TARTU ÜLIKOOL

Arvutiteaduse Instituut

Informaatika õppekava

Olaf Daniel Seisler

Tarkvaralisel signaalitöötlusel põhinev DJI laiatarbedroonide detektor

Bakalaureusetöö (9 EAP)

Juhendaja: Jaanus Kalde, MSc

Kaasjuhendaja: Kadi Tulver, PhD

Tartu 2024

Tarkvaralisel signaalitöötlusel põhinev DJI laiatarbedroonide detektor

Lühikokkuvõte:

Viimastel aastatel on toimunud tohutu kasv tsiviildroonide kasutamises kriminaal- ja vaenutegevuses. Eriti aktiivselt on sellised droonid kasutuses Vene-Ukraina sõjas, kus nad täidavad nii luure- kui ründemissioone. Enim levinud on Hiina tootja DJI neljarootorilised droonid, mille väheselt dokumenteeritud ülesehitus raskendab nende sideprotokollide jälgimist. Droonide tuvastamiseks on erinevad tehnoloogiafirmad k.a. DJI arendanud omi lahendusi, kuid need on enamasti kulukad ning mitte kuigi portatiivsed ega paindlikud kohanema kiiresti muutuva raadiotehnoloogiaga. Võimalik lahendus eelmainitud probleemidele on kasutada odavat tarkvaralist raadiot ning digitaals-eid signaalitöötlustehnikaid. Selles bakalaureusetöös antakse esiteks ülevaade digitaalsest signaalitöötlusest ning kirjeldatakse eelnevaid teadustöid DJI droonide tuvastamise alal. Töö raames lindistatakse ja analüüsitakse ühe DJI droonimudeli signaale ning kavandatakse nende põhjal programm, mis suudab tarkvaraliselt raadiolt pärinevaid andmeid töödeldes ära tunda lähedal asuva drooni. Valminud rakenduse võimekust droone tuvastada testitakse nii simuleeritud kui ka reaalses keskkonnas. Lõpetuseks arutletakse võimalike edasiarenduste ja optimeeringute üle.

Võtmesõnad: droon, DJI, tarkvaraline raadio, signaalitöötlus.

CERCS:

P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria)

T180 Telekommunikatsioonitehnoloogia / Telecommunication engineering

T121 Signaalitöötlus

DJI consumer drone detector based on digital signal processing techniques

Abstract:

In recent years, there has been a tremendous rise in usage of civilian drones in criminal activity and armed conflict. The war in Ukraine has seen the widespread usage of commercial drones in warfare where they fly both reconnaissance and strike missions with improvised payloads. The largest manufacturer of such commercial drones is the China-based company DJI. DJI–produced drones are detectable by their radio emissions by specialist hardware which is expensive and often cumbersome. This bachelor's thesis attempts to create a means of early warning against drones by using cheap Software Defined Radio (SDR) and digital

signal processing (DSP) to detect drone signals. A brief overview of SDR and DSP is given. Past methods of detecting DJI drones are described including findings about the DJI proprietary communication protocols. A DJI drone's signals are recorded and the resulting recordings are analyzed. Based on the data, a DSP application is devised to detect the drone's radio downlink. The application is tested in both simulated and real-world environments. Finally, possible optimizations and further improvements to the system are discussed.

Keywords: drone, DJI, Software Defined Radio, Digital Signal Processing
CERCS:
P170 Computer science, numerical analysis, systems, control
T180 Telekommunikatsioonitehnoloogia
T121 Signal processing

Sisukord

Sissejuhatus

Ukrainas toimuv sõda on toonud esile tohutu kasvu laiatarbedroonide kasutuses lahingtevuses. Kompatksed ja odavad nelikopter-tüüpi droonid leiavad kasutust nii õhuluurel vastase asukoha tuvastamisel kui ka rünnakutes vastase vastu erineva improviseeritud moonaga. Väikse radariläbilõikega, madalal ja aeglaselt lendavad droonid kaovad õhutõrjeradarite ekraanidel kergelt taustamüra sisse ning isegi õnnestunud sihtmärgi jälgimise korral pole mõistlik drooni kalli raketiga rünnata [1]. Kaitsmaks sõdureid droonide eest on tarvis ergonoomilist ja kulutõhusat vahendit, millega vaenlase drooni lähedus aegsasti tuvastada. Samuti on kasvanud vajadus jälgida õhuruumi nt tsiviillennujaamade ümber ebaseadusliku droonilennutamise tõttu [2].

Laiatarbedroonide suurim tootja maailmas on Hiinas baseeruv Da-Jiang Innovations (DJI). Aastal 2020 moodustas nende turuosa 74% kõigist müüdud tsiviildroonidest ning on pidevalt kasvanud [3]. DJI droonid kasutavad suhtluseks juhtpuldi ning drooni vahel võimendatud WiFi protokolli, LightBridge'i ning Ukraina kaitsejõududes enim levinud Mavic mudeliseeriaga [4] firma enda välja töötatud OcuSynci [5]. OcuSync on DJI uusim andmeedastusprotokoll, mis võimaldab drooni juhtida kuni 8 km kauguselt ning suudab lisaks juhtmis- ning telemeetriasignaalidele kanda kõrge lahutusvõimega videot [5].

Käesolevas bakalaureusetöös luuakse signaalitöötlusprogramm, mis töötleb odava ja kättesaadava tarkvaralise raadio väljundandmeid. Programm tuvastab signaalitunnuste põhjal lähedal asuvate DJI laiatarbedroonide suhtlusprotokolli ning teavitab sellest kasutajat. Töö käigus kogutakse ka väärtuslikku infot eelnevalt dokumenteerimata DJI droonide sideprotokolli kohta, mis võimaldab edasiseid arendusi droonituvastuse valdkonnas.

Järgnevates peatükkides kirjeldatakse DJI drooni signaaliandmete kogumist tarkvaralise raadio abil, andmeanalüüsi, droonisignaale tuvastava algoritmi projekteerimist ning selle võimekuse testimist nii simuleeritud kui reaalses keskkonnas. Lisaks käsitletakse võimalikke algoritmi optimeeringuid ning edasiarendusi.

Kasutatavad terminid

Võend - ingl *sample*. Kindlal hetkel mõõdetud pideva signaali hetkväärtus. Selles lõputöös on võend kompleksarvuline väärtus, mis saadakse analoogsignaali diskreetimisel tarkvaralise raadio riistvaras.

Alamkandesagedus - ingl *subcarrier.* Osa suuremast kanalist, mis on sagedusjaotusmultipleksimisega eraldatud.

OFDM - ingl *Orthogonal Frequency Division Multiplexing*. Andmeedastusviis, kus signaalis sisalduv informatsioon jaotatakse erinevatele külgnevatele alamkandesagedustele, mis osaliselt kattuvad. Võimaldab tõhusat ja mürale vastupidavat infoedastust.

QPSK - ingl *Quadrature Phase Shift Keying*. Kvadratuur-faasmodulatsioon. Modulatsiooniskeem, kus igat sümbolit kodeerib kompleksarv, mis langeb reaal-imaginaarteljestikul ühele neljast kvadrandist.

Zadoff-Chu jada - kompleksarvuline jada, mida iseloomustavad konstantne amplituud ning autokorrelatsioon, mis on iga nullist erineva nihke puhul võrdne nulliga. Kasutatakse signaalitöötluses sageduskorrektuuriks.

Diskreetne Fourier’ teisendus - Algoritm teisendamaks jadaandmeid ajadomeenist sagedusdomeeni. Võimaldab lahutada erinevaid sagedusi sisaldava signaali selle algkomponentideks.

SNR - ingl *Signal–to-Noise Ratio*. Signaali ja müratugevuse suhe. Mõõdetakse raadiotehnikas enamasti detsibellides.

AWGN - ingl *Additive White Gaussian Noise*. Matemaatiline mudel mis simuleerib valget müra.

1. Teoreetiline taust

Teema põhjalikuks mõistmiseks oli tarvis ülevaadet täna-
päevasest signaalitöötlustehnoloogiast nagu on kasutusel WiFi- ja *Bluetooth*-võrkudes. Droonisignaalide tuvastamiseks tuli analüüsida raadiospektrit 2.4 GHz ja 5.8 GHz sagedusalal [6].

Signaalide analüüsimiseks oli põhiliseks tööriistaks ülikooli poolt laenatud HackRF One tarkvaraline raadio. HackRF suhtleb läbi draiverite arvutiga ning võimaldab nii saata kui vastu võtta raadiosignaale sagedusvahemikus 20-6000 MHz. Vahendatavad toorandmed on 8-bitisel kvadratuurkujul, mis tähendab et ühte andmepunkti signaalivoos esindab kompleksarv mille komponentideks on kaks märgiga täisarvusid kujutavat baiti, vastavalt reaal ja- imaginaarosa [7]. Signaali komplekskomponendid võimaldavad leida nii selle amplituudi kui faasi.

Tarkvaraline raadio on droonide tuvastamiseks asjakohane ja paindlik tööriist, sest annab kasutajale ligipääsu tooretele signaaliandmetele. Tarkvaralise raadio põhifunktsioon on analoog-raadiosignaalide teisendamine digitaalseks, mis võimaldab nende töötlust tarkvaras. Seega saab ühte tarkvaralise raadio süsteemi kohandada erinevateks ülesanneteks. Näiteks võib tarkvaraliselt emuleerida FM-raadiot [8], satelliidivastuvõtjat [9] ning dekodeerida isegi WiFi-signaale [10].

Tarkvaralist raadiot on kasutatud laiatarbedroonide tuvastamiseks ka varasemates teadustöödes. Teoreetilistest materjalidest andis hea ülevaate Tulsa ülikooli teadlaste Benderi ja Staggsi artikkel DJI droonide signaalianalüüsi alal odaval riistvaral [6]. Artiklis kirjeldatakse HackRFide abil üle OcuSync protokolli saadetud identimiskaadrite dekodeerimist ja nende abil droonide andmete lugemist. Uurijate pidepunktiks on vabatahtlike küberturbespetsialistide avastus, et DJI droonide saadetud identimiskaadrid saadetakse eetrisse krüpteerimata[1] [12].

[1] Autorid pakuvad, et põhjuseks USA lennundusministeeriumi (FAA) nõue, et kõik riiklikus õhuruumis lendavad mehitamata lennuvahendid peaksid saatma avalikult tuvastussignaale [11]

Bender ja Staggs kirjeldavad OcuSync protokolli dekodeerimist. OcuSync on DJI välja töötatud mitteavalik andmevahetusprotokoll, mis töötab nii 2.4 kui 5.8 GHz sagedusalal [6]. Lisaks krüpteeritud videosillale vahendab see lennumasina ja piloodipuldi vahel ka juhtsignaale ja telemeetriat [13].

OcuSync töötab ortogonaalse sagedustihenduse (OFDM) põhimõttel, kasutades ühel suhtluskanalil mitmeid kõrvuti asetsevaid ning osaliselt kattuvaid sagedusribasid [14]. Kanali osi on võimalik üksteisest eraldada faasinihete abil - sagedusel, kus ühe alamkanali signaal on maksimumis, on teised miinimumis. Alamkanalid on omakorda moduleeritud kvadratuur-faasmodulatsiooniga (QPSK) [6].

Bender ja Staggs esitavad OcuSynci DroneID kaadrist drooni info lugemiseks algoritmi [6]. Dekodeeritud identimiskaadrites on muuhulgas kirjas info drooni ja selle juhtimispuldi asukoha, drooni kiiruse, kaldenurga kohta ning seerianumber [6]. Viimane võib tulla kasuks vastase ja omade droonide eristamisel, kuna samad mudelid on Ukrainas kasutusel mõlemal vaenupoolel. Kahjuks on identimiskaadrid DJI droonide teadaolev nõrkus, ning nende võltsimiseks või summutamiseks on erinevaid meetodeid. Üks variant on kirjutada üle droonil olev püsivara [15]. Kui see ebaõnnestub, võib drooni või piloodi asukohta peita nt paigaldades elektroonika sisse positsioneerimissatelliitide signaali võltsiva kiibi. Seega ei pruugi DroneID olla kuigi töökindel viis konfliktipiirkonnas droonide tuvastamiseks.

2. DJI droonisignaalide kogumine

Valmistamaks ette drooniprotokolli dekodeerijat, on tarvis koguda eksperimentaalandmeid. Andmete efektiivseks kogumiseks tuleb arvestada mitmeid kaalutlusi nagu müra minimeerimine ja kaadritüüpide varieeruvus. Järgnevates peatükkides kirjeldatakse eksperimendis kasutatud vahendeid ning antakse detailne ülevaade andmekogumise protseduurist ja tehtud valikute kaalutlustest.

2.1 Andmete kogumise keskkond ja vahendid

Uurimisobjekt oli droon DJI Mavic Pro. Mavic Pro on populaarne mudel, mis tuli turule aastal 2017, ning kasutab tänapäeval enim levinud OcuSync suhtlusprotokolli. OcuSync on kõigi DJI droonide suhtlusprotokollidest pikima ulatusega ning tõenäoliselt ka kõige lihtsamini tuvastatav [5].

Droonisignaalide lindistamiseks kasutati HackRF One tarkvaralist raadiot ja sülearvutit Macbook Air 2020. HackRF ühildub nii Windowsi, Linuxi kui MacOSiga ning võimaldab käsurealt raadioeetri lindistamist. Põhiliste parameetritena saab HackRFile kaasa anda mõõdetava kesksageduse ning diskreetimissageduse, mis määrab mõõtmise ribalaiuse. Vastuvõtja püütud signaali toorandmed võib salvestada faili või suunata standardväljundisse [7]. HackRFil oli raadiosignaalide püüdmiseks antenn ANT700 [16], mis pole droonisignaalide sageduste jaoks optimeeritud, kuid suudab neid siiski vastu võtta ning pole kontrollitud keskkonnas takistavaks faktoriks.

Eelistatavalt tuleks lindistada droonisignaale nn Faraday puuris ehk elektriliselt isoleeritud ruumis, mida ümbritsev võrk varjestab selle sisemuse väliste elektromagnetväljade eest. Kuna OcuSync protokoll töötab samal sagedusalal Bluetoothi ja WiFiga, tuleks välja lülitada kõik sülearvuti kohtvõrguühendused ning ruumist eemaldada kõik kõrvalised digielektroonikaseadmed [17]. Siinkohal kasutati droonisignaalide lindistamiseks Tartu Ülikooli Tehnoloogiainstituudi varjestatud kambrit.

Elektrilise varje puudumisel on parim alternatiiv lindistada droonisignaale avaral väljal võimalikult kaugel elamupiirkondadest. Tähtis on, et lindistamise hetkeks oleks läheduses võimalikult vähe raadiolaineid peegeldavaid objekte nagu puid või hooneid. See aitab

vähendada mitmeid teid pidi vastuvõtjasse eri ajahetkedel jõudvate peegelduste segavat mõju [18].

Arvestama peab ka erinevate signaalitüüpide lindistamist. Kui drooni eristavad kõige enam selle identimiskaadrid, siis nt krüpteeritud videosignaal muudab sagedust harvemini ning võib olla lihtsamini jälgitav, kui signaalimuster on teada.

Tarkvaralise raadio HackRF väljundandmed on küllalti väikese dünaamilise ulatusega - vaid 8 bitti ühele mõõtetulemusele [7]. Andmete varieerimiseks peaks seadistama võimendit nii, et mõõdetava signaali amplituud oleks võimalikult lähedal maksimaalsele väärtusele.

2.2 Signaalide lindistamise protseduur

Järgnevalt kirjeldatakse droonisignaalide lindistamise protseduuri, mis viidi läbi Tartu Ülikooli Tehnoloogiainstituudi varjestatud kambris.

1. DJI Mavic Pro droon ja HackRF raadio paigutati varjestatud kambrisse üksteisest 75 cm kaugusele. Kambri küljel asuvast torust ulatus välja USB-kaabel sülearvutisse. Droon lülitati sisse ning drooni pult asus väljaspool kambrit. Joonisel 1 on toodud mõõtmiseks kasutatavad komponendid.
2. HackRFi võimendi seadistati optimaalsele tasemele tagamaks kogu dünaamilise ulatuse kasutust vastuvõtjas.
3. HackRF seadistati lindistama maksimaalse diskreetimissagedusega 20 miljonit mõõtmist sekundis.
4. HackRFiga mõõdeti sagedusvahemikke 2400-2483 MHz ja 5725-5875 MHz. Mõõtmisi saab piirata antud vahemikesse DJI Mavic Pro sagedusplaanist Euroopa majandustsoonis (CE) lähtuvalt [19]. HackRFiga ühendatud sülearvutis jooksev Pythoni skript lindistas 5 sekundi jooksul eetrit alates eelmainitud sagedusvahemike alampiiridest, tõstis kesksagedust 5 MHz võrra ning kordas mõõtmist kõrgemal sagedusel kuni sagedusvahemike ülempiirideni.
5. Raadiosignaale lindistati kaks korda nii 2.4 kui 5.8 GHz sagedusvahemikel, kuna droonisignaalid võivad sageduste vahel hüpelda [6]. Mõõtmisi teostati mõlemas sagedusalas kord kui pult oli telefonis DJI rakendusega ühendatud ning videosignaali on võimalik telefonist näha ning kord ilma videoülekandeta telefoni.

Joonis 1. Droon ja HackRF One Faraday kambris signaalide lindistamiseks.

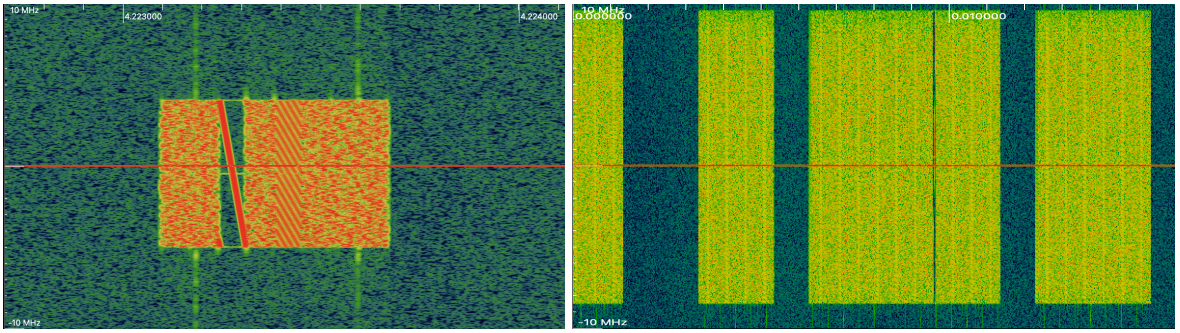
Droonisignaalide lindistamine varjestatud kambris tekitas hulga minimaalse müraga andmeid, mida kasutada statistiliseks analüüsiks ning hiljem droonidetektori testimisel baasjoonena.

3. Mõõtmise tulemused

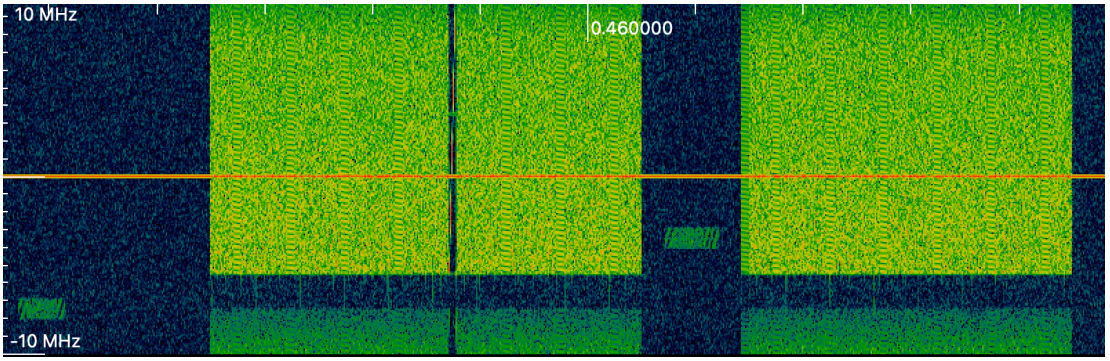
Järgnevas peatükis analüüsitakse põhjalikult mõõtmiste käigus kogutud signaaliandmeid ning kirjeldatakse erinevaid signaalitüüpe mida DJI droonid saadavad. Signaalid on kompleksarvulise võendijada kujul ning neid visualiseeritakse graafilises tarkvaras. Lähtuvalt signaalide omadustest ja varasemast uurimustest liigitatakse signaalid ning võrreldakse nende omadusi droonituvastuse kontekstis.

3.1 Signaalide visuaalne inspektsioon

Lindistuste visuaalseks inspekteerimiseks kasutati rakendust Inspectrum. Mõõtetulemuste analüüsist selgus, et DJI droonisignaalid jaotuvad põhiliselt kolmeks. Kõige märgatavamad signaalid on laiaribaline OFDM-signaal mis on ~18 MHz laiune ning selgesti äratuntav DJI DroneID identimiskaader. Esimene on püsiva kesksageduse ja pideva edastuse põhjal hinnanguliselt videosignaal. Videosignaali-tüüpi kaadreid saadab droon ka ilma pulti ühendamata, kuid need on lühikesed, katkendlikud ning fikseeritud kesksagedusele 2410 MHz, ribalaiusega ~10 MHz. Vaatamata varjestatud kambri kasutusele on spektrogrammil joonisel 4 näha ka FHSS-tüüpi sageduste vahel hüplevaid lühikesi signaale, mida võib teadaoleva info [13] põhjal pidada puldist lähtuvateks juhtsignaalideks.



Joonis 2. DroneID pakett kesksagedusel 2.43 GHz (vasakul) ning videosignaal kesksagedusel 2.45 GHz (paremal).



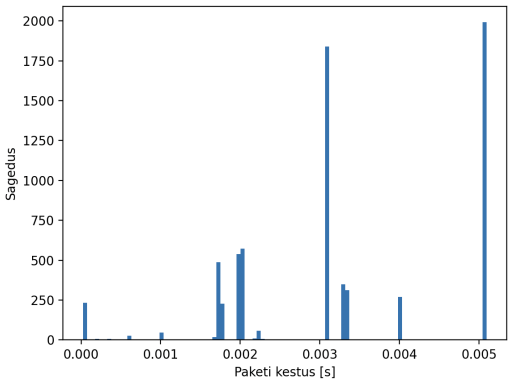
Joonis 3. FHSS-tüüpi juhtsignaalid suuremate videopakettide vahel.

Joonisel 2 on vasakul näha eelnevates uurimistöödes dokumenteeritud DroneID identimiskaadrit. Paremal olev laiem signaal kannab tõenäoliselt videot, sest on ligilähedalselt 20 MHz ribalaiusega ning püsib pikalt ühel sagedusel [20]. Joonisel 3 sagedusriba alumises osas tekkivad “peegeldused” on tõenäoliselt riistvaralise filtreerimise artefaktid ning ei esinda eraldiseisvat signaali.

3.2 Droonisignaalide statistiline analüüs

Tuvastamaks DJI drooni signaali on tarvis saada selge ülevaade signaali omadustest, mis teda teistest samal sagedusalal töötavatest eristavad. Kuna ka WiFi kanalid on samuti ca 20 MHz laiused ei tarvitse ainuüksi ribalaiuse põhjal signaali droonist lähtuvaks pidada [21].

Ajadomeenis on esmapilgul märgata videosignaalil teatud mustrit, millel korduvad erineva pikkusega kaadrid üksteise järel. Tähelepanu tõmbab ka kaader, mille keskelt leiab teravalt tõusva sagedusega peenriba-signaali, arvatavasti Zadoff-Chu jada. Sooritatakse ajadomeeni analüüs läbi programmi, mis arvutab liugakna tehnikal diskreetse Fourier’ teisenduse üle signaali võimsuse vastavalt sagedusele, otsib sagedusdomeenis vähemalt 5 MHz laiust signaali ning mõõdab ajavahemikud mil taoline signaal on aktiivne.



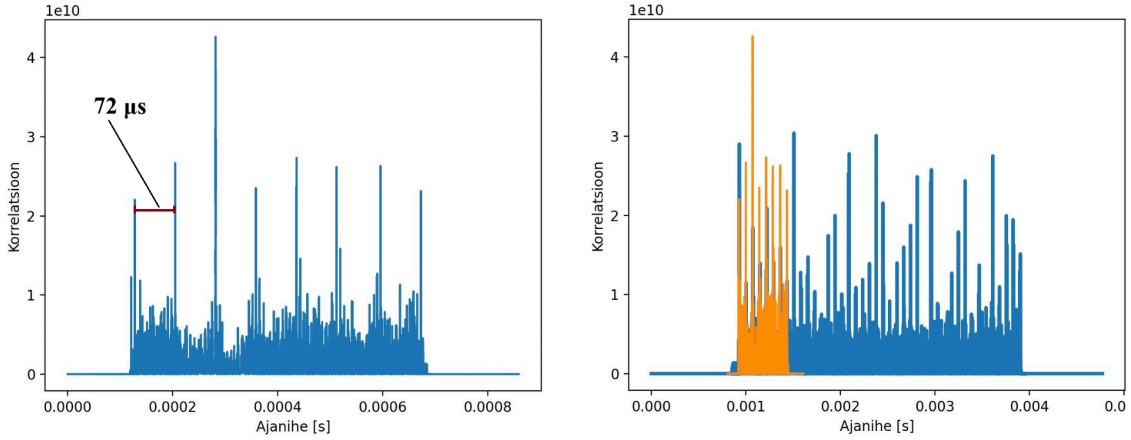
Joonis 4. Histogramm kaadrite pikkuste ja nende esinemise sagedusega üle kõigi lindistatud 5-sekundiste signaalide.

Kuigi kaadrite pikkused on koondunud täisarvuliste millisekundite juurde on see töökindlaks tuvastuseks liialt varieeruv.

Põhjalikumaks signaalianalüüsiks on kasulik teada ka teisi OFDM-signaali omadusi nt sümboli pikkus. OFDM-modulatsioonitehnikas edastatakse andmeid sümbolite kaupa, mis

konstrueeritakse erinevate alamkandesageduste kombineerimisel ning nende teisendusel sagedusdomeenist ajadomeeni. Sümbolitevahelise segunemise vältimiseks kiire andmeedastuse käigus kasutatakse tsüklilist prefiksit, st igast sümbolist võetakse tagantpoolt mingi arv bitte ning lisatakse need sümboli ette [22]. Samade andmete olemasolu iga sümboli alguses võimaldab korreleerida sümbolite alguse ja lõpu. Varasemast uurimistööst on teada, et DroneID kaadris sisalduv Zadoff-Chu jada on u 72 mikrosekundi pikkune [23]. Kuna sümbolite koostamine on spetsialiseeritud elektroonikas riistvaraliselt implementeeritud, on põhjust arvata, et ka teistel signaalidel on sarnane fikseeritud sümbolipikkus.

Fookusesse võeti drooni videosignaal. Videosignaal sobib analüüsiks hästi, sest see on spektrogrammil lai, tugev ning selle kesksagedus on võrdlemisi stabiilne. Sooritati korrelatsioon üle videosignaali sisaldava salvestuse liugakna tehnikal, kus korreleeriti üksteisest ühe sümboli pikkuse võrra nihkes olevad andmeplokid ajadomeenis. Tulemuseks oli korrelogramm, mis tõi esile sümbolite alguspunktid ajas st kohad kus „eesmine" ja „tagumine" plokk üksteisega kattuvad. Protseduur on analoogne Schiller *et al* kirjeldatud meetodiga DroneID sümbolitakti sünkroniseerimiseks [23].



Joonis 5.Vasakul DroneID korrelatsioon, paremal võrdluseks DroneID (oranž) ja videokaadri korrelatsioon.

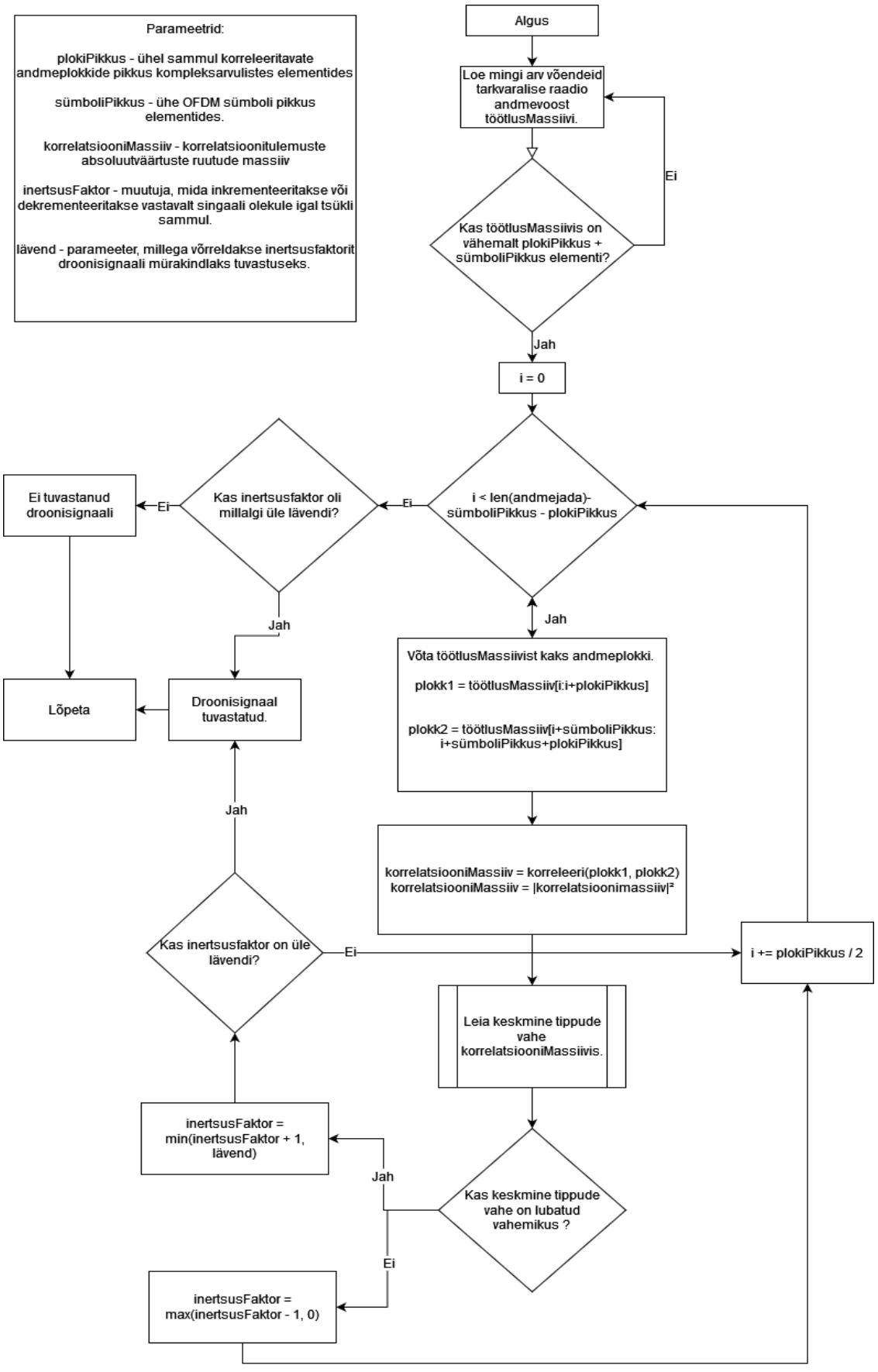
Joonisel 5 on näha korrelatsioonitehnika tulemused nii DroneID kaadril kui ka videokaadril. Mõlemal graafikul joonistuvad väljaulatuvad teravikud mille kaugus üksteisest vastab ligilähedaselt Ocusync protokolli OFDM sümboli pikkusele ehk 72 µs. Sellest järeldub, et keskmine sümboli pikkus on DroneID kaadril ja videosignaalil tõepoolest sama.

4. Droonidetektori projekteerimine

Kogutud droonisignaalide põhjal on võimalik leida neis mustreid mis eristavad neid nii taustamürast kui sarnasel sagedusel töötavatest signaalidest. Neljandas peatükis esitatakse algoritm, mis suudab DJI drooni videosignaalide omadusi arvesse võttes tarkvaralise raadio genereeritud andmejadast videosignaali olemasolu ära tunda.

4.1 Algoritmi kavandamine

Ülejäänud signaalist eristuvate tippude vahemaade järgi saab eristada OcuSynci videokaadreid sarnase ribalaiuse ja kestusega WiFi kaadritest ning muust vastuvõtjasse jõudvast mürast. Siiski võivad korrelatsiooni väärtused erineda olenevalt eetrimürast, tarkvaralise raadio võimendi seadest ning kaadrite omapärast. Näiteks tekitab pika tõusva Zadoff-Chu jadaga videokaader (vt joonis 4) eriti terava korrelatsiooni. Seega peab detektor tulema toime väga erinevate väärtustega. Esmasel katsetamisel selgus et ka eetrimüra võib vahel korrelatsioonis esineda oodatavate sümbolivahemikega. Sellest tulenevalt on valehäirete minimeerimiseks tarvis teatud inertsusfaktorit, mis takistaks detektorit liialt lihtsalt aktiveerumast ning ka deaktiveerumast. DJI drooni videosignaali tuvastamist kujutab järgnev plokkseem.



Joonis 6. DJI droonisignaali tuvastamise algoritm.

Joonisel 6 kujutatud algoritmi sisendiks olev andmejada on kompleksarvuline signaal teatud kesksagedusel. Algoritmis korreleeritakse kaks ühe sümboli võrra nihkes olevat andmeplokki (vt ptk. 3.2). Korrelatsiooni väljundväärtuste absoluutväärtused võetakse ruutu ning tulemuseks on skalaarmassiiv, milles ilmuvad OFDM-sümboli pikkuse vahega tipud. Algoritm töötleb korrelatsiooni massiivi, eemaldades liiga pikad või lühikesed tipud, ning otsustab allesjäänud tippude keskmise kauguse põhjal signaali seisu.

5. Detektori tundlikkuse mõõtmine

Eelmises peatükis kirjeldatud droonidetektori tõhususe hindamiseks viidi läbi nii teoreetilised (simuleeritud) kui ka praktilised eksperimendid. Simuleeritud testimiseks kirjutati programm, mis võtab sisendandmeteks lindistatud droonisignali ning lisab sellele järk-järgult müra. Droonidetektorit katsetati mürase signaaliga leidmaks minimaalset signaali ja müra suhet, millega detektor suudab droonisignaali lindistuselt tuvastada. Praktilise testimise peatükis kirjeldatakse droonidetektori katsetamist pargis, mille käigus tehti kindlaks selle maksimaalne tuvastuskaugus reaalses keskkonnas.

5.1 Simuleeritud testimine

Teoreetiline tuvastusvõime raadiosüsteemides sõltub põhiliselt signaalitugevuse ja müra suhtest (*signal to noise ratio,* edaspidi SNR). Müraks loetakse kõrvaliste signaalide ebakoherentset kombinatsiooni, mis eksisteerib igas reaalse elu süsteemis ning mõjutab otsitava signaali eristatavust. Müra allikateks võivad olla soojusmüra mõõteseadmes, looduslikud protsessid ning ka mõõdetava signaaliga samal sagedusel töötavad elektroonikaseadmed [24]. Eelmainitud allikatest lähtuvad impulsid sulanduvad vastuvõtjas kokku ning tekitavad selles nn müratasseme, millest nõrgemate signaalide tuvastamine on keerukas.

Taolise müra simuleerimiseks katsekeskonnas kasutatakse mõistet AWGN ehk aditiivne valge Gaussi müra. AWGN sobib müra simuleerimiseks sest selle iseloomulikud jooned on ühtlane võimsus üle kogu signaali sageduste spektri ning normaaljaotusele vastav intensiivsus ajadomeenis [24]. Müra lisamiseks olemasolevale signaalile piisab vaid väärtuste liitmisest. AWGN müramudel ei võta arvesse muid maapealses kommunikatsioonis segavaid faktoreid nagu mitmikpeegeldused ja samal kanalil leiduvaid koherentseid signaale, kuid nende simuleerimine on väljaspool selle lõputöö ulatust.

Teoreetilise tuvastusvõimekuse testimiseks simuleeriti AWGN müra lindistatud droonisignaalidel. Testimiseks kohandati müra lisamise algoritm digitaalsel suhtluskanalil [25]:

lisaSignaalileMüra():

sisend: signaal (kompleksarvuline signaalimassiiv)
sisend: n (signaali kompleksarvuliste elementide arv)
sisend: SNR (soovitud signaali ja müra suhe detsibellides)
lineaarneSNR := $10^{SNR/10}$

$$\text{keskmineSignaaliVõimsus} = \sum_{i=0}^{n} |\text{signaal}|^2$$

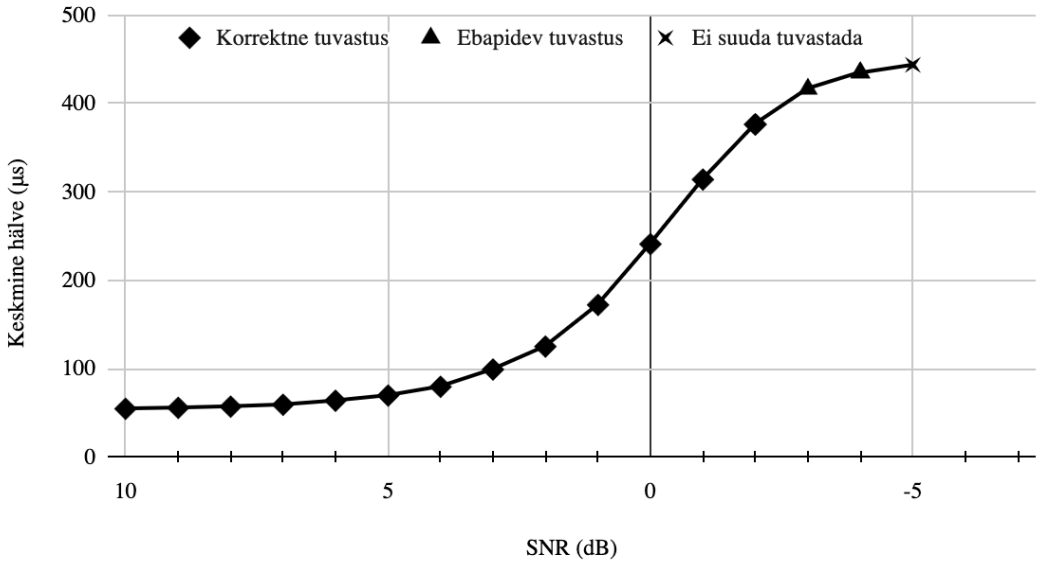
müraVõimsus = keskmineSignaaliVõimsus / lineaarneSNR
müraReaalOsa = $X_1, X_2, \ldots X_n \sim N(0, 1)$
müraImaginaarOsa = $X_{n+1}, X_{n+2}, \ldots X_{2n} \sim N(0, 1)$
lisatavMüra = müraReaalOsa + $i \cdot$ müraImaginaarOsa

$$\text{lisatavMüra} = \text{lisatavMüra} \cdot (\text{müraVõimsus} / \sum_{i=0}^{n} |\text{lisatavMüra}|^2)^{1/2}$$

tagasta: signaal + lisatavMüra

Algoritm 1. Müra lisamine komplekssignaalile.

Testkoodis jooksutati müra lisamise algoritmi järjest kahaneva SNRiga eelnevalt Faraday puuris üles võetud 5-sekundisele lindistusele. Lindistusel oli läbiv drooni videosignaal ning pea olematu taustamüra. Igal sammul testiti eelmises peatükis kirjeldatud droonituvastusalgoritmi, ning langetati SNRi 1 detsibelli võrra. Kui skänner ei suutnud signaali teatud müratasemel lindistuselt enam tuvastada, siis lõpetas testkood oma töö. Simuleeritud testimise tulemused on toodud Joonisel 6.



Joonis 7. Keskmine hälve oodatavast sümboli pikkusest vs. SNR

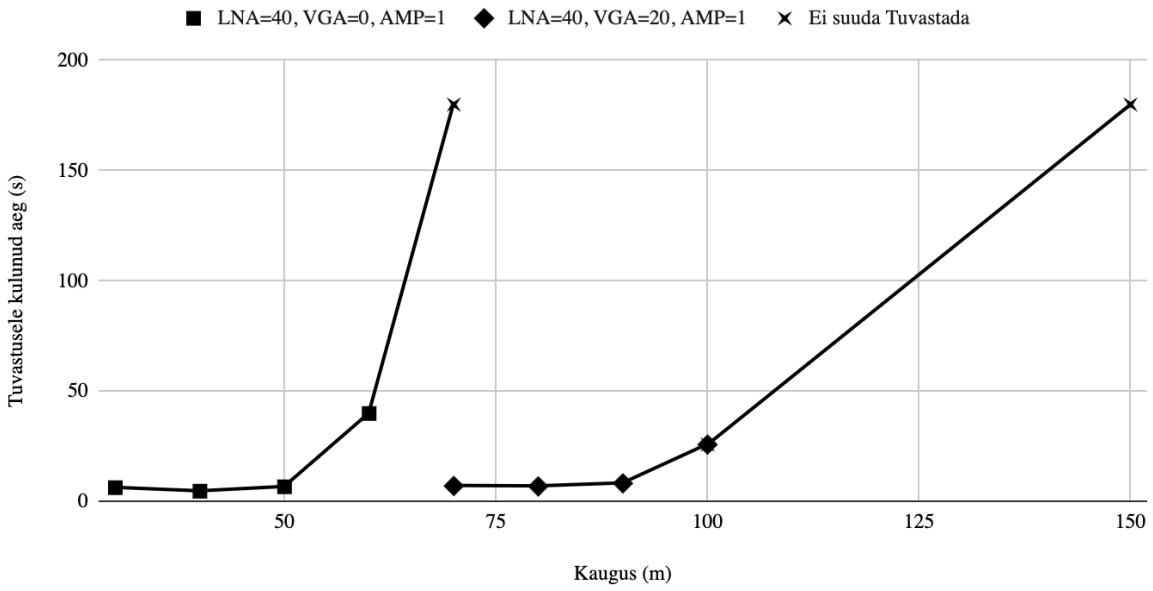
Teoreetilise testimise tulemustest on näha, et droonisignaali tuvastuse algoritm suudab efektiivselt tuvastada kui SNR on kõrgem kui -3dB. Alla SNRi -3dB on tuvastusvõime ebapidev. Detektori suudab kohati signaali tuvastada, kuid kaotab selle tihti taustamüra sisse, ning võib aktiveeruda ning deaktiveeruda korduvalt.

5.2 Testimine reaalses keskkonnas

Lisaks teoreetilisele efektiivsusele katsetati süsteemi ka päris linnakeskkonnas. Tartus Vaksali pargis tehtud mõõtmiste käigus anti algoritmile andmeid faili asemel tarkvaralisest raadiost HackRF. HackRFiga liidestumiseks kasutaty SoapySDR teeki [26]. Droonituvastaja efektiivsuse mõõtmiseks reaalses olustikus seati arvutiga ühendatud HackRF skaneerima raadioeetrit sagedusvahemikus 2400-2480 MHz ning üritati tuvastada drooni signaal erinevatelt kaugustelt ning leida maksimaalne vahemaa, mille tagant suudab droonidetektor drooni ära tunda. Ka drooni videosignaali sagedusala piirati drooni seadetes eeltoodud vahemikku. DJI juhtpuldid võimaldavad määrata 2.4 või 5.8 GHz sagedusala, kuid mitte täpset kanalit nendes vahemikes. Droon võib ka videoedastuse ajal määratud sagedusvahemikus kanalit vahetada. Detektor peab seetõttu rakendama tuvastusalgoritmi üle terve sagedusvahemiku, et leida parasjagu kasutatav kanal. Droon asetati maapinnale tuvastusseadmetest järk-järgult kaugemale kohta, kus oli tagatud otsenähtavus drooni ja saatja vahel. Signaaliandmeid töötles arvutis Pythoni programm, mis seadistas HackRFi kesksagedust 10 MHz pikkuste sammudega sagedusvahemikus edasi ja tagasi, lindistades eetrit igas vahemikus 1 sekundi jooksul. Programm lõpetas töö esimese signaalituvastuse hetkel. Sooritati viis mõõtmist igalt mõõdetavalt kauguselt ning arvutati keskmine aeg, mis kulus droonisignaali tuvastamiseks. Kui rakendus ei suutnud teatud kauguselt drooni 180 sekundi jooksul tuvastada, loeti see katse läbikukkunuks.

HackRFi vastvõtuahelal on kolm sisseehitatud võimendit. AMP ehk antenni eelvõimendi võimendab kõiki vastuvõetud signaale enne töötlusahelasse edasi saatmist. LNA ehk vahesagedusvõimendi võimendab signaali, mis on efektiivsemaks töötluseks madalama sagedusega taktsignaaliga segustatud. LNA eesmärk on muuta signaali võimsus töötluseks kõlblikuks ning minimeerida võimendi enda müra. Viimaks on võimalik signaali amplituudi korrigeerida VGA ehk põhiribavõimendiga, millel on suur seadistusvahemik (0-62 dB) [27]. Droonituvasti testimiseks oli algselt eelvõimendi sisse lülitatud, LNA seadistatud maksimumväärtusele 40 ning VGA välja lülitatud. Kui droon asetati vastuvõtjast liialt

kaugele ning detektor ei suutnud seda enam ära tunda, seati VGA võimendustase kõrgemaks. Esitati katsetulemused koos parasjagu kasutusel olnud võimendi seadetega. Joonis 8 kõrvutab keskmist drooni tuvastusele kulunud aega drooni kaugusega vastuvõtjast.



Joonis 8. Drooni kaugus vs. tuvastusele kuluv aeg.

Seadetega LNA=40, VGA=30, AMP=1 tuvastas rakendus küll droonisignaali samal sagedusel, kus vahetult enne oli drooni videosignaal paiknenud kauguselt 150 m, kuid andis ka mitu valehäiret. Seetõttu ei saa lugeda seda usaldusväärseks tuvastuskauguseks. Kõrgemate VGA võimendustega kaasnes valehäirete tiheduse kasv, mistõttu selle parameetri kergitamist ei jätkatud.

Kuigi valminud tarkvaralisel raadiol põhinev droonidetektor suudab tuvastada drooni umbes 100 meetri kauguselt on süsteemis puudujääke. Esiteks polnud eeltoodud eksperimentideks saadaval uuritavatele sagedustele sobivat antenni. Tuvastuskauguse mõõtmisel kasutati ANT700 antenni, mille ettenähtud sagedusvahemik on 300 MHz ja 1100 MHz vahel [16]. Samuti on HackRFi vastuvõtja 5 GHz sagedusalas võrreldes 2.4 GHz ribaga ligi 20 dB võrra nõrgem [28], mistõttu ei suuda detektor hästi tuvastada kõrgemaid sagedusi kasutavaid droone.

6. Edasiarendused

Saavutamaks oma eesmärki, peaks droonituvastil optimeerima nii tarkvara kui riistvara. Lisaks riistvaralistele puudujääkidele jätab ka droonituvastusalgoritm madala SNRiga signaalis paljud silmaga nähtavad droonikaadrid tuvastamata. Peamiselt on probleem tippude tuvastamisel droonisignaali olemasolu kontrollis, sest mürase signaali korrelatsioonis pole tippude kaugused ühtlased. Kuigi korrelatsioon on kaadri vastuvõtul taustamürast kõrgem, on keeruline seda varieeruvate tippude kauguste tõttu eristada nt WiFi-kaadrist. Tagatipuks nõuab korrelatsiooni algoritm palju arvutusvõimsust ning ei tööta reaalajas ka üsna võimsal Apple Silicon M1 protsessoriga sülearvutil. Suurema jõudlusega kiibi või nt graafikakaardi kasutamine jällegi võtaks rohkem voolu ning teeks kogu süsteemi oluliselt kohmakamaks, rääkimata kõrgemast hinnast. Võimalik lahendus on kasutada mõnda muud tuvastustehnikat nt korrelatsiooni üle signaali spektrogrammi sobitatud filtriga, mis on eeldatava signaalimustriga sarnane.

Tagamaks droonituvasti portatiivsust tuleks lihtsustada algoritmi ja/või kasutada spetsiaalset signaalitöötluse kiipi (DSP - ingl *Digital Signal Processor*). DSP-kiipidel on sageli riistvarasse sisseehitatud funktsioonid nt diskreetse Fourier' teisenduseks, mis vähendaks oluliselt koormust põhiprotsessoril ja võimaldaks korrelatsiooni algoritmi kiirendada [29]. DSP-kiibid on kommertsturul aga üsna väikeses mahus ning seetõttu tavatarbijale ka üsna kulukad. Alternatiivselt võiks ümber programmeerida mõne tarbekaubana müüdava WiFi-adapteri. Kahjuks on enamike WiFi ja Bluetooth sagedustel töötavate kiipide raadiofunktsioone juhtiv püsivara kinnine ning raskesti pöördprojekteeritav. Siiski leiduvad mõnedele Qualcomm Atheros seeria kiipidele Linuxi draiverid, mis võimaldavad adaptereid kasutada spektrianalüüsiks [30]. Taoline lisafunktsioon võimaldaks tuvastada WiFi-st erinevaid raadiosignaalide allikaid, kuid oleks piiratud vaid signaalitugevuse andmetega WiFi sageduste spektril.

Vastuvõtja tuvastuskauguse parandamiseks tuleks kasutada suundantenne, mis võimendavad soovitud sektorist tulevaid signaale ning on optimeeritud töötama nii 2.4 kui 5 GHz sagedusalas. Efektiivseks suunamääramiseks läheb tarvis mitmeid suundantenne ning need tuleks paigutada ringikujuliselt suunatuna eri sektoritesse. Tarvis oleks ka antennimultiplekserit, mis detektori ühendust eri antennide vahel kiirelt ümber lülitaks ning seejärel tugevaima signaali suuna kindlaks teeks.

Kokkuvõte

Lõputöö eesmärk oli luua tarkvaralisel raadiol põhinev lahendus, mis töötaks odaval kommertselektroonikal ning tuvastaks DJI laiatarbedroone.

Koostati droonituvastusprogramm, kanti see sülearvutile ning liidestati tarkvaralise raadioga HackRF. Lõputöö käigus välja töötatud rakendus suudab tuvastada droone arvestatavalt distantsilt ning on töökindel ka mürases keskkonnas. Lisaks on see lihtsalt teisaldatav erinevatele arvutitele, operatsioonisüsteemidele ning tarkvaralise raadio platvormidele.

Droonisignaalide tuvastamisel olid keerukaimad asjaolud DJI droonide dokumenteerimata suhtlusprotokoll ning töökindluse saavutamine nõrga signaali või müra olemasolul. Droonisignaalide omaduste uurimiseks lindistati DJI drooni elektriliselt varjestatud kambris, et tagada analüüsiks võimalikult puhas signaal. Lähtuvalt raadioelektroonika teadmistest ning varasematest teadusartiklitest droonituvastuse alal sooritati kogutud andmetel statistiline analüüs, mis tõi esile uut informatsiooni DJI droonide vähe dokumenteeritud videosignaalide kohta. Statistilises analüüsis selgunud omaduste põhjal kavandati algoritm, mis kasutab tarkvaralist raadiot raadiosignaalide püüdmiseks ning otsib neis DJI droonide videokaadreid.

Valminud droonituvastit hinnati nii uurimistöö käigus tehtud lindistustel, millele lisati järk-järgult simuleeritud müra, kui ka reaalses keskkonnas, kus droonituvastust raskendas kauguse tõttu nõrgenev signaal. Mõõtetulemustest selgus, et droonidetektor suudab tuvastada DJI drooni videosignaali isegi kergelt negatiivse SNRi juures ning tuvastuskaugust piiras eelkõige kasutatav elektroonika.

Võimalikud edasiarendused hõlmaksid tuvatusalgoritmi tõhustamist müraga toime tulekus ja töötluskiiruses. Kompaktsuse nimel tuleks kanda tuvastusalgoritm signaalitöötlusriistvarale. Samuti on võimalik lisada droonidetektorile suunamääramisvõimekus kasutades suundantenne, mis parandaksid ka tuvastuskaugust.

Viidatud kirjandus

[1] D. Kunertova, “The war in Ukraine shows the game-changing effect of drones depends on the game”, Accessed: Apr. 24, 2024. [Online]. Available: https://www.tandfonline.com/doi/epdf/10.1080/00963402.2023.2178180?needAccess=true

[2] G. Lykou, D. Moustakas, and D. Gritzalis, “Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies,” *Sensors*, vol. 20, no. 12, Art. no. 12, Jan. 2020, doi: 10.3390/s20123537.

[3] S. French, “DJI market share: here’s exactly how rapidly it has grown in just a few years,” The Drone Girl. Accessed: Dec. 04, 2023. [Online]. Available: https://www.thedronegirl.com/2018/09/18/dji-market-share/

[4] E. Gosselin-Malo, “Ukraine continues to snap up Chinese DJI drones for its defense,” *C4ISRNet*, Oct. 23, 2023. Accessed: Dec. 04, 2023. [Online]. Available: https://www.c4isrnet.com/global/europe/2023/10/23/ukraine-continues-to-snap-up-chinese-dji-drones-for-its-defense/

[5] “DJI Transmission Systems – Wi-Fi, OcuSync & Lightbridge,” heliguy™. Accessed: Dec. 04, 2023. [Online]. Available: https://www.heliguy.com/blogs/posts/dji-transmission-systems-wi-fi-ocusync-lightbridge

[6] C. Bender and J. Staggs, “Leveling the Playing Field: Equipping Ukrainian Freedom Fighters with Low-Cost Drone Detection Capabilities,” in *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, Tallinn, May 2023, pp. 287–312. doi: 10.23919/CyCon58705.2023.10181421.

[7] “HackRF Tools — HackRF documentation.” Accessed: Dec. 04, 2023. [Online]. Available: https://hackrf.readthedocs.io/en/latest/hackrf_tools.html

[8] v3l0c1r4pt0r, “RTL-SDR FM Radio Receiver With GNU Radio Companion,” Instructables. Accessed: May 10, 2024. [Online]. Available: https://www.instructables.com/RTL-SDR-FM-radio-receiver-with-GNU-Radio-Companion/

[9] D. Estévez, “daniestevez/gr-satellites.” Apr. 30, 2024. Accessed: May 10, 2024. [Online]. Available: https://github.com/daniestevez/gr-satellites

[10] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir, “SWiFi: An Open Source SDR for Wi-Fi Networks High Order Modulation Analysis”.

[11] “14 CFR Part 89 -- Remote Identification of Unmanned Aircraft.” Accessed: Dec. 04, 2023. [Online]. Available: https://www.ecfr.gov/current/title-14/part-89

[12] S. Hollister, “DJI insisted drone-tracking AeroScope signals were encrypted — now it admits they aren’t,” *The Verge*, Apr. 28, 2022. Accessed: Dec. 04, 2023. [Online]. Available: https://www.theverge.com/2022/4/28/23046916/dji-aeroscope-signals-not-encrypted-drone-tracking

[13] I. T. Christof, “DJI Wi-Fi Protocol Reverse Engineering”.

[14] Mohammad S. Obaidat, Alagan Anpalagan, and Isaac Woungang, “Handbook of Green Information and Communication Systems,” in *Handbook of Green Information and Communication Systems*. Accessed: Dec. 04, 2023. [Online]. Available: https://www.sciencedirect.com/topics/engineering/orthogonal-frequency-division-multiplexing

[15] MAVProxyUser, “MAVProxyUser/CIAJeepDoors.” Apr. 12, 2024. Accessed: Apr. 12, 2024. [Online]. Available: https://github.com/MAVProxyUser/CIAJeepDoors

[16] “ANT700 - Great Scott Gadgets.” Accessed: May 09, 2024. [Online]. Available: https://greatscottgadgets.com/ant700/

[17] Ryan Winfield Woodings and M. Gerrior, “2.4 GHz ISM Band: Avoiding Interference,” EE Times. Accessed: May 10, 2024. [Online]. Available: https://www.eetimes.com/avoiding-interference-in-the-2-4-ghz-ism-band/

[18] M. Lichtman, “PySDR: A Guide to SDR and DSP using Python,” in *Multipath Fading — PySDR: A Guide to SDR and DSP using Python*. Accessed: May 10, 2024. [Online]. Available: https://pysdr.org/content/multipath_fading.html

[19] “Mavic Pro User Manual V2.0.pdf.” Accessed: May 02, 2024. [Online]. Available: https://dl.djicdn.com/downloads/mavic/20171219/Mavic%20Pro%20User%20Manual%20V2.0.pdf

[20] “DJI Mobile SDK Documentation.” Accessed: May 07, 2024. [Online]. Available: https://developer.dji.com/api-reference/android-api/Components/OcuSyncLink/DJIOcuSyncLink.html#djiocusynclink_djiocusyncbandwidth_inline

[21] C. Ruth, “The Evolution of Wi-Fi Technology and Standards,” IEEE Standards Association. Accessed: Mar. 08, 2024. [Online]. Available: https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards/

[22] “What is CP-OFDM? - everything RF.” Accessed: May 10, 2024. [Online]. Available: https://www.everythingrf.com/community/what-is-cp-ofdm

[23] N. Schiller *et al.*, “Drone Security and the Mysterious Case of DJI’s DroneID,” in *Proceedings 2023 Network and Distributed System Security Symposium*, San Diego, CA, USA: Internet Society, 2023. doi: 10.14722/ndss.2023.24217.

[24] “What Is Additive White Gaussian Noise & Why Is It Important for Test & Measurement?” Accessed: May 04, 2024. [Online]. Available: https://blog.wtcom.com/what-is-additive-white-gaussian-noise-why-is-it-important-for-test-measurement

[25] “How to Add Noise to Set a Digital Communications Signal to a Given Es/N0 | TomRoelandts.com.” Accessed: May 04, 2024. [Online]. Available: https://tomroelandts.com/articles/how-to-add-noise-to-set-a-digital-communications-signal-to-a-given-esn0

[26] “pothosware/SoapySDR.” Pothosware, May 03, 2024. Accessed: May 06, 2024. [Online].

Available: https://github.com/pothosware/SoapySDR

[27] “Welcome to HackRF’s documentation! — HackRF documentation.” Accessed: Apr. 24, 2024. [Online]. Available: https://hackrf.readthedocs.io/en/latest/

[28] M. Ossman, “Testing a HackRF Clone - Great Scott Gadgets.” Accessed: May 09, 2024. [Online]. Available: https://greatscottgadgets.com/2021/12-07-testing-a-hackrf-clone/

[29] N. S. Senobari *et al.*, “Super‐Efficient Cross‐Correlation (SEC‐C): A Fast Matched Filtering Code Suitable for Desktop Computers,” *Seismol. Res. Lett.*, vol. 90, no. 1, pp. 322–334, Jan. 2019, doi: 10.1785/0220180122.

[30] “en:users:drivers:ath10k:spectral [Linux Wireless].” Accessed: May 09, 2024. [Online]. Available: https://wireless.wiki.kernel.org/en/users/drivers/ath10k/spectral

Lisad

I. Koodirepositoorium

Droonidetektori prototüüpkood asub GitHubi repositooriumis.

Githubi repositooriumi link: https://github.com/Olafseisler/dji-drone-detector

II. **Litsents**

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks.

Mina, Olaf Seisler

1. Annan Tartu Ülikoolile tasuta loa (lihtslitsentsi) minu loodud teose "Tarkvaralisel signaalitöötlusel põhinev DJI laiatarbedroonide detektor", mille juhendajaks on Jaanus Kalde ja kaasjuhendajaks Kadi Tulver, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digiarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Olaf Daniel Seisler
13.05.2024