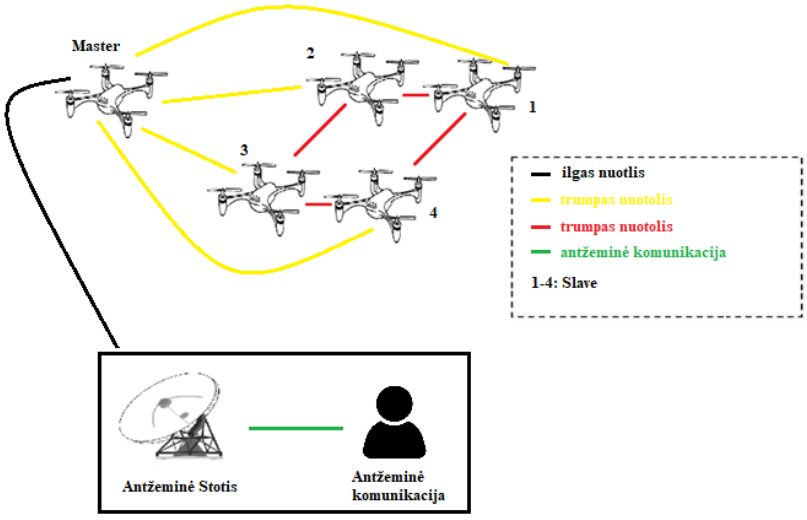


26 pav. Decentralizuota BO spiečiaus architektūra, kai naudojamas lyderis

Remiantis 26 pav. pateikta architektūra, galima daryti išvadą, kad spiečiaus lyderis naudoja didelę galią, kad galėtų pasiekti antžeminę stotį, o su kitais spiečiaus agentais komunikuoja trumpais atstumais ir naudodamas mažą galią. Šis procesas veiksmingai išplečia bepiločių orlaivių tinklo aprėptį ir tinka mažiems bepiločiams orlaiviams su lengvais siųstuvais.

4.2. Saugumo grėsmių vektoriai FANET tinkle

Poskyryje pateiktos FANET tinklo saugumo spragos. 11 pav. pateiktos saugumo grėsmės remiantis šių grėsmių vektoriaus. Grėsmių vektorių rinkinį sudaro 6 jungčių ir 2 mazgų tipai.



27 pav. Saugumo grėsmės BO FANET tinkle

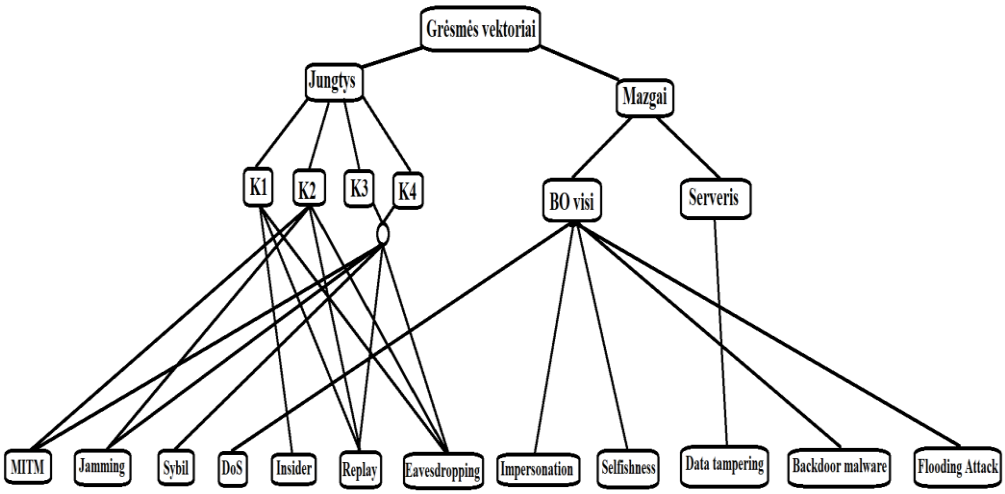
Iš esmės grėsmių vektorius galima klasifikuoti:

1. Antžeminė komunikacija (K1) – komunikacija tarp kliento ir antžeminės stoties.
2. Ryšys tarp antžeminės stoties ir BO spiečiaus lyderio (K2). Komunikacijos tipai: interneto, radijo arba palydovinis ryšys.
3. Ryšys tarp pagrindinio bepiločio orlaivio ir kitų bepiločių orlaivių (K3).
4. Ryšys tarp agentų FANET tinkle (K4).

Ryšys tarp antžeminės stoties ir BO spiečiaus lyderio (2 grėsmės vektorius) gali būti apibrėžtas kaip ryšys su serveriu tarp lyderio BO ir kitų bepiločių orlaivių arba antžeminių įrenginių. Antžeminiai įrenginiai apima komunikacija tarp kliento ir antžeminės stoties. Esant poreikiui galima panaudoti serverį, kaip BO spiečiaus lyderio galimybių padidinimą.

4.3. Saugumo grėsmės ryšiams ir mazgams

Saugumo grėsmes mazgams ir ryšiams galima apibrėžti naudojant STRIDE (*Spoofing identity; Tampering with data; Repudiation; Indormation dislosure; Denial of service; Elevation of privilege*) modelį. STRIDE yra *Microsoft* kompanijos kompiuterinio tinklo saugumo modelis, kurio kiekvieną raidė atitinka pažeidžiamumo įvertinimo etapą: S – autentiškumas (*Authentication*); T – vientisumas (*Integrity*); R – neatmetimas (*Non-repudiation*); I – konfidencialumas (*Confidentiality*); D – prieinamumas (*Availability*); E – autorizacija (*Authorization*);



28 pav. Saugumo grėsmės ryšiams ir mazgams

29 pav. pateikta saugumo grėsmių vizualizacija ryšiams ir spiečiaus mazgams. Jungtys ir mazgai aprašyti 5.2 poskyryje. K1: komunikacija tarp kliento ir antžeminės stoties. Šio belaidžio ryšio gali būti klausomasi (*Eavesdroping*), kliento terminalas gali būti piktavališkai valdomas arba užkrėstas kenkėjiškomis programomis. Grėsmės:

- Ryšio pasiklausymas (*Eavesdroping*) – pasyvia ataka. Užpuolikas pasyviai per tinklą klausosi pranešimo, kad gautų svarbios informacijos (prisijungimo raktas; BO komunikacijos paketai) neklastodamas duomenų.
- Grėsmė, kylanti iš vidaus (*Insider*) – užpuolikas manipuliuoja duomenimis, kad pakenktų FANET, užpuolikas vadinamas *Insider*. Ataka įgyvendinama, jei užpuolikas žino BO spiečiaus išsidėstymo erdvėje koordinates.

- Pakartojimo ataka (*replay*) – ataka koncentruota į antžeminės stoties paveikimą. Net neiššifravus panešimų galima juos pakartotinai siųsti į antžeminę stotį. Atlikus ataką, ryšys perimamas, nes sukuriamas dar vienas komunikacijos kanalas dėl didelio kiekio pasikartotinų pranešimų.

K2: Ryšys tarp antžeminės stoties ir pagrindinio bepiločio orlaivio. Paprastai komunikacijai palaikyti naudojamas interneto ryšys . Jei autentifikavimo metodai nėra tinkamai sukonfigūruoti, šie protokolai gali tapti pasiklausymo arba žmogaus viduryje (MITM) atakų objektu. K2 ryšio palaikymo metodai ir metodų grėsmės saugumui:

- Bevielis internetas (*WiFi*) – belaidžio ryšio technologija, apimanti standartų rinkinį, kuris naudoja radijo bangas, kad būtų užtikrinama interneto prieiga. Naudojamos 2,4, 3,6, 5 ir 60 GHz dažnių juostos. Pasiklausymo arba MITM atakos pavojingos, nes naudojama sąlyginai paprastai dešifruojamas autentifikavimo raktas.
- Radijo dažnis (RF) – žemo dažnio ryšio tipas. Radijo sklidimo atveju taikomas trukdžių mažinimo metodas, o skrydžio valdymui naudojamas aukštakryptis ryšys, o telemetriniams ir naudingojo krovinio duomenims perduoti – žemakryptis ryšys. Norint išvengti signalo trukdžių reikia naudoti sunkiai pasiekiamus radijo dažnius.
- Palydovinis ryšys – saugesnis ryšio tipas nei radijo ar *Wi-Fi* ryšiai, bet palikymo kaina didesnė. Naudojant palydovinį ryšį sukuriamas kanalas tarp siųstuvo ir imtuvo, kurie gali būti nutolę vienas nuo kito.

K2 ryšio grėsmės:

- Ryšio pasiklausymas (*Eavesdroping*). Panašiai kaip ir pasiklausymo atakos K1 vektoriui. Užpuolikas pasyviai per tinklą klausosi pranešimo, kad gautų svarbios informacijos neklastodamas duomenų.
- Trikdymas (*Jamming*). Gali atsirasti dėl tyčinių arba netyčinių priežasčių. Trikdžius gali sukelti trys trukdymo modeliai: 1) pastovaus trukdymo modelyje sekamas įprastas radijo signalas; 2) atsitiktinio trukdymo modelyje keičiami trukdymo režimas; 3) reaktyvaus trukdytojo (trukdymo atakos vykdytojo) modelyje radijo signalas perduodamas, kai tik ryšio kanale girdimas aktyvumas..
- Žmogus ryšio viduryje inicijuota ataka (MITM). Antžeminė stotis komunikuoja su pagrindiniu bepiločiu orlaiviu, pirminį ryšį perima MITM ir jį nutraukia arba pakeičia duomenis. Lyginant su pasiklausymo ataka pagrindinis skirtumas tas, kad užpuolikas klastoja gautus duomenis.
- Pakartojimas (*Replay*). Panašiai kaip ir K1 vektoriaus ataka. Užpuolikas šnipinėja užšifruotus pranešimus tarp antžeminės stoties ir bepiločio orlaivio. Tada užpuolikas pakartotinai persiunčia šiuos pranešimus pagrindiniam BO, apsimesdamas teisėtu siuntėju.

K3 ir K4 ryšiai tarp pagrindinio bepiločio orlaivio ir kitų bepiločių orlaivių. Būtina paminėti, kad K3 ir K4 yra šiek tiek skirtingi, nors ir turi tam tikrų panašumų. K3 yra ryšys tarp magistralinio bepiločio orlaivio ir kitų bepiločių orlaivių, o K4 yra ryšys tarp ne magistralinių bepiločių orlaivių, kurie persiunčia ir dalijasi iš magistralinio bepiločio orlaivio gauta informacija. Bendraujant tarp bepiločių orlaivių gali kilti dalijimosi duomenimis ir privatumo problemų. Bepiločių orlaivių tarpusavio ryšys arba P2P ryšys yra rūšis, kai ryšio standartai nėra apibrėžti. Galimos atakos:

- Ryšio pasiklausymas (*Eavesdropping*). Užpuolikai klausosi neužšifruotų pranešimų tarp pagrindinio BO ir kitų BO panašiai kaip K1 ir K2 vektorių atakose.

- Trukdymas. Panašiai kaip ir K2 atakoje.
- Žmogus ryšio viduryje inicijuota ataka (MITM). Lyginant su pasiklausymo ataka pagrindinis skirtumas tas, kad užpuolikas klastoja gautus duomenis arba juos pakeičia kita komunikacijos sistema, pavyzdžiui, BO užpuoliku. Tuomet BO užpuolikas gali keisti, išmesti arba siųsti netikrus pranešimus.
- Pakartojimas (*Replay*). Kenkėjiškas bepilotis orlaivis skraido aplink bepiločių orlaivių spiečių ir klausosi užšifruotų pranešimų. Apsimesdamas teisėtu siuntėju, kenkėjiškas bepilotis orlaivis pakartotinai siunčia šiuos užšifruotus pranešimus kitam bepiločiam orlaiviui.
- *Sybil* ataka. Vykdant taką naudojamos suklastotos tapatybės, kurios atakuojamam mazgui perduodamo dideliais kiekiais. Jei įdiegiamas pakankamas kiekis *Sybil* mazgų, gali būti vykdomos tolesnės atakos (Visi BO mazgas):
    - *Backdoor*. Naudojant *Maldrone* programinę įrangą *Maldrone* ataka gali būti įdiegta nepastebimai ir naudoja TCP ryšį su kompiuterio valdikliu, kad galėtų sąveikauti su bepiločių orlaivių ryšiu ir perdavinėti jų duomenis. *Maldrone* gali užblokuoti BO lyderį, tada nuotoliniu būdu perimti valdymą, t. y. spiečius yra užgrobtas ir laukia užpuoliko nurodymų.
    - Paslaugų atmetimo (*DoS*) ataka. Jomis bandoma padaryti FANET paslaugas neprieinamas. Siunčiamas didelis kiekis autentifikavimo pranešimų per sąlyginai trumpą laiko tarpą. Užpuolikai gali priversti bepilotį orlaivį veikti neįprastai arba manipuliuoti valdiklio komandomis, kad nutrauktų bepiločio orlaivio skrydžio trajektoriją.
    - Potvynio ataka (*Flooding attack*). Užpuolikas siunčia daug paketų, kad išnaudotų BO išteklius ir sumažintų tinklo pralaidumą. Dėl šio proceso BO tampa sunkiai valdomas, nes jo apdorojimo pajėgumai gerokai sumažėja [76].
    - Savanaudiškumas(*Selfishness*). Kaip aptarta anksčiau, bepiločių orlaivių skaičiavimo galia yra ribota. Situacija, kai dėl techninių galimybių BO nesugeba apdoroti reikalaujamą duomenų kiekį, vadinama savanaudiškumu t. y. bepilotis orlaivis toliau veikia, tačiau gali pabloginti bendrą FANET našumą ir prieinamumą.

Atakos prieš ryšį su serveriu:

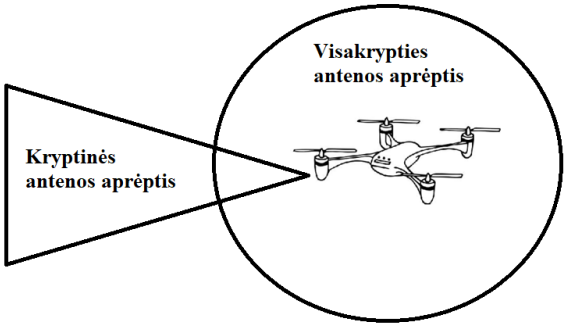
- Duomenų klastojimas (*Data tampering*). Klastojant jutiklių duomenis galima paveikti bendrą spiečiaus vientisumą, pavyzdžiui, pakeistus atstumo jutiklio duomenis galima sukelti spiečiaus susidūrimo reiškinį ir panašiai.
- Ryšio pasiklausymas (*Eavesdropping*). Ryšių pasiklausymas tarp serverio duomenų bazės ir bepiločių orlaivių arba antžeminės stoties.

5. Galimos kibernetinės atakos būdai

Skyriuje pateikiamas galimos atakos prieš BO spiečių variantai.

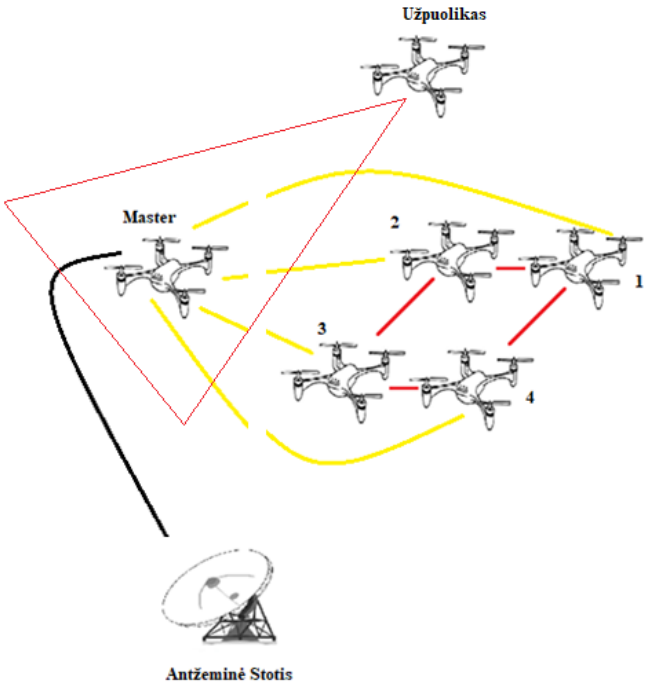
5.1. Trikdymas (*Jamming*)

Trikdymas – tai tyčinis perdavimo signalo blokavimo naudojimas siekiant sutrikdyti dronų ir piloto ryšį. Kai asmuo užblokuoja (*Jams*) droną, jis gali priversti droną atlikti šiuos veiksmus: nusileisti vietoje ir sustabdyti bet kokį tolesnį judėjimą; grįžti į „namų“ vietą.



29 pav. Trukdymas skirtingomis antenomis

Kryptinė antena – tai antena, kuri tam tikromis kryptimis spinduliuoja arba priima didesnę radijo bangų galią. Kryptinės antenos gali spinduliuoti radijo bangas spinduliais, kai norima didesnės spinduliuotės koncentracijos tam tikra kryptimi, Taip galima padidinti į imtuvus perduodamą galią. Tai skiriasi nuo visakrypčių antenų, kurios spinduliuoja arba priima radijo bangas plačiu kampu iš plataus kampo.

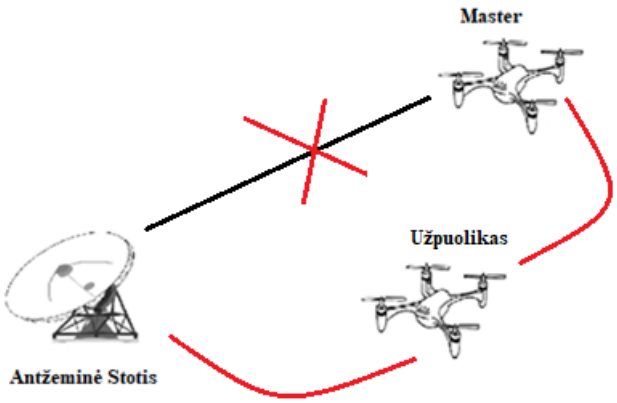


30 pav. Ryšių trikdymas.

Optimalus variantas naudoti keptines antenas, dėl jų didesnės galios. Numatoma, kad reikalingas papildomas BO, kuris atliktų užpuoliko funkciją. Nustatyti galimi trikdymo variantai: tarp antžeminės stoties ir BO lyderio; tarp lyderio ir kitų spiečiaus BO.

5.2. Žmogus viduryje (*MITM)*

Atliekant ataką užpuolikas ne tik išklauso ryšio metu perduodamus paketus, bet ir suklastojąs juos perduoda BO spiečiaus lyderiui per antžeminę stotį.

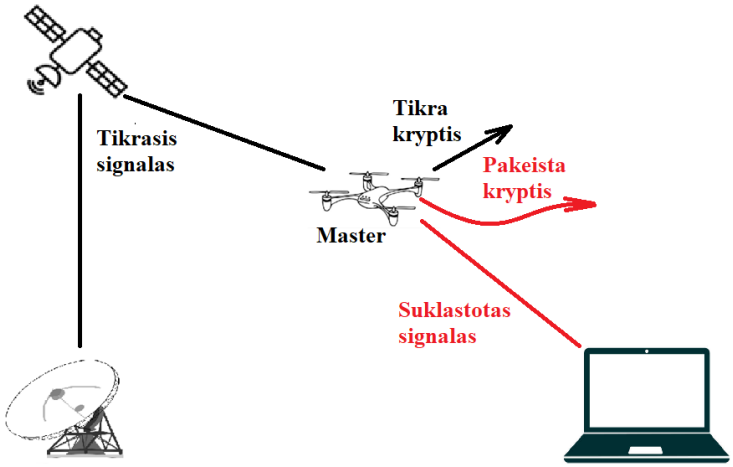


31 pav. *MITM* ataka

32 pav. pavaizduota situacija, kai GCS bendravo su pagrindiniu bepiločiu orlaiviu, pirminį ryšį perima kenkėjiškas bepilotis orlaivis ir jį nutraukia. Tuomet piktavalis bepilotis orlaivis gali atmesti, keisti arba siųsti pranešimus į GCS. Numatoma, kad reikalingas papildomas BO, kuris atliktų užpuoliko funkciją.

5.3. GPS signalo klastojimas

GPS signalo klastojimui nereikia papildomo BO. Atakos esmė – pateikti BO spiečiaus lyderiui suklastotas koordinates, taip pakeičiant spiečiaus misijos tikslumą. Tam reikia galingo stiprintuvo su antena, kad užpuoliko signalas būtų stipresnis už nesuklastotą signalą.

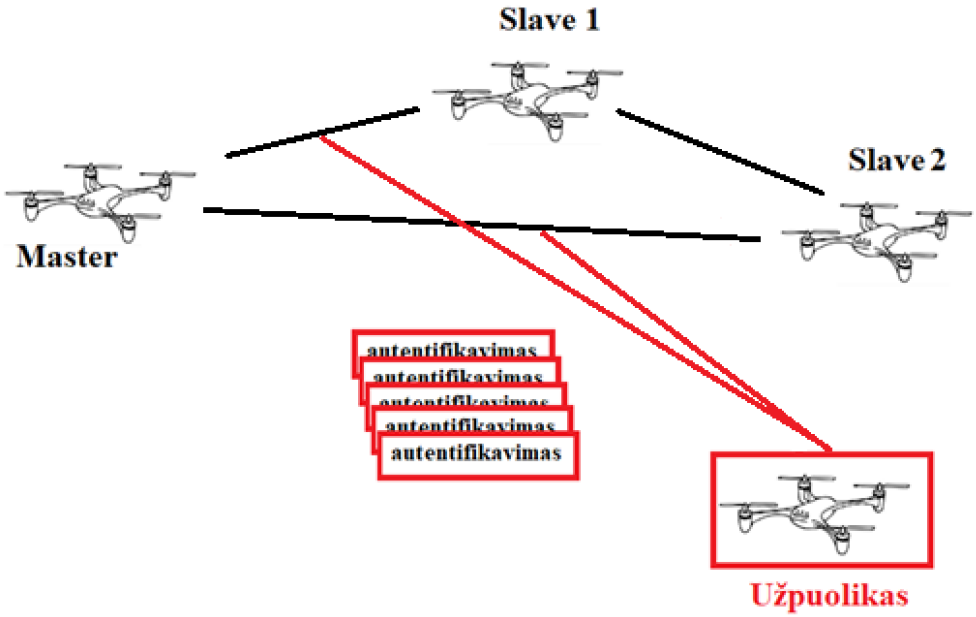


32 pav. GPS koordinačių klastojimas

33 pav. parodyta, kaip veikia GPS suklastojimas. Užpuolikas, naudodamas GPS imitatorių su galios stiprintuvu ir antena, siunčia melagingus duomenis padirbtu signalu. Dėl GPS klastojimo gali kilti saugos problemų, pavyzdžiui, bepiločio orlaivio užgrobimas, veikimo sutrikimai ar avarijos, nes suklastojamos realios BO spiečiaus koordinatės.

5.4. *DoS* ataka

DoS atakai reikalinga įranga, papildomas BO, kuris siunčia milžinišką srautą autentifikavo pranešimų. Papildomas BO privalo turėti galingą duomenų perdavimo sistemą.

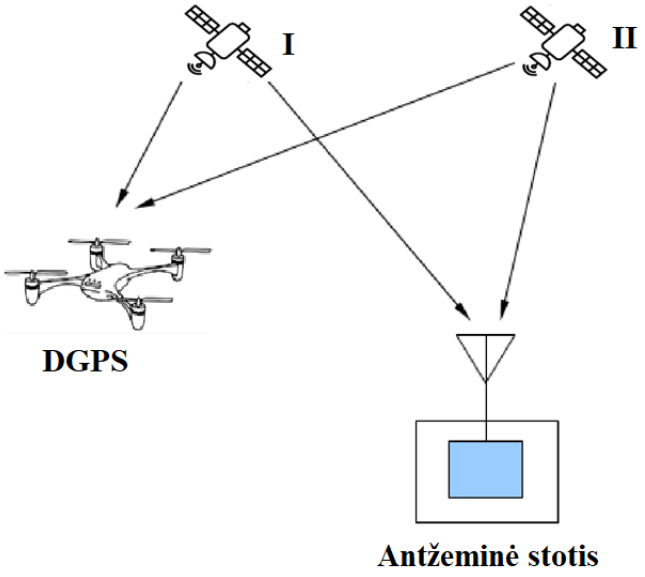


33 pav. *DoS* ataka

34 pav. pavaizduota *DoS* ataka prieš BO spiečiaus lyderi. Užpuolikas apsimeta, kad nori prisijungti prie FANET, siųsdamas didelį kiekį netikrų autentifikavimo pranešimų. Šie pranešimai naudoja daug išteklių, todėl bepilotis orlaivis negali priimti naujų misijų iš pagrindinio bepiločio orlaivio arba bepiločio orlaivio Nr. 2.

6. Kibernetinės atakos algoritmas

Atakos simuliacija tiesiogiai orientuota į BO spiečiaus lyderi. Daroma prielaida, kad kibernetinė ataka prieš BO spiečiaus lyderi perims viso spiečiaus kontrolę arba sujauks spiečiaus valdymo algoritmus. Jei BO spiečiaus lyderis supras, kad jis atakuojamas, tikėtina kad jis persijungs į inercinę navigacinę sistemą. Inercinė navigacijos sistema (INS) – tai savarankiškas navigacijos metodas, kai akselerometrų ir giroskopų teikiami matavimai naudojami objekto padėčiai ir orientacijai stebėti, kai žinoma pradinio taško orientacija ir greitis.

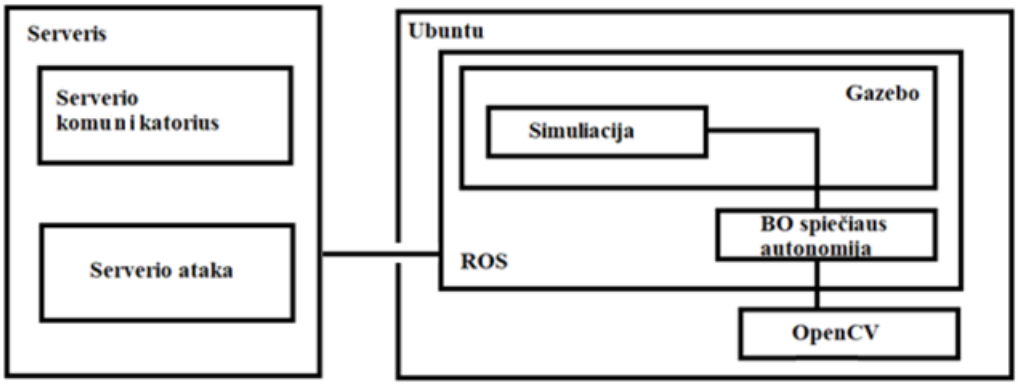


34 pav. Diferencialinis GPS

BO spiečiaus lyderiui persijungus į inercinę navigacinę sistemą spiečius nutrauks misiją ir grįš į namų padėtį (atsijungs nuo serverio). Toks savarankiškas navigacijos modelis tęsiamas nuo paskutinės žinomo GPS koordinatės. Žinant koordinates, galima, naudojant 30 pav. pateiktą atakos modelį, trikdyti spiečiaus judėjimą, kad spiečius pilnai nutrauktų skrydį.

Atakos simuliacijas prieš BO spiečiaus lyderi bus atliekama naudojant programinę įrangą:

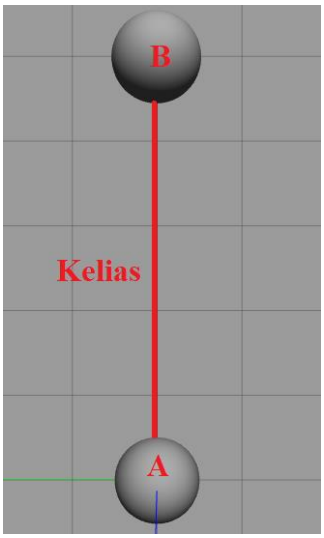
- *Ubuntu* – operacinė sistema pagrįsta *Debian Linux* pagrindu.
- *ROS* – atviro kodo robotų operacinė sistema. Įrangos rinkinys naudotas menamo lyderio judėjimo trajektorijos algoritmams apibrėžti. Simuliacijoje sistema imituoja PID funkciją.
- *Gazebo* – robotų modeliavimo įrankis, skirtas robotinių įrenginių simuliacijoms atlikti 2D ar 3D aplinkoje. *Gazebo* naudodamas *ROS* imituoja simuliuojamo mazgo dinamika. Taip pat sistema palaiko imituojamus jutiklius ir analizuoja jų duomenis.
- *OpenCV* – programavimo įrankių biblioteka, naudojanti vaizdo skaitymo ir analizavimo algoritmus. Naudojant biblioteką, paprasta identifikuoti menamo BO judėjimo trajektoriją
- Serveris – kompiuterinė programa, leidžianti klientui naudotis kompiuterinėmis galimybėmis per ryšio sistemą.



35 pav. Simuliacinės atakos prieš menamą BO spiečiaus lyderį architektūra.

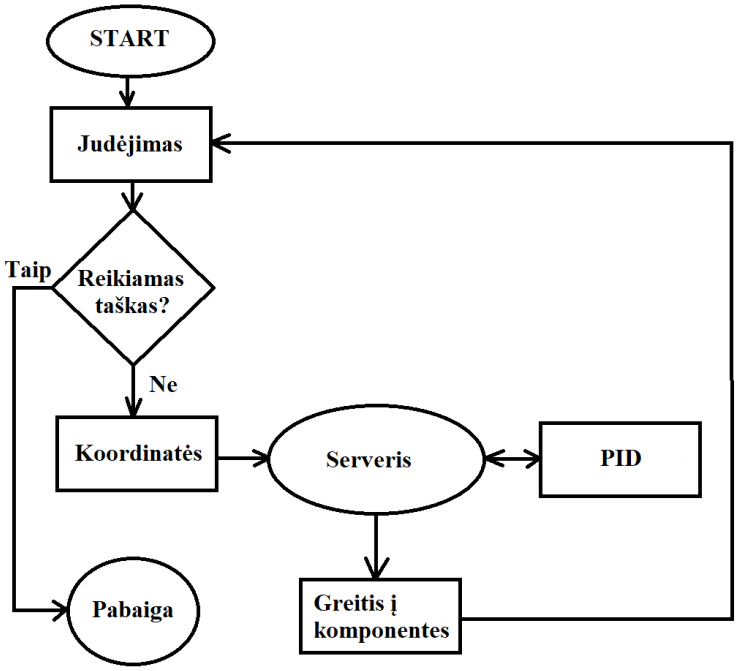
35 pav. pavaizduoti simuliacinės atakos prieš menamą BO spiečiaus lyderį architektūra. Ryšių pagrindą sudaro operacinė sistema, serveris ir *Matlab*, kaip vaizdavimo įrankis. Iš esmės tokią sistemą galima susieti su realaus BO ar BO spiečiaus valdymu.

Atakos simuliacija paremta menamo lyderio judėjimu. Simuliacijoje BO lyderis pateiktas kaip taškas (A), kuris simuliacijos metu turi pasiekti kitą tašką – tikslą (B).



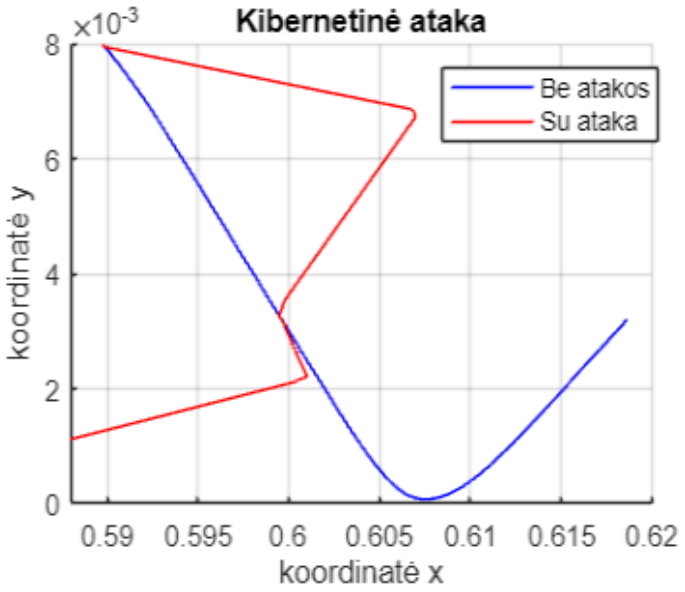
36 pav. Menamo lyderio judėjimas *Gazebo*

Menamo BO lyderio įveikiamo kelio kontrolės algoritmas pateiktas 37 pav. Jo kontrolė paremta serveriu, kuris tiesiogiai bendrauja su proporciniu integraliniu deviacijos kontroleriu (PID). Kontroleris naudodamas serverio išteklius skaičiuoja reikalingo greičio komponentes (X ar Y).



37 pav. Menamo lyderio kontrolės algoritmas

Simuliacijoje pateiktas imituoto lyderio judėjimas 2D erdvėje, kai jį neveikia papildomos atakos. Judėjimas paremtas 37 pav. pateiktu algoritmu. Siekiama, kad taškas judėti kiek įmanoma mažiau nukrypdamas nuo tiesiaeigio judėjimo. Toks judėjimas pasirinktas, kad vizualiai būtų galima pavaizduoti skirtumą po to, kai bus atlikta kibernetinė ataka.



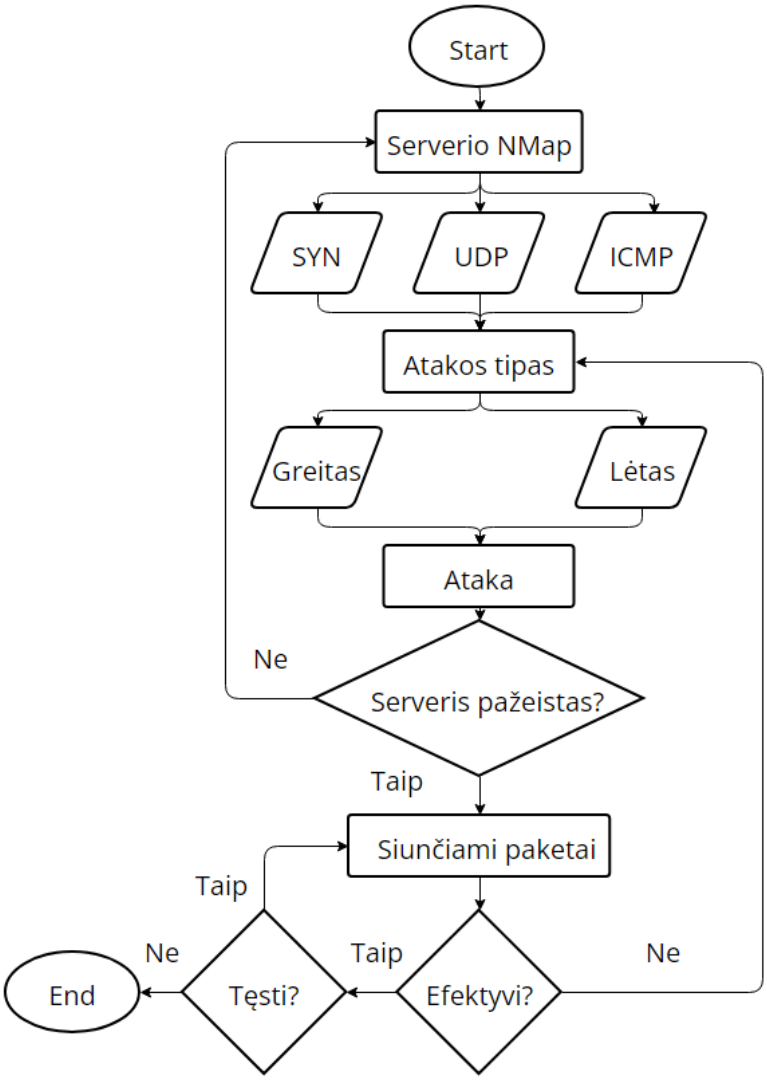
38 pav. Imituoto lyderio judėjimo trajektorija, kai serverį veikia *DoS* ataka

38 pav. pateikta imituoto lyderio judėjimo trajektorija, kai serverį veikia *DoS* ataka.. Pradinis judėjimo taškas [0.59;0,008]. Atlikus *DoS* prieš imituotą lyderi pastebėta, kad jo judėjimo trajektorija kardinaliai pasikeitė. Greitis į komponentę X vis pastrigdavo, t.y. dėl didelio autentifikavimo paketų skaičiaus serveris nepajėgė atlikti visų užduočių, nors simuliacija nesustojo. Kaip matyti iš 37 pav. kontrolės algoritmo, PID kontroleris informacija apie BO spiečiaus lyderio greitį perduoda per

serverį, jam stringant – stringa ir visa sistema, ko pasėkoje greitis į komponentes nesikeičia. Esant tokiai simuliacijos architektūrai ir tokiam valdymo algoritmui greitis į komponentes gali būti ir neigiamas. Iš simuliacijos rezultatų duomenų galima daryti išvadą, kad greitis pastrigo 4 kartus, o paskutinį kart greitis buvo neigiamas X komponentės atžvilgiu, todėl imituotas BO lyderis nepasiekė reikiamo tikslo.

6.1. *DoS* atakos modelis

DoS atakos algoritmas pateiktas 37 pav. Atakos algoritmas pradedamas nuo serverio, kuris bus atakuojamas, skenavimo (*NMAP*).

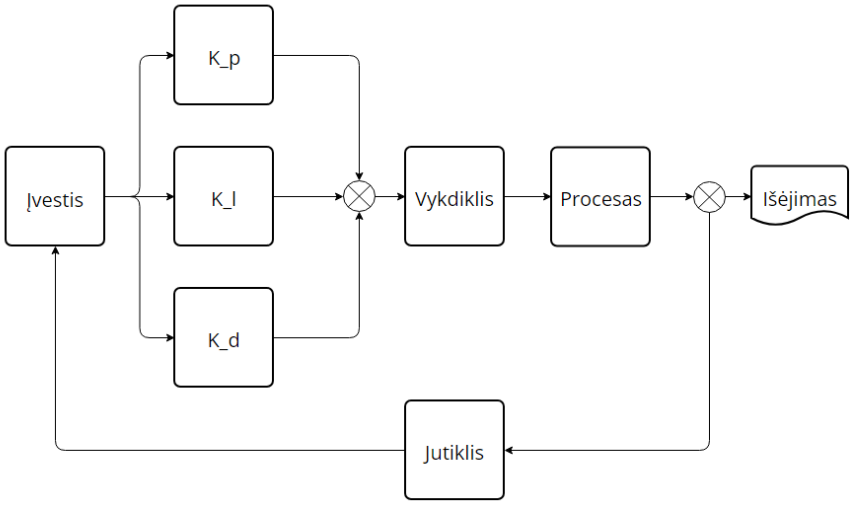


39 pav. *DoS* atakos algoritmas

NMap – laisvai prieinamas *Linux* posistemių interneto tinklo skenavimo įrankis. Prisijungus prie tinklo ir galima aptikti atvirus tinklo prievadus. Nuskenavus serverį pasirenkamas atakos metodas – siūlomi 3 galimi variantai: *SYN; UDP; ICMP*. *SYN* autentifikavimas – ataka, kurios metu siekiama, kad serveris taptų neprieinamas teisėtiems vartotojams. *UDP* autentifikavimas – suklastojamas IP adresas, siunčiant didelį kiekį paketų į norimą serverį. *ICMP* autentifikavimas – autentifikavimo pranešimų srautu siekiama sukelti dirbtinį tinklo uždelsimą.

Pasirinkus atakos metodą pasirenkamas atakos tipo greitis: lėtas arba greitas. Simuliacijai naudotas lėtas atakos greitis į konkretų prievadą. Realiai naudojamas greitas atakos tipas. Priklausomai nuo greičio skiriasi perduodamų paketų skaičius per laiko vienetą. Pasirinkus visus parametrus pradedama ataka ir tikrinamas atakos efektyvumas. Jei įsiųstų paketų skaičius per laiko vienetą atitinka norimą skaičių ataka tęsiama, jei ne – algoritmas pradedamas iš naujo pasirenkant kitą atakos metodą. Jei pastebima, kad paketai visai nesiunčiami – tai serveris skenuojamas iš naujo. Ataka tęsiama iki pageidaujamo išsiųstų paketų skaičiaus arba iki kol serveris užlūžta.

Atakuojamas serveris visoje simuliacijos sistemoje yra duomenų perdavimo srautą užtikrinantis mazgas, kuris tiesiogiai bendrauja su PID (40 pav.). Jis tiesiogiai sąveikauja su PID (žr. 40 pav.) (proporcinis-integralinis-derivacinis) valdikliu, vykdikliu ir IMU (inerciniu matavimų bloku), kad kontroliuotų procesą. PID valdiklis priima įvesties duomenis apie paklaidą, t.y., skirtumą tarp dabartinės ir norimos padėties, ir reguliuoja sistemą taip, kad ši paklaida būtų artima nuliui. Ši korekcija grindžiama trimis skirtingomis konstantomis: P (proporcinis), I (integralinis) ir D (išvestinis) stiprinimais. Šios trys skirtingos PID stiprinimo vertės nusako, kaip jautriai sistema reaguoja.



40 pav. PID valdiklio blokinė schema [28]

Proporcinė dalis (P) apskaičiuoja paklaidą tarp pageidaujamo išėjimo ir faktinės išmatuotos vertės. K_p – proporcinis parametras, kuris lemia reakciją į paklaidas. Integruojančioji dalis (I) sumuoja ankstesnę paklaidą, kad pridėtų prie išėjimo ir toliau stabilizuotųsi apie pageidaujamą nustatytąją vertę. Pagrindinė integravimo dalies paskirtis - pašalinti nusistovėjusios būsenos paklaidą K_I [27].

$$u(t)=K_p e(t)+K_I \int_0^t e(t')dt'+K_d \frac{de(t)}{dt} . \quad (5.5.1)$$

Išvestinė dalis (D) lygina ankstesnę paklaidą su dabartine, nustatydama pokyčio greitį ir slopindama sistemos svyravimus, taip mažinant nereikalingą slopinimą. Pagrindinė išvestinio parametro K_d funkcija yra gerinti judėjimo stabilumą ir greitį. [27].

7. Lyderio indentifikavimo BO spiečiuje algoritmas

Skyriuje atliekama analizė kaip rasti lyderį BO spiečiuje. Spiečiaus agentai ir lyderis komunikuoja naudojant WMN. Pirmiausia tiriama galimybė prisijungti prie BO spiečiaus tinklo, tam kad būtų toliau tiriama spiečiaus architektūra. Skyriuje naudojama SOTA (angl. „state-of-the-art“) metodologija

7.1. Galimybė prisijungti prie BO spiečiaus tinklo

Nepaisant technologijų pažangos WMN tinkluose, jie vis dar susiduria su saugumo iššūkiais [40,41]. Siekiama nustatyti pažangiausiu šiuo metu naudojamų tinklų trūkumus, kurie kelia saugomo iššūkius, kai analizės objektas palyginti nauja mokslinių tyrimų sritis – BO spiečius. Pagrindinė tokio tinklo saugumo problema – tinklo komunikacija vyksta mobilioje (dinaminėje) aplinkoje.

Pagrindiniai pajėgumų apribojimai apsunkina WMN tinklų taikymą BO spiečiams. Paprastai spiečius komunikacija naudoja pusiau dvipusį domenų perdavimą – tarp dviejų įrenginių vienu metu tik vienas įrenginys gali perduoti ir priimti duomenis tinkle arba magistralėje. Duomenys gali būti siunčiami abejomis kryptimis, bet ne vienu metu (tokia komunikacija paprastai naudojama komerciniuose bepiločiuose orlaiviuose). Todėl galima teigti, kad kiekvienas tarpinio mazgo atliktas persiuntimo veiksmas sumažina didžiausią galinį belaidžio ryšio pralaidumą bent 1/N, jei N yra persiuntimo veiksmas [41]. Be to, maršrutizavimo mazgai, atliekantys tolimesnių tinklo mazgų retransliatorių funkcijas, yra priversti dalytis savo dažnių juostos pločiu su atšakomis. Dėl tokių kliūčių tinklui sunku reaguoti į besikeičiančią topologiją arba reaguoti į grėsmes. Centralizuotas spiečiaus valdymas leidžia priimti optimalius sprendimus, užtikrinančius bendrą stebėjimą, tačiau perduodant valdymo signalus per daugelį jungčių atsiranda nemažai papildomų sąnaudų. Valdymo paskirstymas išsprendžia šią problemą ir pagerina reagavimo greitį, tačiau dėl to sumažėja tinklo saugumas.

M. S. Siddiqui ir C. S. Hongas moksliniame straipsnyje „Saugumo klausimai belaidžiuose tinkluose“ pateikia aukšto lygio WMN saugumo problemų apžvalgą: nurodo, kaip tinklinių tinklų apribojimai, tokie kaip procesoriaus našumas, baterijos veikimo laikas, mobilumas ir ribotas dažnių juostos plotis, kelia unikalių saugumo iššūkių. Tačiau, nors belaidžiams tinkliniams tinklams pasiūlyta daug maršrutizavimo protokolų, daugumoje metodų neskiriama dėmesio saugumui[42].

BATMAN (angl. „Better Approach To Mobile Ad-hoc Networking“) [43] ir OSLR (angl. „Optimized Link State Routing“) [44] yra du plačiai naudojami maršrutizavimo protokolai, kuriuose daroma prielaida, kad saugumas bus įgyvendintas aukštesnio lygio tinklo mechanizmo sluoksniuose [6], o asimetrinio rakto šifravimo metodai pasirašo kiekvieną pranešimą, tačiau naudoja išteklius, kurie gali būti kritiniai BO spiečiaus tinkluose [45]. Padėtį nusakantys maršruto parinkimo protokolai – ryšio protokolas pritaikytas BO tinklams. Tokie protokolai naudoja kodavimo rakto atpažinimo metodą tiek išsiunčiamų tiek gaunamų duomenų paketų autentifikavimui. Deja, protokoluose, kuriuose naudojama viešojo rakto infrastruktūra, reikalaujama, kad sertifikatus su viešuoju ir privačiuoju raktu teiktų sertifikavimo įstaiga. Panaudojant serverį kaip papildomą programinę įrangą šią prielaidą įmanoma įgyvendinti BO spiečiuje, pageidautina išvengti centralizuoto sprendimo, kad būtų galima palaikyti visiškai autonominį spiečių ir sumažinti ryšio su pagrindine infrastruktūra nuostolius [47].

Nors WMN tinklas idealiai tinka BO spiečiaus komunikacijai, bet atlikus SOTA analizę pastebėta, kad toks tinklas turi daug galimų atakos vektorių, kurie atsiranda dėl sunkiai įgyvendinamų tinklo saugumo sprendimų, nes BO spiečius turi ribotus išteklius ir juda dinaminėje aplinkoje.

7.2. Tinklo sluoksnių pažeidžiamumas

Daugelis WMN tinklinių protokolų naudojamų BO spiečiuje yra sukurti be saugumo arba manoma, kad saugumo klausimai sprendžiami aukštesniuose sluoksniuose. Išskirti 5 WMN tinklo sluoksniai, kuriems atitinkamai priskirtos grėsmės. Pastebėta, kad norit pažeisti BO spiečiaus kontrolę užtenką atlikti išorinę ataką, kad būtų sutrikdomas bendras spiečiaus vientisumas. Tiesa, priklausomai nuo įgyto prieigos lygio užpuolikas gali pažeisti ryšio mazgus ir vidine ataka. Saugumo grėsmės BO spiečiaus mazgams ir ryšiams pateiktos 22 pav.

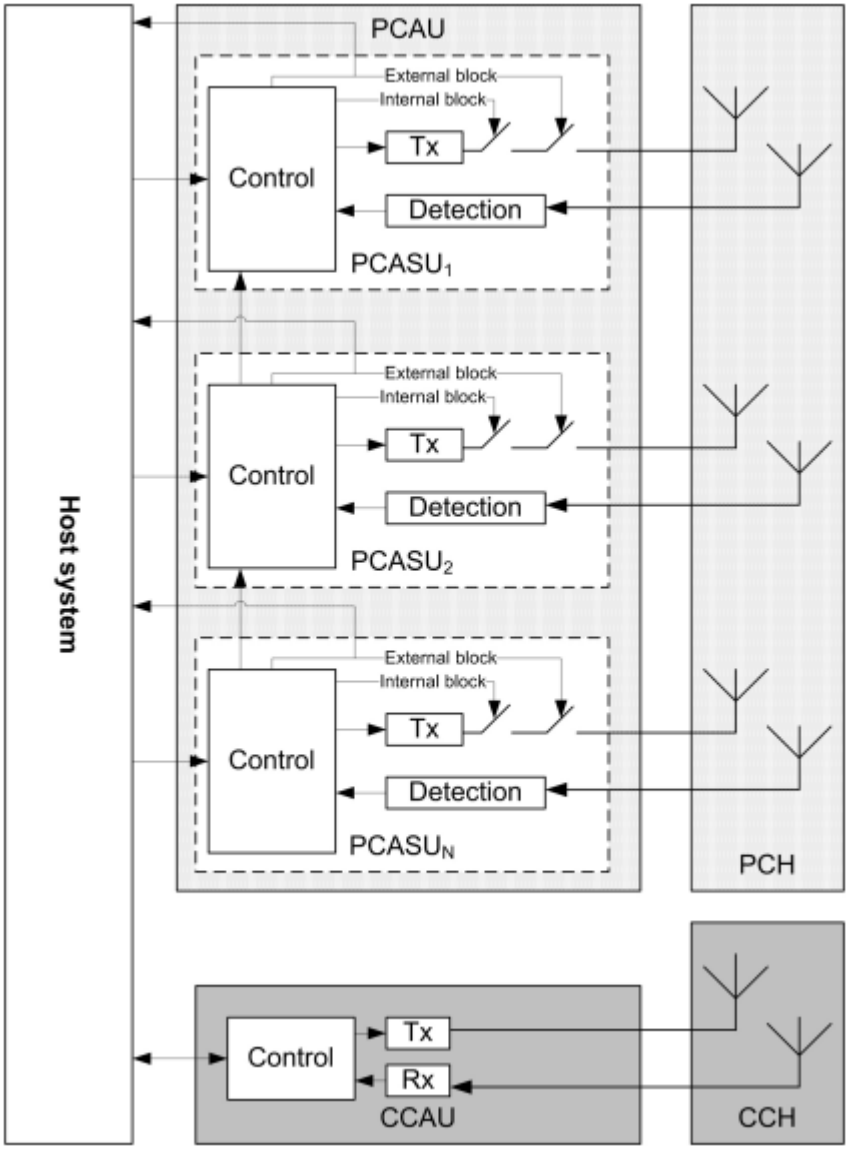
1 lentelė. BO spiečiaus pažeidžiami WMN tinklo sluoksniai

WMN tinklo sluoksnis	**Pažeidžiamumas**	**Išnaudojama**
Fizinis	*Eavesdropping* *Jamming*	Belaidžių kanalų transliavimo pobūdis Belaidžio ryšio argumentai
Nuoroda	*Spoofing* *Frame Modification*	Tyčinis susidūrimas MAC slopinimas
Tinklas	*Routing Forwarding* *Data Forwarding*	*Selfish atakos* *Collision atakos*
Transportas	*Packet Corruption* *Protocol Weakness*	*DoS atakos* *Hijacking*
Paraiškos	*ROS2 Bugs* *Open Protocols*	*Malware atakos* Modifikacijos

1 lentelėje pateikti BO spiečiaus pažeidžiami WMN tinklo sluoksniai. Išskirti 5 tinklo sluoksniai ir jų pažeidžiamumas bei panaudojimas.

7.3. Prisijungimo prie išskirstyto FANET tinklo metodas

Moksliniame straipsnyje – „Laiko algoritmas šeimininko parinkimui *Ad-hoc* belaidžiuose tinkluose“ pasiūlė metodą bazinės juostos radimui, kuris įgyvendina lyderio pasirinkimo *Ad-hoc* tinkle algoritmą ir išsamiai detalizavo reikiamą įrangą tokiam metodui įgyvendinti. Nepriklausomai nuo BO skaičiaus spiečiuje galima išrinkti jo lyderį naudojant palyginimo metodą. Algoritmas leidžia kiekvienam įrenginiui automatiškai nustatyti savo statusą: pagrindinis arba pavaldusis, remiantis identifikatoriumi, nepridedant papildomų pridėtinių nuostolių ir nesikeičiant paketais, kurie lėtina tinklo darbą[48].

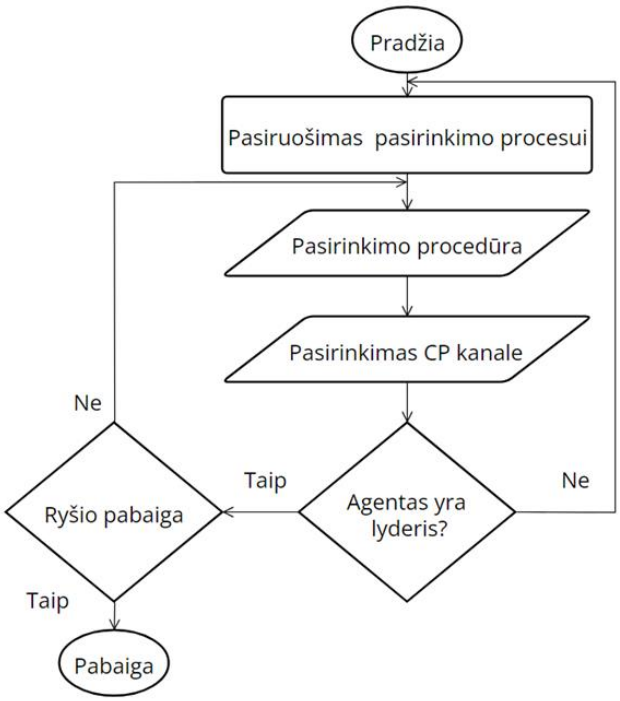


41 pav. Ryšio įrenginys: viršutinio lygmens architektūra [48]

41 pav. pavaizduotas ryšio įrenginys metodo įgyvendinimui. Tokio įrenginio viršutinio tinklo sluoksnių architektūra susideda iš 3 pagrindinių komponentų: priimantysis blokas (*Host Unit*); apsaugos kanalo prieigos blokas (*PCAU*); ryšio kanalo prieigos blokas (CCAU). Ryšio įrenginyje naudojami du specifiniai radijo dažnių kanalai - apsaugos kanalas (PCH) ir ryšio kanalas (CCH), kurių taikymo apimtys skiriasi. 3 blokai: *Host Unit*, *PCAU*, *CCAU* yra atsakingi už lyderio pasirinkimo procesą. Apdorojus *PCH* ir *CCH* kanalų informaciją, *PCAU* kanalas pradeda pasirinkimo procesą *PCH* kanale. *CCAU* blokas atsakinga už apsaugos kanalą – priimamas naujas ryšys į bendrą komunikaciją [48].

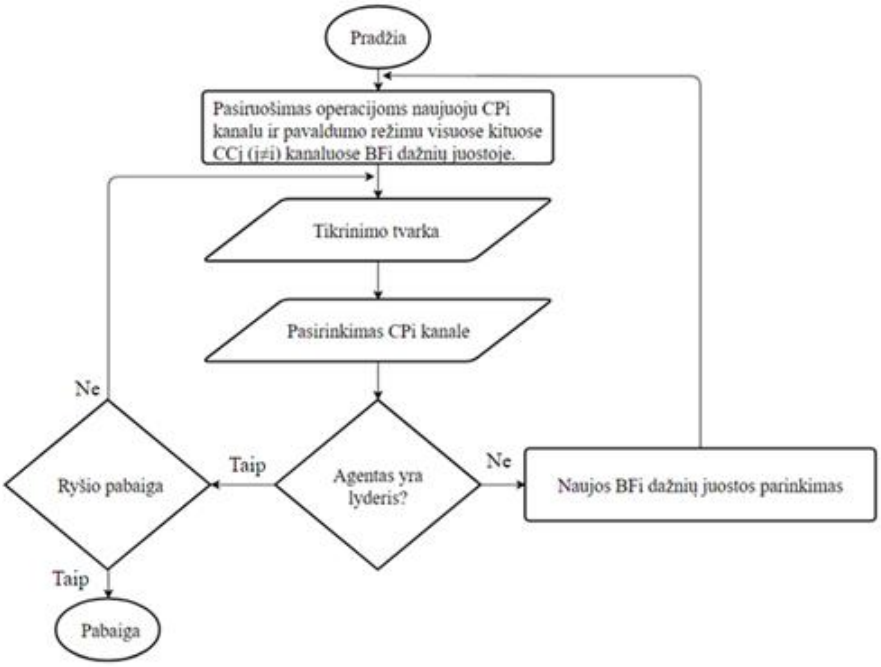
7.4. Lyderio pasirinkimo algoritmas FANET tinkle

Algoritmas sudaromas remiantis tuo, kad komunikacija tarp BO spiečiaus narių naudoja 2 kanalus: apsaugos ir komunikacijos. Algoritmas adaptyvus renkantis vieną ar kelias dažnių juostas. Valdymo procedūra pagrįsta palyginimo metodu, kuris naudoja lygiagretaus perdavimo režimą apsaugos kanale ir leidžia išskirti vieną ryšio įrenginį, kuris turės pagrindinio komunikacijos prietaiso statusą ryšio zonoje.



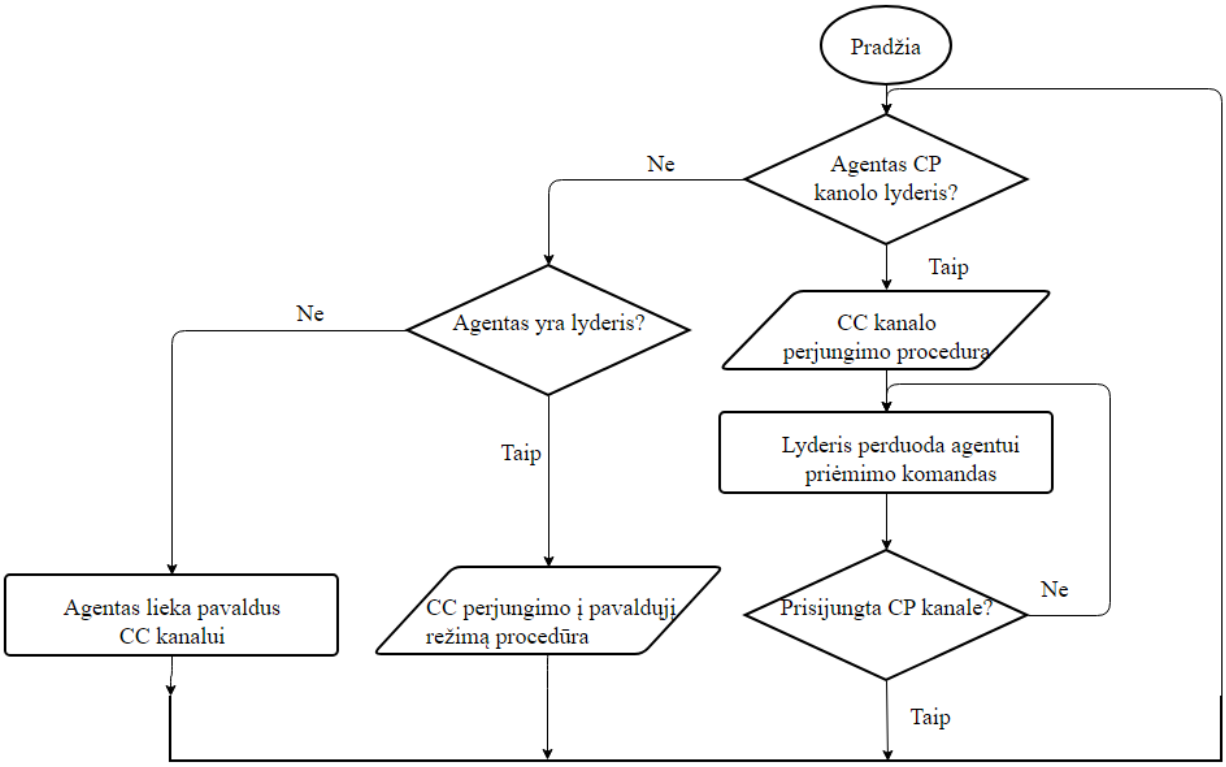
42 pav. Lyderio nustatymo algoritmas vienos dažnių juostos režimu

42 pav. pateiktas lyderio nustatymo algoritmas vienos dažnių juostos režimu. Algoritmas prasideda nuo bendrojo kodinio elemento parinkimo ir pasirinkimo sąlygos patikrinimo. Jei sąlyga patikrinta, kiekvienas komunikacijos įrenginys dalyvauja lyderio parinkimo procese. Komunikacijos įrenginiai tikrinami poromis. Jei vienas iš dviejų įrenginių nustatomas kaip lyderis procesas tęsiamas iki ryšio pabaigos, t.y. kol patikrinamos visos galimos ryšio poros. Veikiant keliems ryšio kanalų diapazonams kiekvienas komunikacijos įrenginys gali naudoti bet kurią dažnių juostą, todėl lyderio nustatymo procesas pradedamas apsaugos kanale (CP), kad įgijus pagrindinio ryšio įrenginio statusą būtų perimtas ir komunikacijos kanalas (CC).



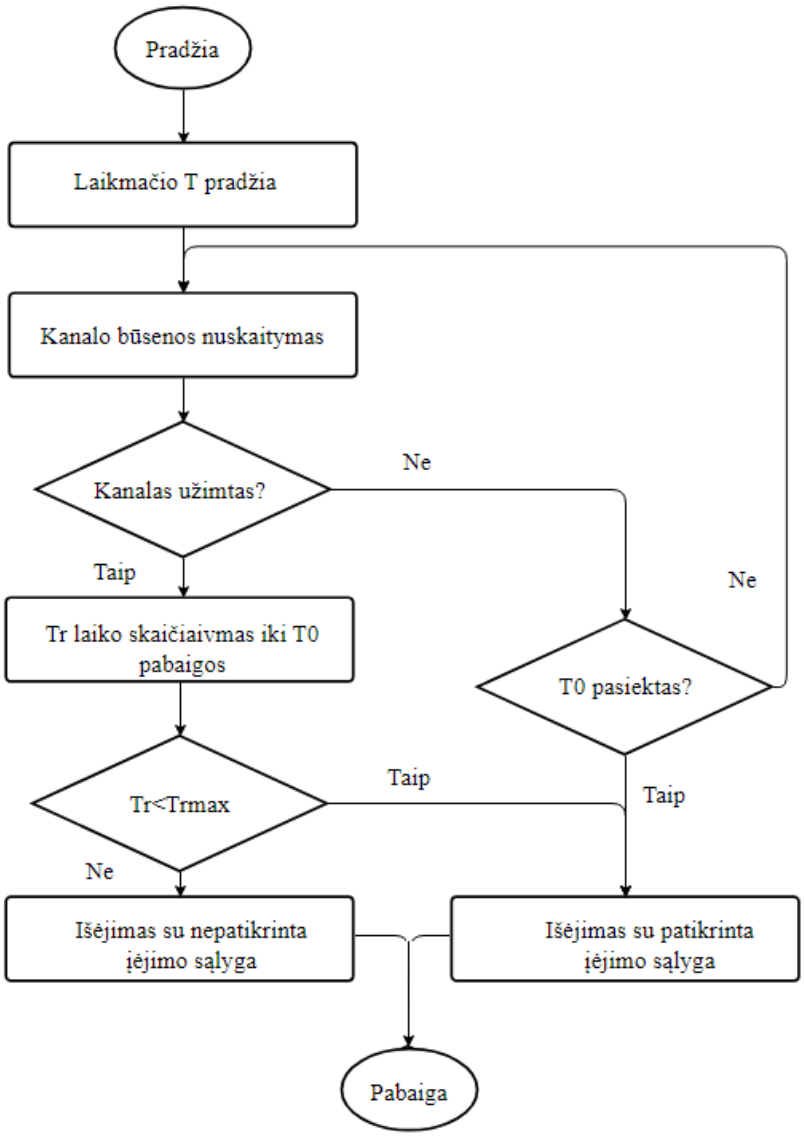
43 pav. Lyderio nustatymo algoritmas režimu, kai naudojamos kelios dažnių juostos

43 pav. pateiktas lyderio nustatymo algoritmas daugiajuosčiu dažnių režimu. Algoritmas iliustruoja procesą, kuris atliekamas norit nustatyti kiekvieno ryšio įrenginio intarpo statusą konfigūracijoje, kuri atitinka kelių dažnių juostų režimą. Metodas panašus kaip ir 42 pav. pateiktas algoritmas, tačiau skiriasi veiksmai tikrinant ryšio įrenginių porą bet kurioje dažnių juostoje (BFi). Jei ryšio įrenginys identifikuojamas kaip komunikacijos kanalo lyderis BFi dažnių juostoje, kuri tiesiogiai susijusi su apsaugos kanalu toje pačioje dažnių juostoje, pradedant naują poros tikrinimo procesą turi būti patikrintos visos galimo BFi dažnių juostos.



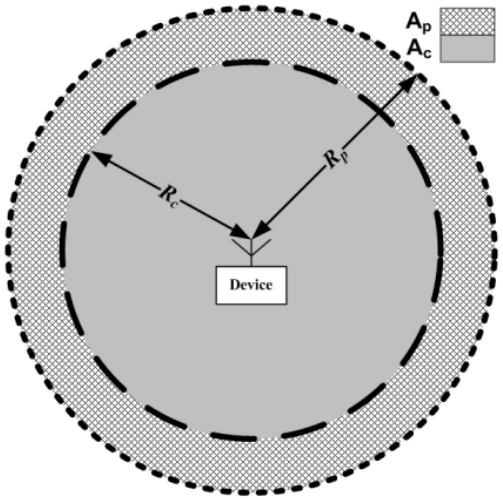
44 pav. Kanalų prieigos procedūros schema

44 pav. pateikta kanalų prieigos procedūros schema. Pirmiausia kiekvienam ryšio įrenginiui parenkamas pavaldusis arba pagrindinis statusas. Jei ryšio įrenginys turi pagrindinį statusą, tai jo ryšio kanalas yra pagrindinis ryšio kanalas. Ryšio lyderis išlaiko kanalo pagrindinį statusą, jei ryšys nėra nutraukiamas ir jei ryšio įrenginys yra vienos dažnių juostos komunikacijos kanalo pagrindinis komunikacijos įrenginys. Jei lyderis praranda savo statusą jis turi inicijuoti komunikacijos kanalo perjungimo į pavalduįį režimą procedūrą, t.y. ryšys su kitais komunikacijos agentais nutraukiamas ir komunikacijos kanalas nutraukiamas. Taip perinama į naują pasirinkimo režimą, kad būtų galima aptikti bet kokius ryšio nurodymus, kurie gali ateiti iš naujo pagrindinio ryšio įrenginio komunikacijos kanale. Jei tas pats ryšio įrenginys buvo ne lyderis, o pavaldusis, tai jis ir lieka pavaldžiuoju ir pereina į priėmimo režimą laisvame kanale.



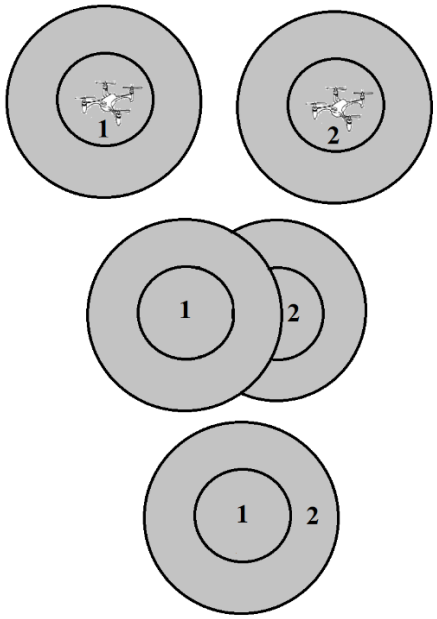
45 pav. Lyderio pasirinkimo algoritmas, skirtas patikrinti laisvo kanalo įėjimo sąlygas

Prieš pradedant lyderio pasirinkimą, bet kuris ryšio įrenginys turi inicijuoti šio pasirinkimo pradžios patikrinimo procedūrą (45 pav.). Per laiko vienetą (*T0*) atliekama pasiklausymo fazė apsaugos kanale naudojant informacijos nešlio egzistavimo detektorius. Įėjimo į apsaugos kanalą sąlyga patikrinama, jei ne vienas iš šių detektorių neaptinka nešlio buvimo tame kanale per laiko vienetą. Tokiu atveju CP kanalas laikomas neužimtu. Šis laiko vienetas interpretuojamas kaip laikas, reikalingas užimti dvi iš eilės einančias kanalų fazes. Jei apsaugos kanalas užimtas per laiko vienetą (*T0*), galima apskaičiuoti didžiausia galimą uždelsimą (*Trmax*). Galimos dvi situacijos: uždelsimas mažesnis nei apskaičiuotas maksimalus uždelsimas – galimas prisijungimo procesas; uždelsimas didesnis nei apskaičiuotas maksimalus uždelsimas – negalimas prisijungimo procesas. Ryšio įrenginys turi persijungti į laukimo režimą, kol kanalas taps laisvu, jei naudojamas vieno dažnių ruožo režimas, arba pasirinkti naują dažnių ruožą prieš pradėdamas naują prisijungimo procesą, jei naudojamas kelių dažnių ruožų režimas.



46 pav. Ryšio topologija: komunikacijos ir apsaugos zonos [48]

Ryšio įrenginyje naudojami du specifiniai radijo dažnių kanalai – apsaugos kanalas ir ryšio kanalas, kurių taikymo sritys skiriasi. Komunikacijos kanalas turi didesnę ryšio aprėptį, nei prisijungimo kanalas. Norit pasiekti komunikacijos kanalą pirmiausia prisijungiama prie apsaugos kanalo, taip apsaugant komunikacijos diapazoną nuo ryšio trikdymo. Tokia ryšio topologija pateikta 46pav. [48].

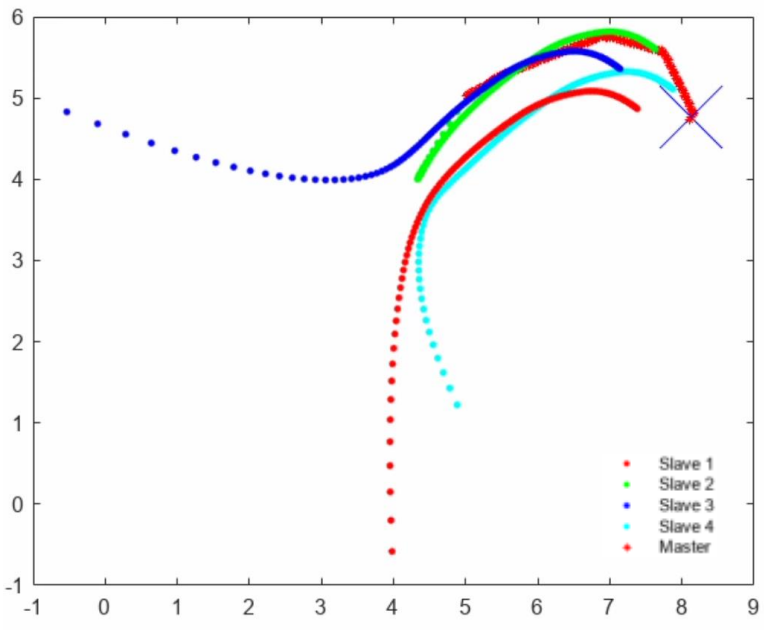


47 pav. Metodas, pagrįstas dviejų kanalų CP ir CC naudojimu problemai, susijusiai su dviejų kaimyninių celių 1 ir 2 persidengimu, spręsti

47 pav. metodo, pagrįsto dviejų kanalų CP ir CC naudojimu problemai, susijusiai su dviejų kaimyninių celių 1 ir 2 persidengimu, spręsti, iliustracija. Šiame pavyzdyje šios dvi ląstelės atitinkamai susijusios su dviem ryšio įrenginiais. Laiko vienetą, kuris lygus maksimaliam prisijungimo uždelsimui, kiekvienas iš šių dviejų įrenginių yra kito įrenginio veikimo zonoje. Pasibaigus prisijungimo procesui, vienas iš dviejų ryšio įrenginių perima lyderio funkcijas.

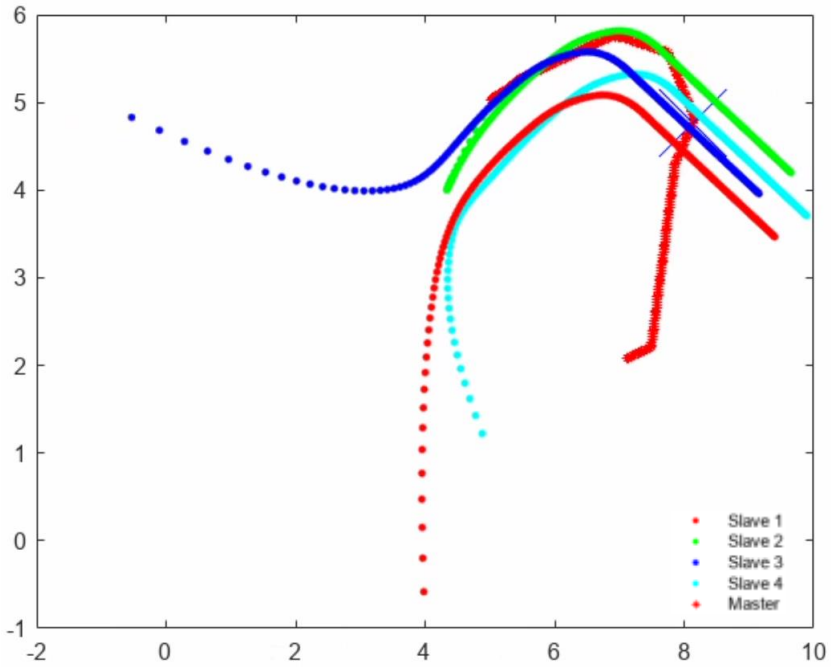
7.5. Spiečiaus lyderio komunikacijos praradimo simuliacija

Poskyryje pateikta komunikacijos praradimo tarp BO spiečiaus lyderio ir agentų. Poskyryje pateiktose simuliacijose BO spiečių sudaro 4 agentai ir vienas lyderis, norit simuliacijos pavaizdavimo aiškumo. Spiečiaus valdymo logika tokia pat kaip 3 skyriuje. Po pusės simuliacijos laiko lyderis praranda komunikacija su spiečiaus agentais. BO spiečiaus lyderis toliau juda atsitiktine trajektorija, o spiečiaus agentai juda paskutine žinoma trajektorija.



48 pav. BO spiečiaus judėjimas iki imituoto komunikacijos praradimo

48 pav. pavaizduota BO spiečiaus judėjimas iki imituoto komunikacijos praradimo simuliacija. Spiečiaus lyderio komunikacijos praradimo taškas pažymėtas mėlynu tašku.



49 pav. BO spiečiaus judėjimas po imituoto komunikacijos praradimo

49 pav. pavaizduota BO spiečiaus judėjimas po imituoto komunikacijos praradimo simuliacija. Spiečiaus lyderi juda atsitiktinai po komunikacijos praradimo, o likę agentai paskutine žinoma trajektorija. Simuliacija imituoja spiečiaus kontrolės pažeidimą, kai lyderis po kibernetinės atakos nebekomunikuoja su agentais, t.y. spiečiaus misija nutraukta.

Simuliacijos logika:

```
for t = 0:deltat:5
    % Paskutinis žinomas greitis
    if t <= 2.5
           pask_greitis(i, :) = (dv(i,:) + f1(i,:));
    end
         % Lyderio pozicijų atnaujinimas
    pozicija(10,:) = pozicija(10,:) + master_greitis_l * master_greitis * deltat;

    % Agentų pozicijų atnaujinimas
    if t <= 2.5
        for i = 1:N
            pozicija(i,:) = pozicija(i,:) + (dv(i,:) + f1(i,:)) * deltat;
        end
    else
        for i = 1:N
            pozicija(i,:) = pozicija(i,:) + pask_greitis(i,:) * deltat;
        end

    end
end
```

Agentų pozicijos atnaujinimo logika paremta paskutiniu žinomu koordinatės kitimo greičiu. Paskutinio žinomo koordinatės kitimo greičio sandauga su simuliacijos laiku ir paskutinės žinomos koordinatės vektorinė suma naudojama kaip BO spiečiaus judėjimas po imituoto komunikacijos praradimo koordinatė kiekvienam agentui.

8. Atakos elektroninėje erdvėje modelis

Jei BO spiečius pilnai autonominis, t.y. jo valdymas pagrįstas BO lyderio valdymu, ataka elektroninėje erdvėje grindžiamas įsilaužimu į BO lyderio sistemą. Kadangi BO spiečius juda erdvėje sąlyginai dideliu greičiu, tai viena iš galimų strategijų – naudoti spiečiui nepriklausantį užpuoliką orlaivį. Orlaivis užpuolikas turi būti greitesnis už spiečiaus agentus, pavyzdžiui, jei naudojami rotoriniai BO užpuolikas gali būti fiksuoto sparno orlaivis, bet pasižymintis manevringumo charakteristikomis.

Specializuotą programinę ir techninę įrangą turintis nepilotuojamas orlaivis užpuolikas galėtų būti užprogramuotas savarankiškai perimti BO lyderio kontrolę ar perimti jo funkcijas. Tokia ataka gali būti paremta BO lyderio ryšio kanalų, programinės įrangos sistemų ar net fiziniu ryšio sluoksnių pažeidžiamumu. Sėkmingai įsilaužęs į pagrindinio bepiločio orlaivio sistemą, orlaivis užpuolikas gali perimti viso spiečiaus kontrolę arba sutrikdyti jo veiklą. Priklausomai nuo savo galimybių, orlaivis užpuolikas galėtų manipuliuoti pagrindinio bepiločio orlaivio komandomis, keisti misijos parametrus ar net įvesti kenkėjišką kodą ir taip pažeisti viso spiečiaus vientisumą. Svarbu pažymėti, kad toks įsilaužimas į BO spiečiaus kontrolę yra nelegalus. Darbe aptariamos atakos prieš BO spiečių tik moksliniu požiūriu.

Norint matematiniame modelyje pavaizduoti scenarijų, kai orlaivis užpuolikas naudojamas BO lyderiui pažeisti, galime apibrėžti šiuos kintamuosius ir sąlygas:

- $P_L(t)$ – BO lyderio pažeidžiamumas laiko momentu t.
- $P_S(t)$ – viso spiečiaus pažeidžiamumas laiko momentu t.
- T_p – pažeidžiamumo tikimybė, kad užpuolikas orlaivis įsilauš į BO spiečiaus lyderio sistemą.
- $K_P(t)$ – pažeidžiamumo veiksmingumas, atsižvelgiant į tokius veiksnius kaip įgytas prieigos lygis ir įgyta kontrolė, laiko momentu t.

Tokiu atveju viso BO spiečiaus pažeidžiamumą galima apibrėžti kaip BO lyderio pažeidžiamumo ir pažeidimo efektyvumo funkciją:

$$P_S(t)=f\left(P_L(t);K_P(t);T_p\right). \quad (8.1)$$

Atsižvelgiant į tai, kad norint paveikti visą spiečių reikia pažeisti BO lyderį, sąlygą galime išreikšti taip:

$$P_S(t)>\text{pažeidžiamumo sąlyga spiečiaus}; \quad (8.2)$$

Jei:

$$P_L(t)>\text{pažeidžiamumo sąlyga lyderio}. \quad (8.3)$$

Ši sąlyga reiškia, kad viso būrio pažeidžiamumas viršija tam tikrą ribos lygį tik tuo atveju, jei pagrindinio bepiločio orlaivio pažeidžiamumas viršija atitinkamą ribą.

Pažeidžiamumo sąlygos:

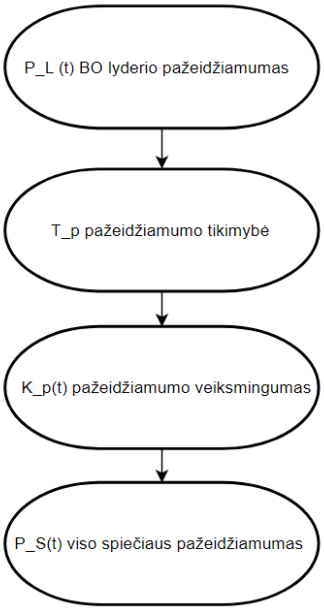
- pažeidžiamumo sąlyga spiečiaus – mažiausias viso bepiločių orlaivių spiečiaus agentų pažeidžiamumo lygis, būtinas reikšmingam poveikiui padaryti.
- pažeidžiamumo sąlyga lyderio – mažiausias spiečiaus lyderio pažeidžiamumo lygis, reikalingas sėkmingam įsilaužimui.

Be to, galima įtraukti sėkmingo pažeidimo tikimybę T_p ir pažeidimo veiksmingumą $K_P(t)$ į modelį. Pavyzdžiui:

$$P_L(t) = T_p \times K_P(t). \quad (8.4)$$

Ši lygtis parodo BO lyderio pažeidžiamumą kaip sėkmingo įsilaužimo tikimybės ir įsilaužimo efektyvumo funkciją.

Toks matematinis modeliavimas suteikia pagrindą analizuoti bepiločių orlaivių spiečiaus pažeidžiamumą, kai orlaivis užpuolikas pažeidžia pagrindinio bepiločio orlaivio sistemą. Jis leidžia įvertinti įvairius pažeidimo scenarijus ir jų galimą poveikį bendram būrio pažeidžiamumui.



50 pav. spiečiaus pažeidžiamumo loginė diagrama

Modelio sudedamosios dalys:

- $P_L(t)$ – apima tokius veiksnius, kaip saugumo priemonės, ryšių protokolai, programinės įrangos patikimumas ir bet kokie kiti svarbūs veiksniai, lemiantys BO lyderio sistemos pažeidžiamumą.
- T_p – atsižvelgiama į tokius veiksnius kaip užpuoliko galimybės, saugumo pažeidžiamumas, aplinkos veiksniai ir kiti svarbūs kintamieji, darantys įtaką sėkmingo įsilaužimo tikimybei.
- $K_P(t)$ – atsižvelgiama į tokius veiksnius kaip pažeidimo metu įgytos prieigos lygis, įgyta sistemos kontrolė, poveikis sistemos funkcionalumui ir kiti svarbūs veiksniai, turintys įtakos pažeidimo veiksmingumui.
- $P_S(t)$ – rodo viso BO spiečiaus pažeidžiamumą, kuriam įtakos turi pagrindinio bepiločio orlaivio pažeidžiamumas, pažeidimo tikimybė ir veiksmingumas.

Išvados

1. Išnagrinėti bepiločių orlaivių kolizijų išvengimo bepiločių orlaivių spiečiuje metodai. Nustatyta, kad nepriklausomai nuo ryšio tipo ar komunikacijos architektūros BO spiečiaus kolizijos išvengimas susideda iš 3 pagrindinių etapų: individualaus susidūrimo išvengimas iki formacijos; grupinio susidūrimo išvengimas po formacijos; judėjimas formacijoje. Neturint galimybės patikrinti kolizijos išvengimo reiškinio realiomis sąlygomis jis aprašytas matematinėmis lygtimis ir pavaizduotas simuliacijose.
2. Pasirinktą spiečiaus konfigūraciją sudaro 10 BO – 1 lyderis ir 9 agentai. Nustatyta, kad naudojant pasiūlytą matematinį valdymo metodą tokio dydžio spiečius atlieka misiją ir jo judėjimo paklaidos nesiekia 1%. Parodyta galimybė performuoti spiečių, kai dėl menamo įsilaužimo pasikeičia spiečiaus lyderis ir jis nebedalyvauja likusioje spiečiaus narių komunikacijoje. Pasiūlytas valdymo algoritmas tinkamas tokiai situacijai, kuris leidžia spiečiui persiformuoti nesusiduriant ir tęsti užduotą misiją toliau.
3. Nustatyta spiečiaus galimi infekavimo būdai. Naudojant STRIDE metodika nustatyti standartinio BO spiečiaus saugumo mazgai, ryšiai ir grėsmės jiems. Išskirti 4 ryšių tipai ir 2 BO spiečiaus mazgai. Ryšiams ir mazgams priskirta 11 saugumo grėsmių. Atlikus analizę, nustatyta, kad paprasčiausias ryšį tarp BO spiečiaus lyderio ir jo agentų ataka. Atlikus simuliaciją, kai naudojama *DoS* (didelis autentifikavimo paketų skaičius per sąlyginai trumpą laiko tarpą) ataka, pastebėta, kad BO lyderio judėjimo trajektorija po atakos kardinaliai pasikeitė, todėl atlikus ataką realiomis sąlygomis prognozuojamas spiečiaus misijos sutrikimas arba darnos išardymas.
4. Sudarytas BO spiečiaus lyderio BO spiečiuje indentifikavimo algoritmas. Išanalizavus spiečiaus komunikacijos ir ryšių architektūrą pastebėta, kad saugumo klausymai dėl ribotų BO spiečiaus narių galimybių nesprendžiami naudojamuose ryšio sluoksniuose arba naudojami nesudėtingai dešifruojami duomenų paketų autentifikavimo raktai. Sudarytas lyderio indentifikavimo metodo algoritmas. Pateikta spiečiaus judėjimo architektūros darnos sutrikdymo simuliacija, kai nutraukus komunikacija tarp spiečiaus lyderio ir jo agentų jie juda paskutiniais žinomais parametrais.
5. Nustatyta, kad bendras BO spiečiaus saugumas priklauso nuo BO spiečiaus lyderio pažeidžiamumo. Nepriklausomai nuo spiečiaus valdymo sistemos spiečiaus pažeidžiamumą galima išreikšti kaip funkciją nuo bendro spiečiaus pažeidžiamumo (kuris yra tiesiogiai proporcingas lyderio pažeidžiamumui duotu laiko momentu), to pažeidžiamumo veiksmingumo duotu laiko momentu ir tikimybės pažeisti BO spiečiaus lyderį. Funkcinis atakos elektroninėje erdvėje modelis gali būti panaudojamas tolimesniems vieno ar kelių sluoksnių bepiločių orlaivių spiečiaus pažeidžiamumo panaudojant ataką elektroninėje erdvėje tyrimams.

Literatūros sąrašas

1. **Daojing He, Sammy Chan, Mohsen Guuizani.** Drone-Assisted Public Safety Networks: The Security Aspect. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/7891797
2. **Mingzhe Chen , Ursula Challita , Walid Saad , Changchuan Yin , and Mérouane Debbah.** Machine Learning for Wireless Networks with Artificial Intelligence: A Tutorial on Neural Networks. Prieiga per internetą: https://scholar.google.lt/scholar?q=Machine+Learning+for+Wireless+Networks+with+Artificial+Intelligence:+A+Tutorial+on+Neural+Networks&hl=lt&as_sdt=0&as_vis=1&oi=scholart
3. **Jochen Dinger and Hannes Hartenstein.** Defending the Sybil Attack in P2P Networks: Taxonomy, Challenges, and a Proposal for Self-Registration. Prieiga per internetą: https://ieeexplore.ieee.org/document/1625383
4. **Mingzhe Chen , Ursula Challita , Walid Saad , Changchuan Yi , Mérouane Debbah**. Machine Learning for Wireless Networks with Artificial Intelligence: A Tutorial on Neural Networks. Prieiga per internetą: https://scholar.google.lt/scholar?q=Machine+learning+for+wireless+networks+with+artificial+intelligence:+A+tutorial+on+neural+networks&hl=lt&as_sdt=0&as_vis=1&oi=scholart
5. **Azade Fotouhi, Haoran Qiang, Ming Ding, Mahbub Hassan, Lorenzo Galati Giordano, Adrian Garcia-Rodriguez, Jinhong Yuan.** Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/8675384
6. **Patrick J. Vincent, Murali Tummala, John McEachen**. An Energy-Efficient Approach for Information Transfer from Distributed Wireless Sensor Systems. Prieiga per internetą: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1652281
7. **Irizarry, Javier, Gheisari, Masoud, Walker, Bruce N**. Usability assessment of drone technology as safety inspection tools. Prieiga per internetą: https://www.itcon.org/paper/2012/12
8. **Parmial Kopardekar, Ph.D.** Unmanned Aerial System (UAS) Traffic Management (UTM): Enabling Low-Altitude Airspace and UAS Operations. Prieiga per internetą: https://ntrs.nasa.gov/api/citations/20140013436/downloads/20140013436.pdf
9. **Naser Hossein MotlaghTarik Taleb, Osama Arouk.** Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/7572034
10. **Finley Barfield.** AUTONOMOUS COLLISION AVOIDANCE THE TECHNICAL REQUIREMENTS.
11. **Liang Yang**; **Juntong Qi**; **Jizhong Xiao**; **Xia Yong**. A literature review of UAV 3D path planning. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/7053093
12. **R.K. Sharma, D. Ghose.** Collision avoidance between UAV clusters using swarm intelligence techniques. Prieiga per internetą : https://www.tandfonline.com/doi/full/10.1080/00207720902750003
13. **Adam M. Brandt; Mark B. Colton**. Haptic collision avoidance for a remotely operated quadrotor UAV in indoor environments. Prieiga per internetą: https://ieeexplore.ieee.org/document/5641798

14. **Jason Israelsen**; **Matt Beall**; **Daman Bareiss**; **Daniel Stuart**; **Eric Keeney**; **Jur van den Berg**. Automatic collision avoidance for manually tele-operated unmanned aerial vehicles. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/6907839
15. **Evşen Yanmaz**; **Robert Kuschnig**; **Markus Quaritsch**; **Christian Bettstetter**; **Bernhard Rinner**. On path planning strategies for networked unmanned aerial vehicles. Prieiga per internetą: https://ieeexplore.ieee.org/document/5928811
16. **Lucía Hernández-Hernández; Antonios Tsourdos; Hyo-Sang Shin; Antony Waldock.** Multi-Objective UAV routing. Prieiga per internetą: https://ieeexplore.ieee.org/document/6842295
17. **Weisi Guo**; **Conor Devine**; **Siyi Wang**. Performance analysis of micro unmanned airborne communication relays for cellular networks. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/6923909
18. **Md. Arafatur Rahman.** Enabling drone communications with WiMAX Technology. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/6878796
19. **N. Fourty; T. Val; P. Fraisse; J.-J. Mercier.** Comparative analysis of new high data rate wireless communication technologies "From Wi-Fi to WiMAX". Priega per internetą: https://ieeexplore.ieee.org/abstract/document/1559918
20. **M.F.J. Pinkney; D. Hampel; S. DiPierro.** Unmanned aerial vehicle (UAV) communications relay. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/568581
21. **Dr. Harald Skinnemoen**. UAV & Satellite Communications Live Mission-Critical Visual Data. Prieiga per internetą: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7024391
22. **Cailian Deng; Xuming Fang; Xiao Han; Xianbin Wang; Li Yan; Rong He; Yan Long; Yuchen Guo.** IEEE 802.11be Wi-Fi 7: New Challenges and Opportunities.
23. **Mohamed-Ayoub Messous; Sidi-Mohammed Senouci; Hichem Sedjelmaci; Soumaya Cherkaoui.** A Game Theory Based Efficient Computation Offloading in an UAV Network. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/8654698
24. **Angela M. Lonzetta, Peter Cope , Joseph Campbell, Bassam J. Mohd and Thaier Hayajneh.** Security Vulnerabilities in Bluetooth Technology as Used in IoT. Prieiga per internetą: https://www.mdpi.com/2224-2708/7/3/28
25. **Drew Gislon.** Zigbee Wireless Networking. ISBN: 978-0-7506-8597-9
26. **Mohammad Tauhidul Islam; Abd-elhamid M. Taha; Selim Akl**. A survey of access management techniques in machine type communications.
27. **Stuart Bennett**. Development of the PID Controller. Prieiga per internetą: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=248006.
28. **Simone A. Ludwig, Kaleb D, Burnham**. Comparison of Euler Estimate using Extended Kalman Filter, Madgwick and Mahony on Quadcopter Flight Data. Prieiga per inernetą: https://ieeexplore.ieee.org/abstract/document/8453465
29. **Xi Chen, Jun Tang, Songyang Lao.** Review of Unmanned Aerial Vehicle SwarmCommunication Architectures and Routing Protocols. Prieiga per internetą: https://www.researchgate.net/publication/341645963_Review_of_Unmanned_Aerial_Vehicle_Swarm_Communication_Architectures_and_Routing_Protocols#fullTextFileContent

30. **Jing Dong, Kurt Ackermann, Cristina Nita-Rotaru**. Secure group communication in wireless mesh networks. Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S1570870509000365
31. **Jayanta Ghosh.** Design of a Communication Architecture for Unmanned AerialVehicle (UAV) Swarm Networks. Prieiga per internetą: https://www.researchgate.net/publication/335107014_Design_of_a_Communication_Architecture_for_Unmanned_Aerial_Vehicle_UAV_Swarm_Networks#fullTextFileContent
32. **Dymas Dymas.** IPV6 BLOCKCHAIN DATA COMMUNICATION FOR UAV SWARM-INTELLIGENCE SYSTEMS BASED ON PEER-TO-PEER, PEER-TO-MANY, AND MANY-TO-PEER SCENARIOS. Prieiga per internetą: https://apps.dtic.mil/sti/trecms/pdf/AD1200491.pdf
33. **Emil Marstrander**. Use of Messaging Layer Security in a Military UAV Swarm. Prieiga per internetą: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3118795?show=full&locale-attribute=en
34. **Mitch Campion,** Prakash Ranganathan, and Saleh Faruque. UAV swarm communication and control architectures: a review. Prieiga per internetą: https://cdnsciencepub.com/journal/doi/10.1139/juvs-2018-0009
35. **Gary B. Lamont.** UAV Swarm Mission Planning Development Using Evolutionary Algorithms - Part I.
36. **Abhishek Phadke, F. Antonio Medrano**. Towards Resilient UAV Swarms—A Breakdown of Resiliency Requirements in UAV Swarms.
37. **Sudip Misra, Pallav Kumar, Kartik Saini.** Dynamic Leader Selection in a Master-Slave Architecture-Based Micro UAV Swarm. Prieiga per internetą: https://cse.iitkgp.ac.in/~smisra/theme_pages/uav/pdfs/uav_gc.pdf
38. **Muhammad Mubashir Iqbal, Zain Anwar Ali, Rehan Khan and Muhammad Shafiq**. Motion Planning of UAV Swarm: Recent Challenges and Approaches. Prieiga per internetą: https://cdn.intechopen.com/pdfs/82985.pdf
39. **Serhii O. Kravchuk, Liana O. Afanasieva**. FORMATION OF A WIRELESS COMMUNICATION SYSTEM BASED ON A SWARM OF UNMANNED AERIAL VEHICLES. Prieiga per internetą: https://core.ac.uk/reader/323529050
40. **Ian F. Akyildiz, Xudong Wang, Weilin Wang.** Wireless mesh networks: a survey. Prieiga per internetą: https://www.sciencedirect.com/science/article/pii/S1389128604003457
41. **Piyush Gupta,P. R. Kumar.** The Capacity of Wireless Networks. Prieiga per internetą: https://ieeexplore.ieee.org/document/825799
42. **Baddeley, Michael.** Software Defined Networking for the Industrial Internet of Things. Prieiga per internetą: https://research information.bris.ac.uk/ws/portalfiles/portal/231887039/baddeley2020thesis
43. **Muhammad Shoaib Siddiqui.** Security Issues in Wireless Mesh Networks. Prieiga per internetą:https://ieeexplore.ieee.org/abstract/document/4197357
44. **Axel Neumann, Corinna Aichele, Marek Lindner, Simon Wunderlich.** Better approach to mobile ad-hoc networking (BATMAN). Prieiga per internetą: https://www.researchgate.net/publication/320172464_Better_approach_to_mobile_ad-hoc_networking_BATMAN

45. **T. Clausen, P. Jacquet.** Optimized Link State Routing Protocol (OLSR). Prieiga per internetą: https://www.rfc-editor.org/rfc/rfc3626
46. **Ozgur Koray Sahingoz.** Networking Models in Flying Ad-Hoc Networks (FANETs): Concepts and Challenges. Prieiga per internetą: https://www.researchgate.net/publication/260526688_Networking_Models_in_Flying_Ad-Hoc_Networks_FANETs_Concepts_and_Challenges
47. **Mohamad Sbeiti, Niklas Goddemeier, Daniel Behnke, Christian Wietfeld**. PASER: Secure and Efficient Routing Approach for Airborne Mesh Networks. Prieiga per internetą: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7317585
48. **Mohammed El Khattabi, Jelloul Elmesbahi, Mohammed Khaldoun, Ahmed Errami, and Omar Bouattane.** Θ(1) Time Algorithm for Master Selection in Ad-hoc Wireless Networks. Prieiga per internetą: https://www.researchgate.net/publication/344158603_TH1_Time_Algorithm_for_Master_Selection_in_Ad-hoc_Wireless_Networks
49. **Guido R. Hiertz, Philips Lothar Stibor, Yunpeng Zang, Xavier Pérez Costa, Bernhard Walke**. The IEEE 802.11 Universe. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/5394032
50. **M. Tahboush, M. Agoyi.** A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET). Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/9321400
51. **J. Grover, M. S. Gaur, V. Laxmi, N. K. Prajapati.** A sybil attack detection approach using neighboring vehicles in VANET. Prieiga per internetą: https://dl.acm.org/doi/abs/10.1145/2070425.2070450
52. **C.S. Raghavendra, K. M. Sivalingam, T. Znati.** Wireles sensor networks. ISBN 9783387352695.
53. **Nian Xia, Hsiao-Hwa Chen, and Chu-Sing Yang.** Emerging Technologies for Machine-Type Communication Networks. Prieiga per internetą: https://ieeexplore.ieee.org/abstract/document/8884232
54. **Neha Garg, Varun Bhardwaj.** Investigating the potential of IoT for Smart Healthcare solutions. Prieiga per internetą: https://www.aarf.asia/current/2023/Oct/JjCWGEpPNqEOBAP.pdf
55. **A. M. Hayajneh, S. Ali Raza Zaidi, Des C. McLernon, M. Ghogho.** Drone Empowered Small Cellular Disaster Recovery Networks for Resilient Smart Cities. Prieiga per internetą: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7746806

Priedai

1 priedas. Spiečiaus valdymo logikos kodas *Matlab* programinėje įrangoje.

Priede pateiktas BO spiečiaus valdymo logikos kodas *Matlab* programinėje įrangoje.

```
%% Start
clc
clear all
close all
%% Pradinė pozicija
poz = randi([-5,10],9,2);
pozprad=poz;
%% Tikslas
t = linspace(0,1,10);
x = cos(t.*2*pi); % nonagon x
y = sin(t.*2*pi); % nanogon y
A=[x,y];
Tikslas =
[[x(1),y(1)];[x(2),y(2)];[x(3),y(3)];[x(4),y(4)];[x(5),y(5)];[x(6),y(6)];[x(7),y(7)
];[x(8),y(8)];[x(9),y(9)]; [x(10),y(10)]];
plot(Tikslas(:,1),Tikslas(:,2),'--r*')
hold on
%plot(pozprad(:,1),pozprad(:,2),'.','Color' ,'black', 'MarkerSize',20)
%hold on;
%% Matricos
%pozicija
poz1 = [];
poz2 = [];
poz3 = [];
poz4 = [];
poz5 = [];
poz6 = [];
poz7 = [];
poz8 = [];
poz9 = [];
%jega
f_c = [];
f_trauk = zeros(1,2); %laikina
%% Kintamieji
deltat = 0.02; % ciklo žingsnis
formaK = 0.85; % formacijos kontroles koeficientas
formaM = 1.5; % formacijos momento koeficientas (prieš tikslą kaip arti
susiformuoja šalia vienas kito)
N = 9; % BO skaičius
spindulys = 0.2; % susidūrimo vengimo spindulys
alpha = 0.5; % rep_a
beta = 0.3; % rep_b

%% Ciklas
for t=0:deltat:1
    deltagreit=zeros(9,2);
    f1=zeros(9,2);
    for i=1:1:N
```

```
        deltagreit_temp = [0.0,0.0];
        for j=1:1:N
            deltagreit_temp = deltagreit_temp + (poz(j,:)-poz(i,:))-((Tikslas(j,:)-
Tikslas(i,:)));

            if norm(poz(j,:)-poz(i,:)) > 0 && norm(poz(j,:) - poz(i,:)) < spindulys
                jegos_atstum = alpha*(exp(-beta*(norm(poz(j,:)-poz(i,:)))) - exp(-
beta*spindulys));
                f_trauk = f_trauk + (poz(j,:)-poz(i,:))/norm(poz(j,:)-
poz(i,:))*jegos_atstum;
            else
                f_trauk = [0,0];
            end
        end
        deltagreit(i,1) = deltagreit_temp(1);
        deltagreit(i,2) = deltagreit_temp(2);
        f1(i,:) = f_trauk;
        f_c = [f_c; f_trauk];
    end

    centras = zeros(1,2);
    for i=1:1:N
        centras = centras + poz(i,:);
    end
    centras = centras/N;
    for i=1:1:N
        poz(i,1) = poz(i,1) + (formaK*deltagreit(i,1) - centras(1,1)*formaM -
f1(i,1))*deltat;
        poz(i,2) = poz(i,2) + (formaK*deltagreit(i,2) - centras(1,2)*formaM -
f1(i,2))*deltat;
    end
    poz1 = [poz1;poz(1,:)];
    poz2 = [poz2;poz(2,:)];
    poz3 = [poz3;poz(3,:)];
    poz4 = [poz4;poz(4,:)];
    poz5 = [poz5;poz(5,:)];
    poz6 = [poz6;poz(6,:)];
    poz7 = [poz7;poz(7,:)];
    poz8 = [poz8;poz(8,:)];
    poz9 = [poz9;poz(9,:)];
    plot(poz(1,1),poz(1,2),'.','Color' ,'red', 'MarkerSize',10);
    hold on;
    plot(poz(2,1),poz(2,2),'.','Color' ,'green', 'MarkerSize',10);
    hold on;
    plot(poz(3,1),poz(3,2),'.','Color' ,'blue', 'MarkerSize',10);
    hold on;
    plot(poz(4,1),poz(4,2),'.','Color' ,'cyan', 'MarkerSize',10);
    hold on;
    plot(poz(5,1),poz(5,2),'.','Color' ,'yellow', 'MarkerSize',10);
    hold on;
    plot(poz(6,1),poz(6,2),'.','Color' ,'black', 'MarkerSize',10);
    hold on;
    plot(poz(7,1),poz(7,2),'.','Color' ,'#D95319', 'MarkerSize',10);
```

```
    hold on;
    plot(poz(8,1),poz(8,2),'.','Color' ,'#77AC30', 'MarkerSize',10);
    hold on;
    plot(poz(9,1),poz(9,2),'.','Color' ,'#7E2F8E', 'MarkerSize',10);
    hold on;

    legend('0','1', '2', '3', '4', '5', '6', '7','8','9', 'Location', 'SouthEast')
    title('Spiečius')
    pause(deltat);
end
```

2 priedas. Spiečiaus valdymo logikos *Matlab* programinėje įrangoje skaičiavimų rezultatai.

2 lentelėje pateikti spiečiaus valdymo logikos *Matlab* programinėje įrangoje skaičiavimų rezultatai siekiant nustatyti valdymo algoritmo patikimumą.

2 lentelė. Spiečiaus valdymo logikos *Matlab* programinėje įrangoje skaičiavimų rezultatai

Tikslas x	**Tikslas y**	**Realus x**	**Realus y**
1	0	1.00077719112483	0.00856707311398047
0.766044443118978	0.642787609686539	0.764251692409020	0.644293825640122
0.173648177666930	0.984807753012208	0.171855426956973	0.986313968965791
-0.500000000000000	0.866025403784439	-0.501792750709958	0.867531619738022
-0.939692620785908	0.342020143325669	-0.941485371495866	0.343526359279252
-0.939692620785908	-0.342020143325669	-0.941485371495866	-0.340513927372086
-0.500000000000000	-0.866025403784439	-0.501792750709958	-0.864519187830856
0.173648177666930	-0.984807753012208	0.165348105798822	-0.987058540680987
0.766044443118978	-0.642787609686540	0.764251692409020	-0.641281393732957

3 lentelėje pateikti spiečiaus valdymo logikos *Matlab* programinėje įrangoje skaičiavimų rezultatų paklaidos. Paklaidos nesiekia 1%, todėl valdymo algoritmas teisingas.

3 lentelė. Spiečiaus valdymo logikos *Matlab* programinėje įrangoje skaičiavimų rezultatų paklaidos

Paklaida x, %	**Paklaida y, %**
-0.0776587567864592	0.867939717949243
0.179135848204436	0.152596415663843
0.179135848204336	0.152596415663843
0.179135848204436	0.152596415663832
0.179135848204436	0.152596415663843
0.179135848204436	0.152596415663838
0.179135848204436	0.152596415663843
0.829362613548284	-0.228029805327058
0.179135848204436	0.152596415663843

3 priedas. Spiečiaus valdymo logika *Matlab* programinėje įrangoje, kai keičiasi lyderis.

Priede pateikta spiečiaus valdymo logika *Matlab* programinėje įrangoje, kai keičiasi BO spiečiaus lyderis.

```
%% Start
clc
clear all
close all
%pozicija
pozicija = randi([-2,5],N,2); %visi BO
%% Duomenų kaupimo matricos
pozicija_masteris = [];
pozicija_slavai = [];
jegos_skaic = [];
pask_jamm_master_pozicija = [];
% Parametrai
deltat = 0.02; % ciklo žingsnis
formaK = 0.85; % formacijos kontrolės koeficientas
formaM = 1.5; % formavimosi momento koeficientas
N = 9; % Slaves skaičius
saugus_atstumas = 1.5; % mažiausias saugus atstumas tarp agentu
alpha = 0.5; % atstūmimo koeficientas alfa
beta = 0.3; % atstūmimo koeficientas beta
master_greitis_l = 1.5; % orlaivio greitis po formacijos
master_greitis = [0.2, 1]; % orlaivio greitis iki formacija ir formacijos metu
posukio_prob = 0.06; % apsisukimo tikimybė kiekvienoje iteracijoje
%% Parametrai
deltat = 0.02; % ciklo žingsnis
formaK = 0.85; %formacijos kontrolės koeficientas
formaM = 1.5; % formavimosi momento koeficientas
saugus_atstumas = 1.5; % minimalus saugus atstumas
alpha = 0.5; % atstūmimo koeficientas alfa
beta = 0.3; % atstūmimo koeficientas beta
masterio_greitis_l = 1.5; % mesterio greitis iki formacijos
masterio_greitis = [0.2, 1]; % orlaivio greitis po formacijos
pasukimo_prob = 0.001; % pasisukimo tikimybė kiekvienoje iteracijoje
jamm_tikimybe = 0.01; % jammed tikimybė kiekvienoje iteracijoje
N = 10; % Slaves skaičius
figure;
%% Ciklas
figure;
pask_jamm_master_pozicija = [];
for t = 0:deltat:8
    dv = zeros(N,2);
    f1 = zeros(N,2);
    for i = 1:N
        dv_laikina = [0.0, 0.0];
        for j = 1:N
            if j ~= i
                dv_laikina = dv_laikina + pozicija(j,:) - pozicija(i,:);
                dist = norm(pozicija(j,:) - pozicija(i,:));
                if dist > 0 && dist < saugus_atstumas
```

```
                    f_repel = alpha * (1/dist - 1/saugus_atstumas) * (pozicija(i,:)
- pozicija(j,:)) / dist^2;
                    f1(i,:) = f1(i,:) + f_repel;
                    jegos_skaic = [jegos_skaic; f_repel];
                end
            end
        end

        dv(i,:) = formaK * dv_laikina - formaM * (pozicija(i,:) - pozicija(N,:));
    end

    if rand() < jamm_tikimybe
        master_indeksas = randi([1,N]);
        masterio_greitis = [0, 0];
        pask_jamm_master_pozicija = pozicija(N,:);
        pozicija(N,:) = pozicija(master_indeksas,:);
        pozicija(master_indeksas,:) = [];
        N = N - 1;
    else
        if rand() < pasukimo_prob
            kampo_adj = rand() * pi/2 - pi/8;
            masterio_greitis = masterio_greitis * [cos(kampo_adj), -sin(kampo_adj);
sin(kampo_adj), cos(kampo_adj)];
        end
    end

    pozicija(N,:) = pozicija(N,:) + masterio_greitis_l * masterio_greitis * deltat;

    for i = 1:size(pozicija, 1)
        pozicija(i,:) = pozicija(i,:) + (dv(i,:) + f1(i,:)) * deltat;
    end

    plot(pozicija(1:N,1), pozicija(1:N,2), '.', 'Color', 'blue', 'MarkerSize', 10);
    hold on
    if ~isempty(pask_jamm_master_pozicija)
        plot(pask_jamm_master_pozicija(1), pask_jamm_master_pozicija(2), 'x',
'Color', 'red', 'MarkerSize', 10);
        hold on
    end
    plot(pozicija(N,1), pozicija(N,2), '*', 'Color', 'red', 'MarkerSize', 4);
    hold on
    %legend('BO spiečiaus agentai, 'BO spiečiaus lyderis');
    title('1 Master 9 Slaves');
    hold off
    xlim([-10 10]);
    ylim([-10 10]);
    drawnow;
    pause(deltat);
end
```