Tampereen yliopisto

Olli Numminen

HENKILÖTASON SUOJA DRONEILTA RADIOMENETELMILLÄ

Kandidaatintyö
Informaatioteknologian ja viestinnän tiedekunta
Tarkastaja: Taneli Riihonen
Tammikuu 2025

TIIVISTELMÄ

Olli Numminen: Henkilötason suoja droneilta radiomenetelmillä
Kandidaatintyö
Tampereen yliopisto
Tietotekniikan tutkinto-ohjelma
Tammikuu 2025

Dronejen rooli sodankäynnissä on noussut merkittäväksi viimeisten vuosien aikana. Dronejen suhteellisen halpa hinta ja niiden tarjoamat mahdollisuudet tiedustelussa sekä kohteeseen vaikuttamisessa ovat tehneet niistä merkittävän uhan taistelukentällä. Dronet ja niiden käyttötaktiikat kehittyvät vauhdilla erityisesti Ukrainan sodan johdosta, jossa osapuolet pyrkivät jatkuvsti kehittämään uusia keinoja dronejen hyödyntämiseen. Tämä on luonut kasvavan tarpeen myös dronejen vastaisten menetelmien ja järjestelmien kehitykselle.

Tässä työssä käsitellään taistelukentän droneuhan torjuntaa radiomenetelmin keskittyen henkilötasoon eli yksittäisen taistelijan tasoon. Työssä käsitellään uhan torjuntaa reaktiivisten vastatoimien näkökulmasta, eli keskitytään havaitsemiseen, paikannukseen sekä torjuntaan. Havaitsemisen ja paikannuksen suhteen esiteltävät tekniset menetelmät sekä julkisista lähteistä löytyvät järjestelmät, toimivat passiivisesti eli ne eivät lähetä radiosignaaleja ympäristöönsä, eikä niitä näin ollen kykene signaalitiedustelun keinoin havaitsemaan. Torjunnassa esiteltävät häirintämenetelmät sekä löydetyt häirintälähettimet ovat aktiivisia, eli ne lähettävät ympäristöönsä radiosignaaleja ja ne kyetään myös vastapuolen signaalitiedustelun keinoin potentiaalisesti havaitsemaan.

Työssä esitellään ensin vaatimukset, joita henkilötaso ja taistelukentän olosuhteet luovat droneuhan torjunnan näkökulmasta. Seuraavaksi esitellään eräitä teknisiä menetelmiä, joilla droneja voidaan havaita sekä paikantaa. Näiden avulla analysoidaan julkisista lähteistä löytyneiden järjestelmien kyvykkyyksiä ja sopivuutta henkilötasolla käytettäväksi modernin taistelukentän olosuhteissa. Menetelmiä tai olemassa olevia järjestelmiä ei esitellä tyhjentävästi, vaan tarkoituksena on esitellä sopivia esimerkkejä ja luoda näin käsitys droneuhan havaitsemisen ja paikannuksen nykytilanteesta.

Tämän jälkeen työssä edetään torjuntaan. Ensin esitellään torjunnassa käytettävät erilaiset häirinnän muodot, josta edetään analysoimaan julkisista lähteistä löytyneitä järjestelmiä. Erityisesti torjunnan tapauksessa valmista järjestelmää henkilötasolle ei löydy, joten työssä on keskitytty etsimään järjestelmiä, jotka ovat mahdollisimman sopivia kyseiseen tarkoitukseen.

Työssä havaittiin, että erityisesti dronejen havaitsemiseen on olemassa henkilötason radiomenetelmin toimivia järjestelmiä, joita hyödynnetään jo nyt taistelukentällä. Toisaalta havaittiin myös, ettei torjuntaan ole avoimista lähteistä havaittu henkilötason vaatimuksia täyttävää järjestelmää. Suurimpana haasteena henkilötason järjestelmillä ovat dronejen jatkuva kehitys, mikä tuottaa jatkuvan tarpeen kehittää uusia järjestelmiä tai päivittää vanhoja sekä erityisesti torjunnan suuri energiankulutus, mikä vaatii suurten akkujen kantamista yksittäiseltä taistelijalta.

Avainsanat: drone, drooni, lennokki, torjunta, havaitseminen, paikannus, radiomenetelmä, henkilötaso, taistelukenttä, elektroninen suojautuminen

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -ohjelmalla.

TEKOÄLYSOVELLUSTEN KÄYTTÖ OPINNÄYTETYÖSSÄ

Opinnäytteessäni käytetyt tekoälytyökalut ja niiden käyttötarkoitukset on kuvailtu alla:

Työkalun nimi (ja versio):

- ChatGPT-4

Käyttötarkoitus ja osio, jossa työkalua käytettiin:

- Työkalulla käännettiin tekstiä ukrainasta, venäjästä ja englannista suomeksi.

Olen tietoinen siitä, että olen täysin vastuussa koko opinnäytteeni sisällöstä, mukaan lukien tekoälyllä tuotetut osat, ja hyväksyn vastuun mahdollisista eettisten ohjeiden rikkomuksista.

SISÄLLYSLUETTELO

1. Johdanto 1
2. Dronen havaitseminen ja paikannus radiosignaaleja hyödyntäen 3
2.1 Vaatimukset henkilötasolla ja taistelukentällä 3
2.2 Dronen havaitseminen 6
2.3 Dronen paikannus 9
3. Dronen havaitseminen ja paikannus käytännössä 11
3.1 Sormenjälkeen pohjautuvat järjestelmät 11
3.2 Spektrianalysaattorit 15
3.3 Analogisen videosignaalin kaappaus 17
4. Dronen torjunta 19
4.1 Dronen torjunta radiohäirinnällä 19
4.2 Torjunta käytännössä 22
5. Yhteenveto 26
Lähteet 28

LYHENTEET JA MERKINNÄT

AOA	Atsimuuttikulma (engl. Angle Of Azimuth)
AOE	Korotuskulma (engl. Angle Of Elevation)
DWT	Diskreetti aallokemuunnos (engl. Discrete wavelet transform)
F2T2EA	Löydä, Lukitse, Seuraa, Valmistele, Vaikuta, Arvioi (engl. Find, Fix, Track, Target, Engage, Assess)
F5	Löydä, Lukitse, Valmistele, Vaikuta, Arvioi (engl. Find, Fix, Fire, Finish, Feedback)
FHSS	Taajuushyppelyhajaspektri (engl. Frequency-hopping spread spectrum)
FPV	Ensimmäisen persoonan näkymä (engl. First-person view)
GNSS	Maailmanlaajuinen satelliittinavigointijärjestelmä (engl. Global satellite navigation system)
IP	Kotelointiluokka (engl. Ingress protection)
ISM	Teollinen, tieteellinen ja lääketieteellinen (engl. Industrial, scientific and medical)
MUSIC	Usean signaalin luokittelu (engl. Multiple signal classification)
OSINT	Avointen lähteiden tiedustelu (engl. Open source intelligence)
PSE	Tehospektrientropia (engl. Power spectral entropy)
RF	Radiotaajuus (engl. Radio frequency)
RSSI	Vastaanotetun signaalin voimakkuuden ilmaisin (engl. Received singal strength indicator)
SFS	Taajuusspektri (engl. signal frequency spectrum)
WEE	Aallon energian entropia (engl. Wavelet energy entropy)

1. JOHDANTO

Erilaisten dronejen rooli sodankäynnissä on kasvanut merkittävästi viime vuosien aikana. Dronejen suhteellisen halpa hinta ja erilaisten dronejen tarjoamat laajat käyttötarkoitukset mahdollistavat dronejen käytön niin suurille valtiollisille armeijoille, kuin myös pienille sissiryhmittymille. Droneja voidaan hyödyntää sekä ilmasta tapahtuvaan tiedusteluun että hyökkäämiseen yhdistämällä niihin erilaisia aseita. Dronejen käytön lisääntyessä on kasvanut myös tarve niiden havaitsemiseen, paikantamiseen sekä torjuntaan.

Työn tavoitteena on selvittää onko taistelukentälle realistista kehittää järjestelmää droneuhan torjuntaan henkilötasolla. Tämä selvitetään vertaamalla järjestelmän vaatimuksia ja avoimista lähteistä löytyviä järjestelmiä. Vaatimukset määritellään selvittämällä ensin taistelukentän ja erityisesti henkilötason tuottamat haasteet droneuhan torjunnassa. Tämän jälkeen kirjallisuuden avulla määritellään periaatteet, joiden avulla järjestelmät toimivat. Näitä yhdistämällä arvioidaan avoimista lähteistä löytyneiden järjestelmien soveltuvuutta henkilötason droneuhan torjunnassa.

Työssä dronejen havaitsemista ja paikannusta käsitellään passiivisten radiomenetelmien avulla. Täten työstä rajataan pois muut havaitsemistavat kuten tutkat, akustiset sekä optiset havaitsemismenetelmät. Työstä rajataan pois myös havaitsemis- ja paikannusmenetelmät, jotka pohjautuvat jonkinlaiseen valmistajan asentamaan identifikaatiomenetelmään. Tälläisen aina päällä olevan identifikaatioprotokollan käyttäminen taistelukentällä on epätodennäköistä. Torjunnassa käsitellään häirintää radiomenetelmiin pohjautuvien häirintälähettimien avulla. Täten torjunnasta rajataan ulos kaikki muut kuin radioliikenteeseen pohjautuvat keinot kuten laserit ja kineettinen torjunta.

Sen lisäksi aihetta käsitellään yksittäisen taistelijan näkökulmasta, eli hyödynnettävän laitteiston tulee olla henkilökohtaiseen varustukseen sopivaa esimerkiksi hinnan sekä painon puolesta. Työssä ei myöskään pystytä luonnollisesti käsittelemään droneja, jotka eivät kommunikoi radiosignaalien avulla, kuten autonomiset tai kaapelin avulla ohjattavat dronet.

Dronejen henkilötasolla aiheuttaman uhan torjunnassa on tärkeää huomioida myös, kuinka dronea käytetään henkilötasoa vastaan. On epätodennäköistä, että suurta, korkealla lentävää tiedusteludronea käytettäisiin itsensä räjäyttämällä yksittäistä taistelijaa vastaan. Toisaalta suhteellisen halvat kameralla varustetut dronet aiheuttavat henkilötasolle realis-

tisen uhan pudottamalla taistelijoiden päälle räjähteitä tai lentämällä taistelijaa kohti räjähtäen. Työssä keskitytäänkin tästä syystä erityisesti halpojen, kameraohjattujen dronejen havaitsemiseen ja torjuntaan.

Käytössä olevia ratkaisuja etsittiin avoimista tietolähteistä (OSINT). Erityisesti Telegram ja X (ent. Twitter) osoittautuivat hyviksi lähteiksi yritysten nettisivujen ja käyttöohjeiden ohella. Tarvittavat käännökset tehtiin joko Telegramin omaa käännösohjelmaa käyttäen tai Chrome Web Storesta löytyvää Immersive Translator selainlaajennusta hyödyntämällä.

Työssä luvussa 2 perehdytään dronejen havaitsemisen ja paikannuksen tekniseen perustaan. Luvussa 3 esitellään ja analysoidaan avoimista tietolähteistä löytyneitä järjestelmiä dronejen havaitsemiseen. Luvussa 4 perehdytään dronejen torjunnan taustaan ja esitellään lyhyesti avoimista tietolähteistä löytyneitä järjestelmiä.

2. DRONEN HAVAITSEMINEN JA PAIKANNUS RADIOSIGNAALEJA HYÖDYNTÄEN

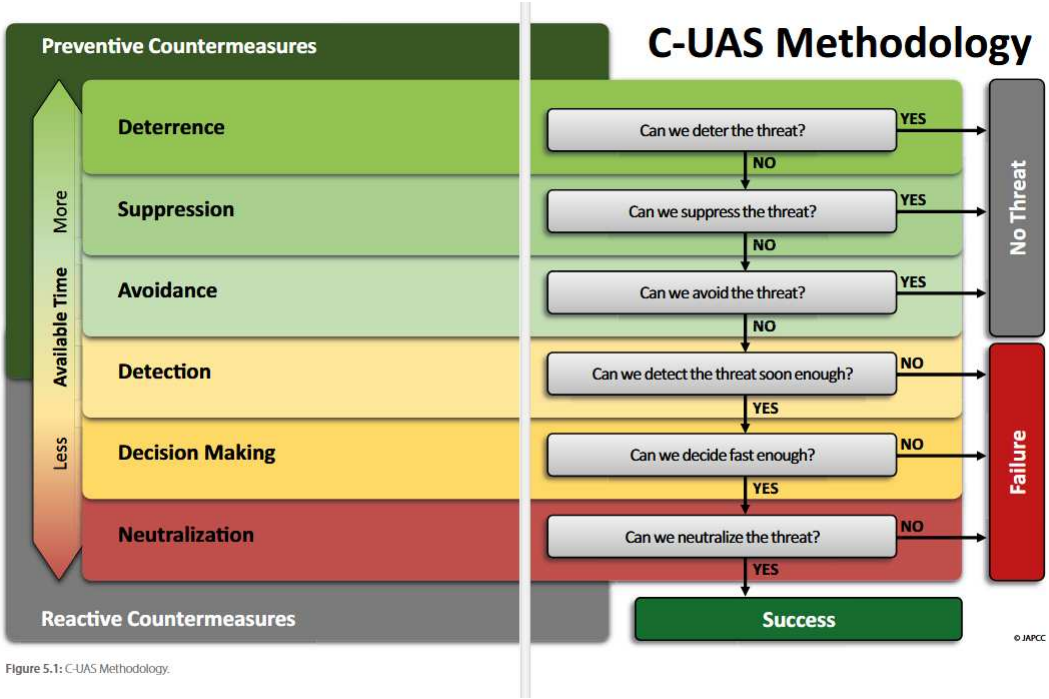
Ensin esitellään dronen torjunnan vaatimuksia henkilötasolla taistelukentän olosuhteissa. Tämän jälkeen dronen havaitsemiseen ja paikannukseen liittyvää tutkimusta tarkastellaan ja analysoidaan niissä esiintyvien menetelmien ominaisuuksia ja käytettävyyttä peilaten aiemmin esiteltyihin vaatimuksiin. Torjunta esitellään luvussa 4, ja myös sitä analysoidaan käyttämällä pohjana tässä luvussa esiteltyjä henkilötason ja taistelukentän luomia vaatimuksia.

2.1 Vaatimukset henkilötasolla ja taistelukentällä

Dronejen taistelukentällä aiheuttaman uhan vastatoimet voidaan jakaa karkeasti kahteen erilliseen osaan eli ennakoiviin vastatoimiin (*engl. preventive countermeasures*) ja reaktiivisiin vastatoimiin (*engl. reactive countermeasures*), jotka on esitelty kuvassa 2.1. Tämän työn kannalta ennakoivat vastatoimet eli pelotevaikutus (*engl. deterrence*), tukahduttaminen (*engl. suppression*) ja väistäminen (*engl. avoidance*) eivät ole merkityksellisiä. Työssä keskitytään reaktiivisiin vastatoimiin eli havaitsemiseen (*engl. detection*), päätöksentekoon (*engl. decision making*) ja neutralisointiin (*engl. neutralization*).

Kuvasta 2.1 voimme havaita, että reaktiivisten vastatoimien tapauksessa käytettävissä olevaa aikaa on vähän ja minkä tahansa vaiheen epäonnistuminen tarkoittaa vastatoimien epäonnistumista. Mikäli dronea ei kyetä havaitsemaan, päätöstä ei kyetä tekemään tai torjuntaa aloittamaan riittävän nopeasti, drone kykenee vaikuttamaan ilman vastatoimia. Dronejen torjunnan kannalta aika onkin hyvin kriittinen elementti ja tämä tulee erityisen selkeästi esille niin kutsutun toimintaketjun (*engl. kill chain/processing chain*) tapauksessa

Toimintaketjussa eri toiminnan vaiheet suoritetaan ketjussa vaihe kerrallaan ja yksittäisen vaiheen keskeytyminen johtaa koko toiminnan keskeytymiseen. Erilaisia toimintaketjuja on useita kuten esimerkiksi Yhdysvalloissa ilmavoimien käytössä ollut F2T2EA [7] tai siitä kehitetty F5 [28]. Menemättä tarkemmin erilaisten toimintaketjujen etuihin ja haittoihin, tässä työssä käytettäväksi sopii Yhdysvaltain sisäisen turvallisuuden ministeriön esittelemä [46], kuvassa 2.2 näkyvä toimintaketju. Kyseinen toimintaketju kuvastaa hyvin kaikki askeleet, jotka dronen onnistunut torjunta vaatii.



Kuva 2.1. *Dronejen aiheuttaman uhan vastatoimet [7]*

Kuva 2.2. *Toimintaketju dronen torjunnassa [46]*

Kuvan 2.2 toimintaketju etenee kohteen havaitsemisen (*engl. Find*), kohteen määrityksen (*engl. Fix*) ja kohteen seuraamisen (*engl. Track*) kautta uhkaan vaikuttamiseen, joka käsittää dronen aiheuttaman uhan lieventämisen (*engl. Mitigate*) ja dronen tuhoamisen (*engl. Defeat*). Toimivaan toimintaketjuun kuuluu myös vaikutuksen arviointi ja tarvittaessa uuden toimintaketjun aloitus kohteelle mikäli haluttua vaikutusta ei olla saavutettu. Toimintaketjun ollessa käynnissä on hyvin mahdollista, että myös drone on havainnut torjuntaa yrittävän osapuolen ja sen vuoksi aika on erittäin kriittinen elementti taistelukentän tapauksessa. Uhan aiheuttavalla dronella on käynnissä todennäköisesti hyvin samantyyppinen toimintaketju, jonka katkaisuun tai vähintäänkin viivyttämiseen dronen torjunnassa on pyrittävä. Dronen torjunnassa hyödynnettävissä järjestelmissä onkin huomioitava käytettävyyden nopeus ja niiden on mahdollistettava nopea päätöksenteko ja droneen vaikuttaminen ollakseen hyödyllisiä. Käytännössä tämä tarkoittaa esimerkiksi sitä, ettei havaitsemiseen tai torjuntaan käytettävä järjestelmä voi olla esimerkiksi repussa kannettava, vaan sen tulee olla käytettävissä niin nopeasti kuin mahdollista.

Kaupalliset drone toimivat yleensä ISM-taajuusalueilla 2400,000-2483,500 MHz tai 5725,000–5875,000 MHz, joilla toimii myös monia muita laitteita, kuten Wi-Fi tai Bluetooth tekniikoita käyttävät laitteet. Suuri määrä erilaisia laitteita samoilla taajuusalueilla voi tietyissä olo-

suhteissa tuottaa paljon häiriötä, joka vaikeuttaa dronen havaitsemista. [19] Suurin osa kaupallisista laitteista käyttää 2400,000–2483,500MHz taajuusaluetta dronen ohjausyhteyteen ja joko samaa 2400,000–2483,500 MHz taajuusaluetta tai 5725,000–5875,000 MHz taajuusaluetta hyötykuorman eli esimerkiksi kameran ja ohjaajan väliseen kommunikointiin [20].

Taistelukentän olosuhteissa dronen havaitsemisessa tulee ottaa huomioon taajusalueiden laajempi käyttö. Taistelukentällä käydään jatkuvaa kilpailua muun muassa juuri uusien taajuuksien käytössä, jotta havaitsemista ja häirintää kyettäisiin välttämään. Viitteitä onkin siihen, että esimerkiksi Venäjän FPV-dronet voivat operoida esimerkiksi 422–476 MHz taajuuksilla [21], jolloin pelkkien ISM-taajuuksien tarkastelulla ja häirinnällä ei kyetä saamaan droneuhkaan minkäänlaista vaikutusta.

Taistelukentällä käytettävät FPV-dronet eivät myöskään välttämättä lähetä mitään telemetriatietoja ohjaajalleen, vaan niitä ohjataan puhtaasti videosignaalin avulla [22]. Tämä tarkoittaa sitä, että dronen havaitakseen, järjestelmän on kyettävä havaitsemaan FPV-dronen lähettämä videosignaali. Toisaalta se tarkoittaa myös, että FPV-dronejen ja jatkuvaa videokuvaa lähettämättömien dronejen havaitsemiseen käytettyjen järjestelmien tulee havainnoida eri taajuusalueita.

Laboratorio-olosuhteiden ulkopuolella dronen havaitsemiseen ja paikannukseen käytettävää järjestelmää suunnitellessa tulee ottaa huomioon myös taistelukentän olosuhteet ja yksittäisen taistelijan tarpeet. Modernilla taistelukentällä taistelijan kantama kokonaiskuorma vaihtelee 25-65 kg välillä [32]. Tästä johtuen järjestelmän paino tulee miminoida eikä useiden kilojen painoinen järjestelmä ole realistinen henkilötasolla käytettäväksi. Järjestelmien painoa voidaan vähentää esimerkiksi energiankulutusta vähentämällä, koska suuri osa järjestelmien painosta tulee niiden vaatimien akkujen painosta.

Järjestelmien tulee lisäksi kestää taistelukentän olosuhteita. Laitteen tulee kestää pölyä sekä vähintään satavaa vettä ja roiskeita, mutta mielellään myös veteen uppoamista. Lisäksi laitteen täytyy kestää myös iskuja, paineaaltoja sekä lämpötilanvaihtelua ollakseen taistelukentällä käytettävissä. Esimerkiksi kotelointiluokka (IP) (*engl. Ingress Protection*) on yksi standardi, jolla voidaan määritellä laitteen olosuhteiden kestävyys [27].

Järjestelmää suunniteltaessa tulee ottaa huomioon myös järjestelmän hinta sekä saatavuus. Vaikka yksittäisen järjestelmän hinta ei vaikuttaisi kovin suurelta, jokaiselle taistelijalle annettavan järjestelmän kappalehinnan noustessa kokonaiskustannukset nousevat nopeasti. Lisäksi saatavuuden kannalta pitää ottaa huomioon se, mitä kyetään valmistamaan paikallisesti ja mistä olisi mahdollisesti saatavuuspulaa konfliktitilanteessa. Nämä rajoitteet muovaavat järjestelmän vaatimuksia varsin olennaisesti.

Lisäksi taistelukenttä on jatkuvassa muutoksessa, mikä luo omat haasteensa järjestemän kehitykselle. Ukrainan sodassa on viitteitä hyvin lyhyelle, jopa viikkojen, eliniälle käytetyis-

sä menetelmissä [23]. Tästä johtuen järjestelmän tulee olla muokattavissa sopeutumaan jatkuviin muutoksiin vastapuolen käyttämissä menetelmissä.

2.2 Dronen havaitseminen

Kirjallisuudessa esitellyt havaitsemismenetelmät voidaan jakaa karkeasti kahteen erilaiseen toteutustapaan. Kirjallisuudessa [19, 35] siepatusta signaalista eritellään ominaisuuksia, joilla luodaan signaalille niin kutsuttu sormenjälki (engl. fingerprint). Sormenjäljestä voidaan tunnistaa, onko kyseessä drone ja mahdollisesti voidaan selvittää myös dronen tyyppi. Kirjallisuudessa [42] esitellään toinen tapa dronen havaitsemiseen, mikä pohjautuu dronen ja ohjaajan välisen Wi-Fi- pakettiliikenteen analysointiin. Pakettiliikenteen analysoinnilla voidaan dronen tyypin identifioinnin lisäksi päätellä sen status eli onko drone maassa vai lentääkö se.

Radiosignaalin sormenjälkeen perustuva dronen havaitseminen etenee tyypillisesti siten, että ensin siepataan signaali radiovastaanotinta käyttäen [37]. Radiosignaalin kaappamiseen voidaan käyttää laitteina oskilloskoopia, spektrianalysaattoria tai ohjelmistoradioa. [20]. Ohjelmistoradiot ovat hyvin muokattavia alustoja, joilla kyetään toteuttamaan monia eri toiminnallisuuksia kytkentöjä muuttamatta [29]. Ohjelmistoradion pieni koko, monipuolisuus ja suhteellisen halpa hinta tekevätkin siitä potentiaalisen alustan myös dronejen henkilötasolla tapahtuvaan dronejen havaitsemiseen.

Kaapatusta signaalista täytyy seuraavaksi erotella ominaisuudet, joiden avulla tehdään päätös siitä, tuleeko signaali dronesta vai ei. Usein yhden ominaisuuden hyödyntämisen sijasta signaalista eristetään useita eri ominaisuuksia ja luodaan näitä analysoimalla signaalille uniikki sormenjälki.

Kirjallisuudessa [19] 15 ominaisuuden joukosta karsitaan kolme tilastollisesti hyödyllisintä ominaisuutta, joita sitten hyödynnetään koneoppimismallin opettamiseen. Kyseisen koneoppimismallin avulla kyetään siten identifioimaan dronen tyyppi. Hyödyllisimpänä valitut kolme ominaisuutta havaittiin olevan muototekijä (*engl. shape factor*), huipukkuus (*engl. kurtosis*) ja varianssi(*engl. variance*). Muototekijä kertoo signaalin muodosta ja se lasketaan signaalin datapisteiden neliöllisen keskiarvon ja datapisteiden itseisarvojen keskiarvon suhteena. Huipukkuus kertoo kuinka voimakkaasti tutkitun signaalin äärimmäiset reuna-arvot (*engl. tails*) poikkeavat normaalijakauman äärimmäisistä reuna-arvoista. Huipukkuus lasketaan kaavalla 2.1

$$k = \frac{\sum_{i=1}^{N}(x_i - \bar{x})^4}{(N-1)\sigma_T^4}, \tag{2.1}$$

missä x_i on yksittäinen datapiste, $\bar{x}$ on datapisteiden keskiarvo, N on datapisteiden kokonaismäärä ja σ datapisteiden keskihajonta. Varianssi taas kertoo datapisteiden hajonnan

ja se lasketaan kaavalla 2.2

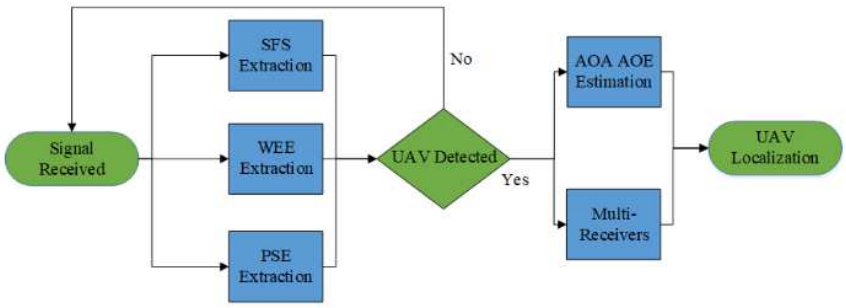
$$\sigma^2 = \frac{1}{N}\sum_{i=1}^{N}(x_i - \mu)^2, \tag{2.2}$$

missä x_i on yksittäinen datapiste, μ on datapisteiden keskiarvo, ja N on datapisteiden kokonaismäärä.

Kirjallisuudessa [35] käytetty yhdistelmä on eristää signaalista taajuusspektri (SFS) (engl. signal frequency spectrum), aallon energian entropia (WEE) (engl. wavelet energy entropy) sekä tehospektrientropia (PSE) (engl. power spectral entropy), joiden avulla tehdään päätelmä onko signaalilähteenä drone vai jokin muu kuvan 2.3 mukaisesti. Taajuusspektriksi muuttaminen mahdollistaa alunperin aikatasossa olevan signaalin tarkastelemisen taajuustasossa, mikä mahdollistaa eri taajuuskomponenttien analysoinnin. Aallon energian entropia on ominaisuus, joka kuvastaa signaalilähteen energian jakautumista. Se voidaan laskea jakamalla signaali pienempiin komponentteihin diskreetin aallokemuunnoksen (DWT) (*engl. Discrete wavelet transform*) avulla, jolloin yksittäisistä komponenteista voidaan laskea niiden energiat, joista muodostetaan todennäköisyysjakauma. Tämän jakauman avulla voidaan laskea Shannonin entropia kaavalla 2.3

$$H = -\sum_{k=1}^{K} P_k \log_2 |P_k|, \tag{2.3}$$

Tehospektrienergian avulla taas voidaan määrittää kuinka teho on jakautunut eri taajuuskomponenttien kesken. Tässä menetelmässä tehon jakautumisesta eri taajuuksille luodaan todennäköisyysjakauma, jota voidaan hyödyntää entropian laskemisessa kaavalla 2.3.



Kuva 2.3. *Esimerkki havaitsemisen ja paikannuksen etenemisestä [35]*

Yhdistämällä kerättyjä ominaisuuksia voidaan luoda droneille uniikki tunniste, niin kutsuttu sormenjälki. Vertaamalla havaitsemisvaiheessa luotua sormenjälkeä tietokannassa oleviin sormenjälkiin voidaan tunnistaa onko signaalilähde dronen ja jos on, mikä dronen tyyppi on. Tämä tietokantaan vertaaminen tehdään kirjallisuudessa usein hyödyntämällä

erinäisiä koneoppimisalgoritmeja, kuten satunnaismetsä-algoritmia (*engl. random forest*) [19, 35]. Satunnaismetsä toimii luomalla useita päätöspuita ja suorittamalla luokittelun näiden päätöspuiden yhdistelmällä [47].

Sormenjälkeen perustuvalla menetelmällä on saatu varsin hyviä tuloksia testiolosuhteissa. Hyödyntämällä useita eri signaalin ominaisuuksia ja koneoppimismenetelmiä on päästy jopa noin 98 % havaitsemistarkkuuteen (*engl. detection accuracy*) noin 25 sekunnin aikajaksossa [19]. Tulee kuitenkin tiedostaa, että 25 sekuntia on dronejen torjunnassa aivan liian pitkä aika luotettavaan havaintoon ja testiolosuhteet eivät vastaa taistelukentän olosuhteita. Menetelmässä on silti potentiaalia olla toimiva myös taistelukentällä.

Signaalista ominaisuuksien eristäminen ja niiden hyödyntäminen vaatii kuitenkin hyvät ja luotettavat algoritmit, mikä luo oman haasteensa menetelmälle. Tietyt signaalin ominaisuudet voivat myöskin olla toisiinsa liittyviä, mikä voi hankaloittaa niiden keräämistä signaalista. Kyseisen ongelman välttämiseksi, koneoppimisalgoritmeilla voitaisiin luokitella ominaisuuksien sijasta raaka signaali sellaisenaan. Tällöin voitaisiin välttää ominaisuuksien keräämisvaihe kokonaisprosessissa. [34]

Käytettäessä radiosignaalin sormenjälkeä havaitsemismenetelmänä, riippumatta siitä analysoidaanko raakasignaalia vai tiettyjä signaalin ominaisuuksia, ongelmaksi muodostuu siepatun signaalin vertaaminen tietokantaan tunnetuista droneista. Esitellyt koneoppimismallit eivät kykene tunnistamaan muunalaisia droneja kuin ne, joita on käytetty mallin opettamiseen. Tähän menetelmään pohjautuva järjestelmä ei siis kykene havaitsemaan uusia dronetyyppejä ilman päivitystä koneoppimismalliin, mikä tulee ottaa huomioon järjestelmää suunniteltaessa.

Drone voidaan havaita ja identifioida myös analysoimalla kaapattua pakettiliikennettä pelkän RF signaalin analysoinnin sijaan. Tällöin pakettien kaappamiseen voidaan hyödyntää esimerkiksi tavallista Wi-Fi vastaanotinta ja paketinkaappausohjelmaa [42]. Menetelmällä kyetään myös havaitsemaan onko drone maassa vai lentääkö se ja minkälaisia ohjausliikkeitä dronella tehdään [42].

Pakettiliikenteen analysoinnilla on saavutettu hyviä tuloksia erityisesti sisätiloissa ja lyhyillä etäisyyksillä ulkotiloissa. 200 metrin etäisyydellä tehdyissä kokeissa pakettihävikin (engl. packet loss) ollessa jo 73.8%, ilmaisutaso (engl. detection rate) pysyy 99.68%:ssa. [42] Menetelmän heikkous on kuitenkin sen riippuvaisuus Wi-Fi protokollalla toimivasta ohjaussignaalista. On äärimmäisen epätodennäköistä, että taistelukentällä käytettäviä droneja ohjattaisiin Wi-Fi protokollan avulla ja näin ollen kyseinen menetelmä on niissä olosuhteissa mitä suurimmalla todennäköisyydellä hyödytön.

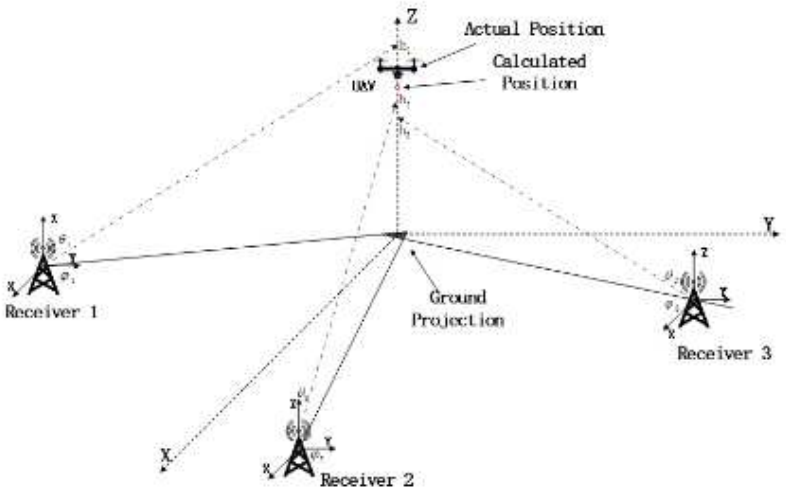
2.3 Dronen paikannus

Dronen signaalin havaitseminen voi olla taistelukentällä jo itsessään arvokas tieto. Havaitsemisen jälkeen oma toiminta voidaan pysäyttää uhan välttämiseksi ja vastatoimia voidaan valmistella. Dronen aiheuttamaan uhkaan vaikuttamiseksi drone täytyy kuitenkin myös paikantaa. Paikannus voidaan sekin toteuttaa useilla menetelmillä, joista todennäköisesti yksinkertaisin ja merkittävin henkilötasolla on silmin tehtävä havaitseminen. Tätä voidaan kuitenkin helpottaa merkittävästi erinäisin radioteknisin menetelmin kuten selvittämällä antenniryhmän ja MUSIC algoritmin avulla signaalin tulosuunta [35] tai hyödyntämällä signaalin vaimenemista ja triangulaatiota [25].

Drone voidaan paikantaa hyödyntämällä useammasta antennista koostuvaa antenniryhmää ja MUSIC (*engl. multiple signal classification*) algoritmia. Tällöin signaali kaapataan usealla eri vastaanottimella ja hyödynnetään signaalin ja kohinan aliavaruuksien (*engl. subspace*) ortogonaalisuutta tulosuunnan selvittämisessä [24]. Tätä ominaisuutta hyödyntämällä voidaan laskea avaruudellisen spektrin (*engl. spatial spectum*) huiput kaavalla 2.4

$$P_{\text{MUSIC}}(\theta) = \frac{1}{\mathbf{a}^*(\theta)\mathbf{E}_N\mathbf{E}_N^*\mathbf{a}(\theta)}, \tag{2.4}$$

joka tuottaa spektriin selvän huipun kulman θ ollessa sama kuin signaalin tulokulma. [24] Tästä voidaan päätellä signaalin tulosuunta. Kyseistä menetelmää voidaan soveltaa myös siten, että selvitetään samaan aikaan sekä atsimuuttikulma (*engl. Angle Of Azimuth (AOA)*) että korotuskulma (*engl. Angle Of Elevation (AOE)*) [35]. Tällöin hyödyntämällä vähintään kolmea vastaanottoaseamaa, kuvassa 2.4 näkyvällä tavalla, voidaan päätellä dronen sijainti varsin tarkasti kolmiulotteisessa avaruudessa.

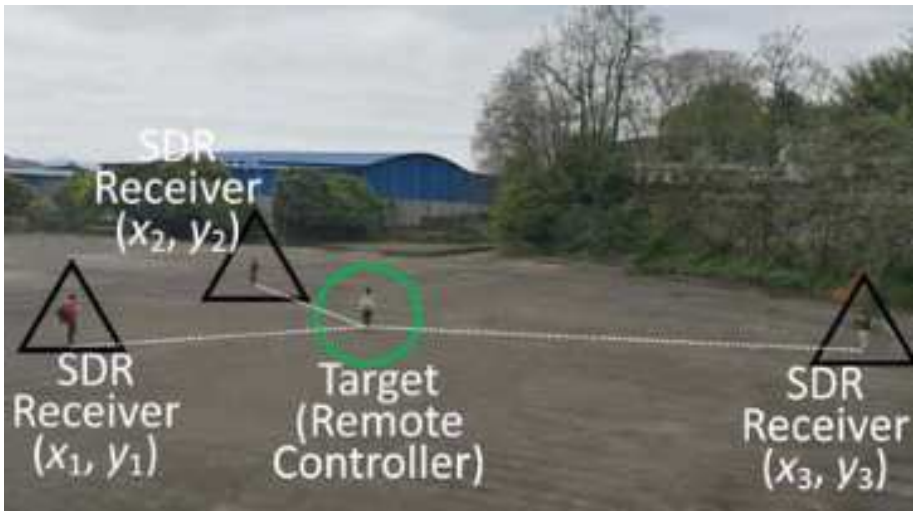


Kuva 2.4. *Esimerkki paikannuksesta kolmiulotteisessa avaruudessa [35]*

Vaikka tarkan sijainnin määrittäminen vaatiikin kolme vastaanottoasemaa, voidaan jo yhdellä asemalla saada tietoon dronen karkea suunta. Henkilötasolla karkea suunta on jo erittäin hyödyllinen informaatio ja sen avulla kyetään tilanteen mukaan väistämään uhkaa tai mahdollisesti vaikuttamaan siihen. Henkilötasolla onkin tärkeää huomioida, että paras tulos saavutetaan usein taistelijan omien aistien ja toiminnan sekä teknisten menetelmien yhteisvaikutuksella.

Toinen esiteltävä mahdollinen tapa paikantaa drone on hyödyntää kirjallisuudessa [25] esiteltyä paikannusmenetelmää, joka pohjautuu trilateraatioon ja vastaanotetun signaalin voimakkuudeen ilmaisimeen (RSSI) (*Received signal strength indicator*). Tässä menetelmässä vastaanottoaseman vastaanotetun signaalin voimakkuuden ilmaisimen ja oletetun vaimennusmallin avulla lasketaan vastaanottimen etäisyys signaalilähteeseen. Laskemalla etäisyydet vähintään kolmelta vastaanottoasemalta, voidaan näiden etäisyyksien ja trilateraation avulla laskea signaalilähteen sijainti.

50 m etäisyydeltä tehdyissä paikannuksissa paikannustarkkuudeksi on saatu noin 2.47 m [25]. Tulokset on kuitenkin saatu kuvan 2.5 mukaisessa testausympäristössä, jossa etäisyydet ovat lyhyitä ja vaimennusmalli voidaan arvioida varsin helposti. Realistissa olosuhteissa etäisyydet ovat pidempiä ja vaimennusmallin arvionti haastavampaa vaihtelevan maaston johdosta. Paikannustarkkuus voi täten huonontua hyvin merkittävästi taistelukentän olosuhteissa. Lisäksi paikallaan olevan dronen ohjaajan sijaan tavoitteena olisi taistelukentällä paikantaa liikkuva drone. Menetelmä vaatii vähintään kolme toisistaan erillään olevaa paikannusasemaa, mikä ei ole yksittäiselle taistelijalle käytännössä mahdollista toteuttaa, vaan vaatisi useamman vastaanottimen välistä kommunikaatiota.



Kuva 2.5. *Esimerkki signaalilähteen paikannuksesta [25]*

3. DRONEN HAVAITSEMINEN JA PAIKANNUS KÄYTÄNNÖSSÄ

Luvussa esitellään ja analysoidaan julksisista lähteistä löytyneitä, dronen havaitsemiseen tarkoitettuja järjestelmiä. Ensin esitellään sormenjälkitekniikkaan pohjautuvat järjestelmät, joista edetään todennäköisesti spektrianalyysiin pohjautuviin järjestelmiin. Viimeiseksi esitellään vielä puhtaasti dronen videosignaalin kaappamiseen pohjautuva järjestelmä.

3.1 Sormenjälkeen pohjautuvat järjestelmät

Dronen havaitsemiseen henkilötasolla voidaan käyttää monia erilaisia järjestelmiä. Järjestelmät vaihtelevat erikoistuneista ja massatuotetuista järjestelmistä yksinkertaisiin kaupan hyllyltä ostettuihin spektrianalysaattoreihin. Signaalin kaappamiseen ja signaalin ominaisuuksista sormenjäljen luontiin perustuvia järjestelmiä ovat esimerkiksi australialaisen DroneShield yrityksen Rfpatrol Mk2 [40], venäläisen 3mx yrityksen Bulat [3], kiinalaisen Skyfend yrityksen Tracer [43], ukrainalaisen Kara Dag yrityksen Obriy [12]. Näiden laitteiden toimintaperiaate vaikuttaa kaikissa pohjautuvan jonkinlaisen tietokannan ylläpitoon, johon kaapatusta signaalista luotua sormenjälkeä verrattaan. Laitteiden suorituskyvyssä, koossa, hinnassa sekä yhdistettävyydessä muihin järjestemiin on kuitenkin suuria eroja.

RfPatrol Mk2 on RF-signaalin havaitsemiseen perustuva järjestelmä [40]. Järjestelmän valmistaja, DroneShield, on onnistuneesti myynyt tuotteitaan muun muassa Yhdysvaltain hallinnolle [36]. DroneShield onkin esitellyistä havaitsemiseen kehitetyistä järjestelmistä ainut, joka on myynyt tuotteitaan NATO-maille. Taulukko 3.1 esittelee RfPatrol Mk2 järjestelmän tärkeimmät ominaisuudet.

RfPatrolMk2-järjestelmän todellisesta kyvykkyydestä ja toimintatavasta on hyvin vähän tietoa saatavilla, mutta sivustolla [40] kuitenkin puhutaan helposti asennettavista päivityksistä joilla laitteen tietokanta pidetään ajantasalla, mikä viittaa tietokantaan, johon laite vertaa kaapattua signaalia. Näistä päätellen laite todennäköisesti sieppaa signaalin, vertaa signaalia koneoppimisalgoritmien avulla tunnettuihin droneihin ja ilmoittaa mikäli havaitsee uhan. Laitteen toiminta onkin todennäköisesti hyvin samankaltaista kuin luvussa 2 esitellyissä havaitsemismenetelmissä. Lisäksi RfPatrolMk2-järjestelmä voidaan

Kuva 3.1. *RfPatrol Mk2 [40]*

Taajuusalueet	Ei tietoa
Kantama	Ei tietoa
Havaitsemisaika	Ei tietoa
Kokonaispaino	1200 g
Mitat (ilman antennia)	228 x 92 x 49 mm
Antennien pituus	Useita vaihtoehtoja
Toiminta-aika yhdellä latauksella	10 h
Hinta	10 000–35 000 $
Käyttölämpötila	-20–67 °C
Kotelointiluokka (IP)	67
Hälytystapa	Kuva, värinä, ääni

Taulukko 3.1. *RfPatrol Mk2-järjestelmän ominaisuudet*

yhdistää DroneShieldin johtamisjärjestelmään (C2) (*engl. Command and Control*), jolloin paikannetusta dronesta saadaan välitettyä tieto eteenpäin tehokkaasti ja tilannekuva on helpompi pitää ajantasalla.

Järjestelmän esittelystä saa käsityksen, että kyseinen järjestelmä on tarkoitettu dronen ja ohjaajan välisen kontrollisignaalin havaitsemiseen. Tämä tekisi järjestelmästä hyödyttömän taistelukentälle suunniteltujen FPV-dronejen havaitsemiseen, mikäli ne eivät lähetä telemetriatietoja ohjaajalleen. Toisaalta on myös mahdollista, että laite kykenee havainnoimaan taajuusalueita, joilla drone lähetää videosignaalia, jolloin FPV-dronejen havaitseminen olisi järjestelmällä mahdollista.

Bulat-järjestelmä on varsin pieni, noin radiopuhelimen kokoinen laite, josta on valmistettu useita eri versioita. Telegramissa jaettavista päivityksistä päätellen käytössä ovat tällä hetkellä versiot Bulat v.3 ja Bulat v.4 [5] [6]. Bulat v.3 on ulkoisesti hyvin samankaltainen kuin Kiinalaisen Al asar yrityksen AAT-DT02-H handheld UAV detector [10] ja BoriStone yrityksen järjestelmä [50], mikä viittaa vähintäänkin epäselvään laitteen alkuperään. Järjestelmän eri versiot vaikuttavat hyvin samankaltaisilta ja tässä työssä käsitelläänkin vain uusinta versiota Bulat v.4. Bulat v.4-järjestelmän tärkeimmät ominaisuudet on esitellään taulukossa 3.2.

Taajuusalueet	300-6200 MHz
Kantama	1,5 km
Havaitsemisaika	Ei tietoa
Kokonaispaino	300 g
Mitat (ilman antennia)	120 x 60 x 34 mm
Antennit	1x 125 mm ja 1x 220 mm
Toiminta-aika yhdellä latauksella	6,5 h
Hinta	88 000 ruplaa
Käyttölämpötila	-20–45 °C
Kotelointiluokka (IP)	Ei tietoa
Hälytystapa	Kuva, värinä, ääni

Taulukko 3.2. *3mx Bulat v.4-järjestelmän ominaisuudet*

Kuva 3.2. *Bulat [3]*

Bulat-järjestelmän toimintatavasta ei ole saatavilla varmaa tietoa, mutta sen toiminta pohjautuu jälleen hyvin todennäköisesti siepatun signaalin ja tunnetuista droneista muodostetun tietokannan vertaamiseen. Jonkinalaiseen tietokantaan viittaa ainakin valmistajan sivuilta löytyvä kappale, jossa he pyytävät lähettämään erilaisia 300-6200MHz taajuusalueella toimivia droneja, jotta ne voidaan lisätä laitteen tietokantaan [3]. Bulat-järjestelmää voidaan käyttää myös spektrianalysaattorina, jolloin se ei automaattisesti hälytä havaituista droneista, eikä pyri tunnistamaan niiden tyyppiä [2].

Bulat-järjestelmän pystyy yhdistämään Tair-rannekelloon Bluetooth Low Energy-teknologian (BLE) avulla, jolloin yhtä Bulat-laitetta voidaan käyttää lähettämään varoitus useaan Tair-kelloon. Tair-kellot kykenevät myös lähettämään tiedon havaitusta dronesta muille Tair-kelloille [4]. Valmistaja takaa Bulat-järjestelmän ja Tair-kellon väliselle kommunikaatiolle 50m kantaman sekä 20m kantaman kellojen väliselle tiedonsiirrolle, olettaen molemmissa tapauksissa näköyhteyden säilyvän. Ideaalitilanteessa laitteiden maksimikommunikaatioetäisyyteen vaikuttavat lähetysteho, antennit sekä signaalin vaimeneminen siirtokanavassa. Lisäksi todellisuudessa maksimietäisyyteen vaikuttavat lisäksi kohina ja häiriöt siirtokanavassa. [49] Tuntematta laitteiden todellista rakennetta ja olosuhteita joissa järjestel-

miä käytetään sekä testaamatta laitteita todellisissa olosuhteissa, niiden todellista maksimikommunikaatioetäisyyttä on haastavaa arvioida luotettavasti. Valmistajan ilmoittamat etäisyydet vaikuttavat kuitenkin mahdollisilta.

Skyfend Tracer järjestelmästä on kahta eri versiota, Tracer P ja Tracer S [15]. Tracer P-järjestelmä kykenee havaitsemaan vain tiettyä tunnistusprotokollaa, kuten DroneID:tä, lähettävät dronet [43]. Tälläisen tunnistussignaalin lähettäminen taistelukentän olosuhteissa on epätodennäköistä, ja työn kannalta kiinnostavampi versio onkin Tracer S. Tracer S kykenee valmistajan mukaan analysoimaan taajuusspektriä ja näin tunnistamaan myös tunnistusprotokollaa käyttämättömät dronet vertaamalla havaittua dronea laitteessa olevaan dronetietokantaan [44]. Taulukko 3.3 esittelee järjestelmän tärkeimmät ominaisuudet.

Kuva 3.3. *Tracer S [44]*

Taajuusalueet	868 MHz/915 MHz/2,4 GHz/5,2 GHz/5,8 GHz
Kantama	2 km
Havaitsemisaika	< 3 s
Kokonaispaino	1000 g
Mitat (ilman antennia)	222 x 85 x 45 mm
Antennit	3x 200 mm
Toiminta-aika yhdellä latauksella	5 h
Hinta	Ei tietoa
Käyttölämpötila	-20–60 °C
Kotelointiluokka (IP)	65
Hälytystapa	Värinä, ääni

Taulukko 3.3. *Tracer S-järjestelmän ominaisuudet*

Lisäksi suunnatulla antennilla Tracer S-järjestelmä kykenee havaitsemaan dronen valmistajan mukaan jopa 5 km päästä. Toisaalta suunnattuja antenneja käytettäessä vain 2,4 GHz taajuudesta ylöspäin olevat taajuudet ovat käytettävissä havaitsemiseen. [44]

Tracer-järjestelmän suurin ulkoinen ero aiemmin esiteltyihin järjestelmiin on se, ettei laitteessa itsessään ole näyttöä. Laite ilmoittaa havaituista droneista joko äänen tai värinän avulla. Vaihtoehtoisesti Tracer-järjestelmät voidaan yhdistää myös Skyfend yrityksen tarjoamaan johtamisjärjestelmään, jolloin useaa laitetta voidaan hyödyntää yhtäaikaisesti.

Obriy-järjestelmä on FPV-dronejen havaitsemiseen tarkoitettu järjestelmä. Obriy on Ukrainalaisen Kara Dag yrityksen tuote. Obriy on FPV-dronejen havaitsemiseen kehitetty järjestelmä, joka toimii yleisimmillä kaupallisten dronejen käyttämillä taajuuksilla. Järjestel-

mä kykenee havaitsemaan vain videosignaalia lähettävät dronet. [12] Tärkeimmmät tiedot järjestelmästä on esitelty taulukossa 3.4.

Kuva 3.4. *Obriy [12]*

Taajuusalueet	1,2 GHz/2,4 GHz/5,2 GHz/5,8 GHz
Kantama	2,5–4 km
Havaitsemisaika	Ei tietoa
Kokonaispaino	Ei tietoa
Mitat (ilman antennia)	n. 170 x 70 x 35 mm
Antennit	3x suunnattu ja 2x suuntaamaton
Toiminta-aika yhdellä latauksella	8 h
Hinta	n. 550 $
Käyttölämpötila	-20–60 °C
Kotelointiluokka (IP)	51 (arvio)
Hälytystapa	Kuva, ääni

Taulukko 3.4. *Obriy-järjestelmän ominaisuudet*

Obriy-järjestelmällä voidaan selvittää myös dronen suunta. Tarkempaa tietoa suunnan selvitystavasta ei ole, mutta esimerkiksi signaalin tulosuunnan selvittäminen luvussa 2 esitellyllä MUSIC-algoritmilla on mahdollinen selvitystapa. Valmistajan tiedoista selviää, että signaalin suunnan selvittäminen vie 15-20 sekuntia, mikä viittaa siihen, että laitteen tulee suorittaa laskuoperaatioita suunnan selvittämiseksi [12]. Lisäksi kyseinen järjestelmä kykenee myös vastaanottamaan ja näyttämään dronen lähettämää videoa näytöllään.

3.2 Spektrianalysaattorit

Ukrainan sodassa käytetään myös vähemmän erikoistuneita laitteita kuten yksinkertaisia spektrianalysaattoreita. Kuvassa 3.5 näkyy väitetysti venäläinen spektrianalysaattori. Kyseinen spektrianalysaattori kykenee ilmeisesti seuraamaan neljällä eri taajuusalueella tapahtuvaa liikennettä saman aikaan ja hälyttää mikäli näillä alueilla tapahtuva tietoliikenne ylittää ennalta määritetyn rajan. Laitteen alkuperästä tai mahdollisesta ohjelmiston uudelleenasennuksesta ei ole varmaa tietoa, mutta laite vaikuttaa olevan muokattu dronekäyttöä varten päätellen sen antamista hälytyksistä.

Myös yksinkertaista, muokkaamatonta spektrianalysaattoria voi käyttää dronejen havaitsemiseen. Tälläinen spektrianalysaattori näyttää tarkastellulta taajuusalueelta vain taajuusspektrin, joten sen tulkitseminen jää laitteen käyttäjän vastuulle. Taistelutilanteessa käyrän tulkitseminen voi olla haastavaa ja vaatii ennalta opeteltuja taitoja ja tietämystä

Kuva 3.5. *Väitetysti venäläinen spektrianalysaattori [41]*

dronejen käyttämästä taajuusalueesta, joten nopeatempoiseen päätöksentekoon taistelukentällä kyseinen ratkaisu ei ole optimaalinen.

Spektrianalysaattoreiden käytettävyys riippuu myös hyvin paljon alueen tietoliikenteen määrästä. Mikäli analysaattoreiden tarkastelemalla taajuusalueella on paljon liikennettä, analysaattoreiden näyttämästä taajuuspektristä on hyvin vaikeaa, ellei peräti mahdotonta päätellä onko lähistöllä drone vai tuleeko signaali jostain muusta, samalla taajuusalueella toimivasta lähteestä. Toisaalta liikuttaessa alueella, jossa ei ole paljoa häiritsevää liikennettä voi spektrianalysaattori olla varsin hyödyllinen laite antamaan ennakkovaroituksen lähistöllä liikkuvasta dronesta.

Suoraan kaupasta ostettujen spektrianalysaattoreiden lisäksi Ukraina käyttää sodassa laitteita kuten Tsukorok [13]. Tsukorok on Drone Spices yrityksen järjestelmä, josta on kaksi eri versiota: Tsukorok ja Vanilla Tsukorok. Tsukorok kykenee valmistajan mukaan havaitsemaan siivellisiä droneja taajuusalueilla 865-885 MHz, 902-928 MHz sekä 970-1020 MHz. Tyypillisiä havaittavia droneja ovat esimerkiksi Venäjän käyttämät, siivelliset Eleron- ja Lancet-dronet. Näiden lisäksi Vanilla Tsukorok kykenee havaitsemaan 2,4 GHz taajuusalueella tapahtuvaa liikennettä eli esimerkiksi DJI Mavic-droneja. 2,4 GHz taajuudella laitteen tehokas kantama on hyvin lyhyt, vain 300-400 m, mikä rajoittaa ominaisuuden hyödyllisyyttä merkittävästi. [18, 45] Tsukorikin tärkeimmät ominaisuudet on esitelty taulukossa 3.5.

Tsukorokin toiminta perustuu ilmeisesti dronen lähettämien telemetriatietojen havaitsemiseen. Tämä voi aiheuttaa haasteita, mikäli samalla taajuudella toimii omia droneja joita ohjataan läheltä Tsukorok-järjestelmää. Tsukorok todennäköisesti havaitsee tällöin oman dronen kontrollisignaalin, eikä vastapuolen dronen lähettämiä telemetriatietoja. Kyseinen ongelma voi helposti aiheuttaa vääriä havaintoja, jotka tekevät järjestelmästä epäluotettavan.

Kuva 3.6. *Tsukorok [18]*

Taajuusalueet	701–1020 MHz
Kantama	8–16 km
Havaitsemisaika	< 5 min
Kokonaispaino	100 g
Mitat (ilman antennia)	100 x 120 x 40 mm
Antennit	2x
Toiminta-aika yhdellä latauksella	15–20 h
Hinta	n. 60 $
Käyttölämpötila	Ei tietoa
Kotelointiluokka (IP)	Suojattu pölyltä, mutta ei tarkempaa tietoa
Hälytystapa	Kuva, ääni

Taulukko 3.5. *Tsukorok-järjestelmän ominaisuudet*

3.3 Analogisen videosignaalin kaappaus

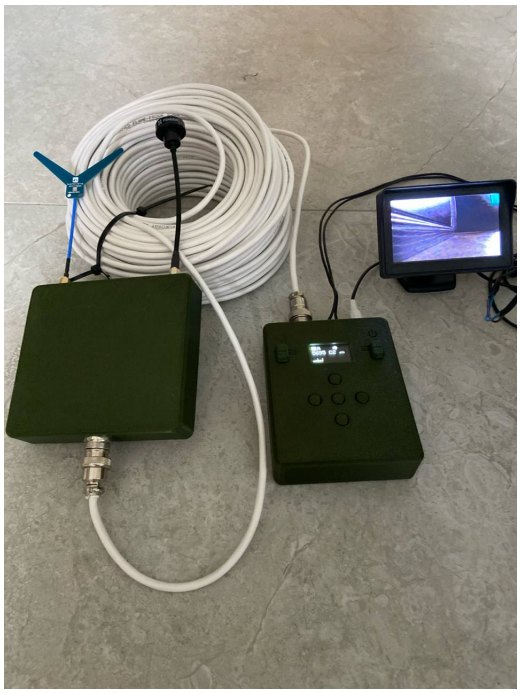
Dzyga-järjestelmä on videosignaalin kaappamiseen pohjautuva järjestelmä. Dzyga toimii 1010-1780 MHz ja 4900-6060 MHz taajusalueilla, joista analogisen videosignaalin havaitessaan laite antaa ilmoituksen pienellä näytöllä taajuudesta ja kanavasta jolla laite on havaittu. Samanaikaisesti isolla näytöllä näkyy dronen lähettämä videosignaali. Laitteessa on myös yksinkertainen salauksenpurku mikäli kaapattu signaali on salattu käännettynä videona (engl. inverted video). Laitteen käyttäjä voi laitteessa olevasta kytkimestä manuaalisesti kytkeä salauksenpurun päälle mikäli video vaikuttaa käännetyltä. Dzyga-järjestelmässä ei vaikuta olevan keinoja monimutkaisempien salausmenetelmien purkuun. [17] Taulukko 3.6 esittelee järjestelmän tärkeimmät ominaisuudet.

Dzyga-järjestelmästä on saatavilla myös versio, jossa vastaanottoyksikkö antenneineen on erillinen kontrolliyksiköstä. Tällöin laitteen käyttäjä voi olla esimerkiksi auton sisällä ja antennit auton katolla. Muuten järjestelmä toimii samalla periaatteella kuin kannettava Dzyga. [33]

Kuva 3.7. Dzyga [16]

Taajuusalueet	701–1020 MHz
Kantama	Ei tietoa
Havaitsemisaika	< 10 s
Kokonaispaino	600 g
Mitat (ilman antennia)	n. 200 x 100 mm
Antennit	2x
Toiminta-aika yhdellä latauksella	Ei tietoa
Hinta	n. 480 $
Käyttölämpötila	Ei tietoa
Kotelointiluokka (IP)	Ei tietoa
Hälytystapa	Kuva, ääni

Taulukko 3.6. *Dzyga-järjestelmän ominaisuudet*



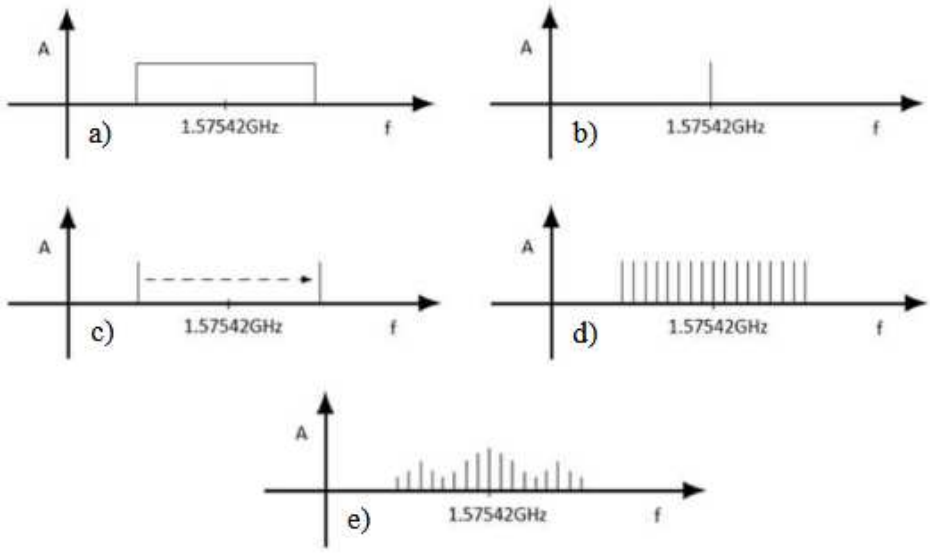
Kuva 3.8. *Kuva Dzyga-järjestelmästä, jossa vastaanottoyksikkö ja kontrolliyksikkö ovat erillisiä [33]*

4. DRONEN TORJUNTA

Luvussa esitellään dronen torjuntaa radiohäirintää käyttäen. Ensin esitellään radiohäirinnän perusperiaatteita ja analysoidaan erilaisten menetelmien käytännöllisyyttä henkilötasolla käytettäväksi. Sen jälkeen esitellään julkisista lähteistä löytyneitä, radiohäirintään pohjautuvia järjestelmiä ja analysoidaan niiden toiminnallisuutta.

4.1 Dronen torjunta radiohäirinnällä

Radiohäirintää voidaan toteuttaa monin eri tavoin. Tämän tutkimuksen tavoitteena ei ole esitellä kaikkia mahdollisia tapoja toteuttaa radiohäirintää vaan käydä läpi dronen häirintään käytännöllisimmät menetelmät. Nämä menetelmät ovat monikanavahäirintä (*engl. barrage jamming*), kapeakaistainen häirintä (*engl. tone jamming*), täsmähäirintä (*engl. smart jamming/protocol-aware jamming*) ja pyyhkäisyhäirintä *engl. sweep jamming*, pulssimuotoinen häirintä (*eng. pulse jamming*) sekä reaktiivinen häirintä (*engl. reactive jamming/follower jamming*). Kuva 4.1 esittelee teoreettisia spektrejä käsiteltäville häirintämenetelmille.



Kuva 4.1. *Teoreettiset spektrit a.) monikanavahäirinnälle, b.) kapeakaistaiselle häirinnälle, c.) pyyhkäisyhäirinnälle, d.) pulssimuotoiselle häirinnälle ja e.) täsmähäirinnälle [39]*

.

Monikanavahäirinnässä häiritään montaa taajuuskanavaa samanaikaisesti. Häirintä voi kohdistua koko taajuusalueseen tai vain osaan siitä. Monikanavahäirinnän toimintaperiaatteena on käytännössä nostaa taustamelun tasoa vastaanottimessa lähettämällä taustamelua muistuttavaa signaalia halutulla taajuusalueella. Monikanavahäirinnän hyvä puoli häirintämenetelmänä on se, ettei se vaadi tarkkaa tietoa häirittävästä signaalista vaan tarkoituksena on estää kommunikaatio koko taajuusalueella. Toisaalta menetelmän huonona puolena on häirintäsignaalin tehon jakautuminen suurelle taajuusaluelle, jolloin halutun vaikutuksen saavuttaminen häirinnässä voi vaatia hyvin suurta lähetystehoa. [38] Lisäksi monikanavahäirintä estää myös oman osapuolen kommunikoinnin häirityllä taajuusalueella, joten häirintämenetelmän käytettävyys voi olla vahingollista myös omalle toiminnalle.

Kapeakaistaisessa häirinnässä voidaan häiritä yhtä tai useampaa taajuutta samanaikaisesti. Yhden taajuuden häirintä voidaan toteuttaa tuottamalla halutulla taajuudella jatkuva aalto ja lähettämällä sitä häirittävälle vastaanottimelle. Haluttaessa häiritä useampaa taajuutta toimintaperiaate on sama, mutta jatkuvia aaltoja tuotetaan kaikille halutuille taajuuksille yhtäaikaisesti. [38] Menetelmän hyvänä puolena on häirintätehon kohdistaminen tietylle taajuudelle, jolloin haluttu vaikutus on mahdollista saavuttaa tilanteessa, jossa häirinnän kohde toimii yhdellä tai useammalla ennalta tiedetyllä taajuudella, eikä kykene hyödyntämään hajaspektritekniikkaa (*engl. spread spectrum technique*). Menetelmä on käytännöllinen esimerkiksi perinteisiä viestijärjestelmiä vastaan [29], mutta erityisesti taajuushyppelyhajaspekti (FHSS) (*engl. frequency-hopping spread spectrum*), jossa käytetty taajuus vaihtelee tietyn mallin mukaisesti tekee kapeakaistaisesta häirinnästä hyödytöntä [38].

Mikäli tiedämme ennalta tiedonsiirtoprotokollan voidaan sitä häiritä täsmähäirinnän avulla. Tässä häirinnän muodossa häirintää toteuttava taho on ennalta kyennyt selvittämään tarvittavat tiedot kohteesta, kuten taajuushyppelyhajaspektrin taajuuksien järjestyksen ja tarkat ajoitukset [48]. Täsmähäirintä eroaa muista esitellyistä häirinnän muodoista myös siten, että kohdetta häiritään kohinan sijaan kohteen omia signaaleja muistuttavilla signaaleilla. Tälläistä signaalia on vaikeaa havaita erityisesti sen toimiessa reagoivana eli häiritään vain oikean lähettimen lähettäessä [29].

Täsmähäirinnällä voidaan saavuttaa muita menetelmiä parempi häirintäteho halutuilla taajuuksilla mikäli kokonaislähetysteho pysyy samana [26]. Menetelmän huonona puolena on kuitenkin se, että kommunikaatioprotokollan ominaisuudet ja ajoitukset tulee tuntea etukäteen, joten häirintälähettimen tulee olla tietoinen dronen tyypistä ja sen kommunikaatioprotokollasta. Esimerkiksi Ukrainalaisen Kvertus yrityksen LTEJ Mirage hyödyntää täsmähäirintää saavuttaakseen valmistajan tietojen mukaan kohinaan perustuvaa häirintää paremman häirintävaikutuksen samalla lähetysteholla [30]. Käytännössä taistelukentällä erityisesti henkilötasolla FPV-dronejen torjunnassa kyseistä menetelmää on kuitenkin haastavaa hyödyntää. FPV-dronejen käyttämät kommunikaatioprotokollat voivat olla

vastapuolen itse kehittämiä ja tällöin on varmempaa pyrkiä häiritsemään niitä kohinalla ja suurella teholla.

Pyyhkäisyhäirinnässä häirintä toteutetaan siten, että taajuutta vaihdetaan tietyin aikavälein ja kanaville kohdistetaan näin häirintää yksi kerrallaan. Pyyhkäisyhäirinnän tulee häiritä yhtä kanavaa riittävän kauan verraten signaalin symboolinopeuteen, jotta häirinnällä saavutetaan haluttu vaikutus. [29] Toisaalta pyyhkäisyn tulee olla niin nopea, että haluttu taajuusalue saadaan käytyä läpi riittävän lyhyessä ajassa. Pyyhkäisyhäirinnässä voidaan myös häiritä useaa kanavaa kerrallaan, mikä pidentää aikaa joka yhden kanavan häirintään voidaan käyttää. Tämän kääntöpuolena taas on sama rajoite kuin monikanavahäirinnässä eli yhden kanavan häirinnän teho laskee mikäli kokonaisteho pysyy samana tehon jakautuessa usealle kanavalle. [38]

Pulssimuotoisessa häirinnässä signaalin pulssia vaihdellaan päälle ja pois. Pulssisuhteella (*engl. duty cycle*) määritetään kuinka paljon ja kuinka usein häirintäsignaalia lähetetään. Pulssimuotoisella häirinnällä voidaan saavuttaa sama häirintäteho kuin monikanavahäirinnässä huomattavasti pienemmällä energiankulutuksella, koska lähetin ei ole päällä kokoajan. [38]

Reaktiivisessa häirinnässä häirintälaite pyrkii paikantamaan mille kanavalle taajuushyppelyä hyödyntävä lähetin vaihtoi ja siten "seuraamaan"signaalia. Tällä tavoin häirintälaite kykenee häiritsemään signaalia taajuushyppelystä huolimatta. Häirintälaite ei kykene täysin reaaliaikaisesti seuraamaan häirittävää lähetintä, mutta teknisesti on mahdollista kyetä paikantamaan oikea kanava riittävän nopeasti häirinnän mahdollistamiseksi. Varsinaisesti häirinnän muotona voisi toimia esimerkiksi aiemmin esitelty kapeakaistainen häirintä. [38]

Sopivan menetelmän valinta riippuu monista asioista kuten kohteesta, häirinnän tavoitteesta ja siitä kuinka paljon halutaan itse tuottaa havaittavaa radioliikennettä. Mikäli kohde on kyetty tunnistamaan, sen tiedonsiirtoprotokolla tunnetaan riittävällä tarkkuudella ja halutaan häiritä vain kyseistä kohdetta, täsmähäirintä on periaatteessa toimiva vaihtoehto häirinnän muodoksi. Parhaimmillaan menetelmällä voidaan saavuttaa hyvin vaikeasti havaittavissa olevaa ja paikannettavaa häirintää, joka on myös hyvin tehokasta ja suhteellisen vähän energiaa kuluttavaa. Toisaalta taistelukentän nopeasti muuttuvissa olosuhteissa ja hyvin lyhyessä aikaikkunassa pelkästään täsmähäirintään pohjautuva järjestelmä ei tarjoa välttämättä riittävää suojaa. Uusien dronejen taistelukentälle tulo ja haasteet esimerkiksi dronen tyypin tunnistamisessa voivat tehdä täsmähäirinnästä hyödyttömän.

Henkilötasolla tapahtuva häirintä on luonteeltaan omasuojahäirintää ja tällöin esimerkiksi laajalla taajuusalueella tapahtuva monikaistahäirintä voisi toimia lyhyen kantaman häirinnässä. Sillä voitaisiin saavuttaa häirinnän taso, jossa dronen kommunikaatio häiriintyisi ja voitaisiin onnistua väistämään kiireellinen uhka sekä saada lisäaikaa muiden torjuntamenetelmien käytölle. Pitkän kantaman häirintään menetelmä ei toimisi häirintätehon

jakautuessa usealle kanavalle, eikä myöskään pitkäkestoiseen häirintään suuren energiankulutuksensa takia. Pyyhkäisyhäirintä sekä pulssimuotoinen häirintä voisivat toimia samassa tarkoituksessa, mutta hieman pienemmällä energiankulutuksella.

4.2 Torjunta käytännössä

Henkilötason järjestelmälle kriittisiä ominaisuuksia, kuten alhainen paino, täyttäviä järjestelmiä ei löydy julkisista lähteistä. Tässä alaluvussa esitelläänkin järjestelmiä, jotka ovat edes lähelllä käytettävyyttä henkilötasolla. Lisäksi luvussa analysoidaan järjestelmien toiminnallisuutta ja sitä miksi ne eivät sovella käytettäväksi henkilötason järjestelmänä. Esiteltäviä järjestelmiä ovat Droneshield DroneGun Mk4 [14], NT Service EDM4S [11], Kvertus AD Counter FPV Backpack [31] ja lisäksi eräs tunnistamaton järjestelmä [1].

DroneGun Mk4 on suuren pistoolin kokoinen, yhdellä kädellä käytettävä järjestelmä dronejen torjuntaan. Järjestelmän taajuuksista mainitaan, että se toimii ISM-taajuuksilla sekä GNSS-taajuuksilla. [14] Järjestelmällä kyetään siis vaikuttamaan ainakin kaupallisiin droneihin, jotka hyödyntävät näitä taajuuksia. Järjestelmän häirintään käyttämästä tavasta ei löydy mitään tietoja, joten sitä on mahdotonta arvioida luotettavasti. Järjestelmä on IP67 suojattu [14] eli se on pölytiivis ja kestää hetkellisen upotuksen veteen [27]. Taulukko 4.1 esittelee järjestelmän keskeiset ominaisuudet.

Kuva 4.2. *DroneGun Mk4 [14]*

Taajuusalueet	ISM- ja GNSS-taajuuksia
Kantama	Ei tietoa
Käynnistysaika	< 3 s
Kokonaispaino	3200 g
Mitat	n. 500 x 300 mm
Toiminta-aika yhdellä latauksella	1 h
Hinta	Ei tietoa $
Käyttölämpötila	-20–55 °C
Kotelointiluokka (IP)	67

Taulukko 4.1. *DroneGun Mk4-järjestelmän ominaisuudet*

DroneGun Mk4 on henkilötasolle käytettäväksi liian painava 3,2 kilogramman painoisena. Jokaiselle taistelijalle ei voida realistisesti lisätä noin suurta painoa kannettavaksi. Tämän lisäksi järjestelmä on käytännössä erillinen ase, jonka käyttöönotto vie ylimääräistä aikaa ja vaatii käyttäjältä kahden eri aseen välillä vaihtelemista.

Toinen järjestelmä dronejen torjuntaan on EDM4S, jota markkinoidaan myös nimellä Skywi-

per. Kyseinen järjestelmä on kahdella kädellä käytettävä, kivääriä muistuttava laite, joka kykenee häiritsemään valmistajan mukaan ISM- sekä GNSS-taajuuksilla sekä lisäksi muita, käyttäjän valitsemia taajuusalueita. [11] Järjestelmää on väitetysti käytetty onnistuneesti Ukrainassa tuhoamaan Eleron-3 drone [9] ja sen kappalehinnan on vuonna 2022 ilmoitettu olevan noin 15000 euroa [8]. Taulukko 4.2 esittelee järjestelmän tärkeimmät ominaisuudet.

Kuva 4.3. *ED4MS [11]*

Taajuusalueet	433 MHz/900 MHz/2,4 GHz/5,8 GHz/GNSS
Kantama	3-5 km
Käynnistysaika	Ei tietoa
Kokonaispaino	5,5 kg
Mitat	1050 x 220 x 360 mm
Toiminta-aika yhdellä latauksella	Ei tietoa
Hinta	n. 15 000 € $
Käyttölämpötila	Ei tietoa
Kotelointiluokka	MIL STD 810G

Taulukko 4.2. *EDM4S-järjestelmän ominaisuudet*

EDM4S on henkilötasolla käytettäväksi liian painava 5,5 kilogramman painoisena [11], ja se on liian kallis jokaiselle taistelijalle annettavaksi. Järjestelmää on kuitenkin julkisten lähteiden mukaan käytetty onnistuneesti dronejen torjuntaan taistelukentällä [9].

Häirintälähettimen voi sijoittaa myös reppuun kuten Kvertus on tehnyt AD Counter FPV Backpackin tapauksessa. Tällöin saadaan painavat akut ja häirintälähettimet kannettua selässä käsien sijasta. Henkilötason torjuntaan kokonainen kannettava reppu ei kuitenkaan ole realistinen, koska esimerkiksi kyseinen reppu painaa n. 9 kilogrammaa. Lisäksi repun tehokas kantama on valmistajan ilmoituksen mukaan maksimissaan vain 150m, joten kyseisellä järjestelmällä voitaisiin realistisesti suojata ryhmän kokoista osastoa. [31] Todennäköisesti kyseinen järjestelmä on suunniteltu siten, että häirintää toteutetaan mahdollisimman tasaisesti kaikkiin suuntiin mikä heikentää kantaman todella lyhyeksi. Taulukko 4.3 esittelee järjestelmän tärkeimmät ominaisuudet.

Näiden järjestelmien lisäksi julkisista lähteistä löytyy joitakin tunnistamattomia laitteita. Eräs niistä on esimerkiksi kuvassa 4.5 näkyvä häirintälähetin. Lähetin koostuu suuntaavista antenneista sekä kiväärin kylkeen kiinnistetystä osasta, joka todennäköisesti sisältää itse häirintälähettimen sekä laitteen akun. Käyttäjän puoleisessa päädyssä taas on virtapainike, jolla laite käynnistetään. Kyseinen lähetin on kiinnitetty rynnäkkökiväärin kylkeen ja näin ollen suuntaaminen tapahtuu rynnäkkökiväärillä tähtäämällä. Tämä nopeuttaa järjestelmän käyttöönottoa ja tekee siitä helppoa käyttäjälle. Huonona puolena kui-

Kuva 4.4. *AD Counter FPV backback[31]*

Taajuusalueet	130–1350 MHz
Kantama	150 m
Käynnistysaika	< 30 s
Kokonaispaino	9 kg
Mitat	500 x 300 x 200 mm
Toiminta-aika yhdellä latauksella	2 h
Hinta	Ei tietoa
Käyttölämpötila	Ei tietoa
Kotelointiluokka	Ei tietoa

Taulukko 4.3. *AD Counter FPV backback-järjestelmän ominaisuudet*

tenkin on, että järjestelmän paino on todennäköisesti useita kiloja ja se on täysin yhdellä puolella kivääriä. Tämä tekisi kiväärin käyttämisestä mitä suurimalla todennäköisyydellä hyvin haastavaa. Kuvassa 4.6 on myös samankaltainen häirintälähetin kiinnitettynä kypärään. Kypärään kiinnittämisessä myös etuna järjestelmän nopea käyttöönottovalmius, mutta pitkäaikaisessa käytössä järjestelmä ei ole toispuoleisena realistinen ergonomisista syistä.

Kuva 4.5. *Tunnistamaton dronen häirintälähetin kiväärin kylkeen kiinnitettynä [1]*

Kuva 4.6. *Tunnistamaton dronen häirintälähetin kypärään kiinnitettynä [1]*

Kokonaisuudessaan julkisista lähteistä löytyneet henkilötasoon parhaiten sopivat lähettimet eivät tarjoa valmista ratkaisua henkilötason torjunnassa käytettäväksi. Kaikki löy-

tyneet järjestelmät ovatkin henkilötasolla jokaisen taistelijan kannettavaksi liian painavia, suurikokoisia ja liian hitaita ottaa käyttöön. Jotta henkilötason järjestelmä olisi hyödyllinen, tulisi sillä kyetä häiritsemään erityisesti räjähteillä varustettuja FPV-droneja, jotka aiheuttavat välittömän uhan yksittäiselle taistelijalle. Usein nämä dronet kuitenkin käyttävät varsin matalia taajuksia, mikä aiheuttaa haasteita antennien suunnitteluun. Lisäksi vaadittavan tehon aiheuttama suuri energiankulutus, ja tästä johtuva isojen akkujen paino aiheuttaa vaikeasti ratkaistavan haasteen henkilötason järjestelmän suunnitteluun.

Vaikuttaa siltä, ettei nykyisillä menetelmillä voida saavuttaa tehokasta häirintävaikutusta henkilötasolla. Monet tässä työssä esitellyistä järjestelmistä voisivat kuitenkin toimia ryhmätason järjestelmänä, mikäli esimerkiksi yhden taistelijan kantoon annetaan dronen häirintään suunnattu reppu, tai jonkun taistelijan pääase korvataan dronea vastaan tarkoitetulla häirintälaitteella. Tällöin ryhmällä olisi jonkinasteinen kyky vaikuttaa droneen ja henkilötasolla tehtäväksi jäisi pyrkiä väistämään uhkaa niin kauan, että ryhmätason järjestelmällä saataisiin haluttu vaikutus aikaan.

5. YHTEENVETO

Työssä esiteltiin sekä teknisten menetelmien perusperiaatteiden että henkilötason ja taistelukentän luomia vaatimuksia dronejen havaitsemiseen ja torjuntaan. Näiden vaatimusten pohjalta analysoitiin nykyisten järjestelmien kyvykkyyksiä ja niihin peilaten pohdittiin mahdollisuuksia kehittää taistelukentän droneuhan torjuntaa henkilötasolla.

Työssä havaittiin, että droneuhan torjunnassa aika on eräs kriittisimmistä, ellei peräti kaikkein kriittisin muuttuja. Etäisyydestä, jolta pienen, itsensä räjäyttävän dronen voi havaita, aikaa uhan realisoitumiseen on hyvin vähän. Tästä johtuen kaikkien henkilötason droneuhan vastajärjestelmien tulee olla nopeasti käyttöönotettavissa ja niiden tulee kyetä nopeaan havaitsemiseen. Järjestelmien tulee ajan puutteen vuoksi olla myös autonomisia siinä suhteessa, ettei havaitseminen vaadi käyttäjältä toimenpiteitä. Muita kriittisiä vaatimuksia ovat esimerkiksi suhteellisen laaja taajuusalue, jolla droneuhka kyetään havaitsemaan ja siihen kyetään vaikuttamaan sekä mahdollisimman pieni järjestelmän koko ja paino.

Kirjallisuutta ja avoimia lähteitä vertaamalla havaittiin, että kauko-ohjattujen dronejen havaitsemiseen on realistista toteuttaa varsin toimivia järjestelmiä henkilötasolla. Useita eri periaatteilla toimivia järjestelmiä on jo käytössä esimerkiksi Ukrainan sodassa ja niiden kehitys vaikuttaa olevan molemmille osapuolille varsin tärkeää. Yksikään löydetty järjestelmä ei kuitenkaan ole täydellinen ja esimerkiksi hinta vaikuttaa olevan monissa järjestelmissä toistaiseksi liian korkea jokaiselle taistelijalle jaettavaksi. Myös dronejen nopea kehitys tuottaa haasteita erityisesti osapuolten itse kehittämien dronejen tapauksessa, koska monet havaitsemisemenetelmät vaativat ennakkotietämystä havaittavasta uhasta. Vaikuttaa kuitenkin siltä, että havaitseminen henkilötasolla on realistista ja siihen kyetään luomaan uskottavia järjestelmiä.

Paikannus henkilötasolla on hieman havaitsemista haastavampi osa-alue. Työssä havaittiin, että tarkkaa paikannusta on henkilötasolla monimutkaista tehdä, koska tämä vaatisi useita, toisistaan erillisiä havaitsemisasemia. Toisaalta olisi mahdollista lähettää henkilötason järjestelmien keräämä data yhteiselle palvelimelle, joka näiden tietojen avulla laskisi dronen tarkan sijainnin. Tällöin haasteena olisi kuitenkin se, että tarkan paikannuksen saavuttamiseksi yksittäisten havaitsemisjärjestelmien tulisi lähettää myös tarkka aika ja oma sijaintinsa palvelimelle. Menetelmiä voidaan kuitenkin hyödyntää karkean suunnan selvittämiseen myös henkilötasolla, mitä voitaisiin hyödyntää apuvälineenä dronen pai-

kannukseen. Tällöin tarkka paikannus tehtäisiin taistelijan omilla aisteilla, mutta radiomenetelmiin pohjautuvaa järjestelmää käytettäisiin avustamaan näitä aisteja.

Työssä havaittiin myös, että dronejen torjunta henkilötasolla radiomenetelmin on ainakin toistaiseksi osoittautunut epärealistiseksi. Torjunnan vaatima teho aiheuttaa sen, että energiankulutus kasvaa liian suureksi henkilötasolla kannettavalla järjestelmälle. Tämä aiheuttaa sen, että järjestelmän koko ja paino kasvavat liian suureksi. Jokaisen taistelijan kannettavaksi ei yksinkertaisesti voida lisätä useiden kilogrammojen painoista, kahdella kädellä kannettavaa erillistä asetta. Toisaalta työssä löytyneistä järjestelmistä moni sopisi esimerkiksi ryhmätasolla käytettäväksi, jolloin voitaisiin saada hieman suuremmalle yksikölle realistinen vaikutuskyky. Vaikuttaakin siltä, että henkilötasolla tulee keskittyä uhan väistämiseen ja pyrkiä sitomaan uhka niin pitkäksi aikaa, että esimerkiksi ryhmäkohtaisella järjestelmällä kyetään vaikuttamaan uhkaan.

On tärkeää tiedostaa että henkilötason dronejen vastaiset toimet radiomenetelmillä liittyvät aina suurempaan kokonaisuuteen. Dronejen, kuten monien muidenkin asejärjestelmien, uhkaa onkin hyvin vaikeaa, ellei mahdotonta, poistaa kokonaisuudessaan. Uhan torjuntaan ei ole olemassa yhtä toimivaa järjestelmää, joka ratkaisisi kaikki ongelmat nyt ja tulevaisuudessa. Dronejen aiheuttama uhka on myös jatkuvassa muutoksessa sekä tekniikan että taktiikan osalta, mikä tulee ottaa huomioon niin kokonaisuudessa kuin myös henkilötason järjestelmää suunniteltaessa. Erilaisten teknisten ratkaisujen ja niihin soveltuvien taistelutapojen avulla sekä näiden hyvällä koulutuksella dronejen aiheuttamaa uhkaa voidaan kuitenkin lieventää nyt ja tulevaisuudessa.

Työssä on pyritty keskittymään kokonaisuuteen esittelemällä menetelmät ja olemassa olevat järjestelmät varsin lyhyesti. Työtä voisikin jatkaa tutkimalla molempia kokonaisvaltaisemmin. Mielenkiintoista olisi myös rakentaa taistelukentälle tarkoitettu henkilötason järjestelmä. Tälläisellä järjestelmällä voisi saada hyvän käsityksen siitä mihin nykytekniikalla kyetään. Toisaalta työn pohjalta voisi jatkaa tutkimusta myös vähemmän teknisestä näkökulmasta ja testata minkälainen vaikutus esimerkiksi taisteluharjoituksessa henkilötason järjestelmillä on.

LÄHTEET

[1] The Dead District [@TheDeadDistrict]. en. Kesäkuu 2024. URL: https://x.com/TheDeadDistrict/status/1796811821023735987 (viitattu 03. 12. 2024).

[2] 3mx. *Bulat manual*. URL: https://docs.3mx.ru/detektor-bpla-bulat-v4/user-manual.

[3] 3mx. *Bulat v.4*. URL: https://3mx.ru/products/detektor-bpla-bulat-v4 (viitattu 29. 10. 2024).

[4] 3mx. *Tair*. Syyskuu 2024. URL: https://www.youtube.com/watch?v=qvZDxBnlLCA (viitattu 29. 10. 2024).

[5] 3mx.ru. *Bulat v.3 firmware update 4.8*. Russian. Lokakuu 2024. URL: https://t.me/ru3mx/235.

[6] 3mx.ru. *Bulat v.4 firmware update 1.60*. Russian. Lokakuu 2024. URL: https://t.me/ru3mx/234.

[7] *A Comprehensive Approach to Countering Unmanned Aircraft Systems - Joint Air Power Competence Centre*. en-US. Tammikuu 2021. URL: https://www.japcc.org/books/a-comprehensive-approach-to-countering-unmanned-aircraft-systems/ (viitattu 06. 12. 2024).

[8] Andrius Tapinas [@AndriusTapinas]. en. Kesäkuu 2022. URL: https://x.com/AndriusTapinas/status/1536342733987516418 (viitattu 04. 12. 2024).

[9] Arslon Xudosi [@Arslon_Xudosi]. en. Lokakuu 2022. URL: https://x.com/Arslon_Xudosi/status/1576878212000649219 (viitattu 04. 12. 2024).

[10] *China Customized Handheld Drone Detection Suppliers, Manufacturers, Factory - Wholesale Discount - AL ASAR TECH*. en. URL: https://www.alasartech-security.com/drone-detection/protable-drone-detection/drone-detection-technology.html (viitattu 29. 10. 2024).

[11] *COUNTER UAV SOLUTIONS – NT Service*. en-US. URL: https://ntservice.eu/products/defense-solutions/counter-uav-solutions/ (viitattu 04. 12. 2024).

[12] KARA DAG. *Obriy Drone Detectors - KARA DAG*. en-US. Marraskuu 2023. URL: https://karadagtech.com/en/obriy-drone-detectors/ (viitattu 08. 11. 2024).

[13] Fabrice Deprez. *Ukraine's Pocket-Sized Answer to Russian Drones*. en-US. Marraskuu 2024. URL: https://foreignpolicy.com/2024/08/05/ukraine-russia-war-drone-detectors-jamming-tsukorok/ (viitattu 07. 11. 2024).

[14] *DroneGun Mk4: Counterdrone (C-UAS) Protection*. en-US. URL: https://www.droneshield.com/c-uas-products/dronegun-mk4 (viitattu 03. 12. 2024).

[15] Droneshop. *Buy Skyfend Tracer in Dubai | Drone Shop*. en-US. URL: https://droneshop.ae/drones/skyfend-tracer/ (viitattu 01. 11. 2024).

[16] DZYGA. Ukrainian. Syyskuu 2024. URL: https://t.me/DZYGA_Drone_Detector/29.

[17] dzyga. URL: https://docs.google.com/document/u/0/d/15dBQieKEtSVy-m2iiT_bj3NXdN8rtXTLCigEfh8wLo0/mobilebasic?tab=t.0&_immersive_translate_auto_translate=1&usp=embed_facebook (viitattu 07. 11. 2024).

[18] Defense Express. *Ukrainian Manufacturer of Tsukorok Drone Detector Wants to Shift From Chinese Components | Defense Express*. en. URL: https://en.defence-ua.com/industries/ukrainian_manufacturer_of_tsukorok_drone_detector_wants_to_shift_from_chinese_components-10263.html (viitattu 07. 11. 2024).

[19] Martins Ezuma ym. ”Detection and Classification of UAVs Using RF Fingerprints in the Presence of Wi-Fi and Bluetooth Interference”. *IEEE Open Journal of the Communications Society* 1 (2020). Conference Name: IEEE Open Journal of the Communications Society, ss. 60–76. ISSN: 2644-125X. DOI: 10.1109/OJCOMS.2019.2955889. URL: https://ieeexplore.ieee.org/document/8913640/?arnumber=8913640&tag=1 (viitattu 29. 09. 2024).

[20] Przemysław Flak. ”Drone Detection Sensor With Continuous 2.4 GHz ISM Band Coverage Based on Cost-Effective SDR Platform”. *IEEE Access* 9 (2021). Conference Name: IEEE Access, ss. 114574–114586. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2021.3104738. URL: https://ieeexplore.ieee.org/document/9513316/?arnumber=9513316&tag=1 (viitattu 28. 09. 2024).

[21] Serhii Flash. Joulukuu 2024. URL: https://t.me/serhii_flash/4555 (viitattu 22. 12. 2024).

[22] Serhii Flash. Marraskuu 2024. URL: https://t.me/serhii_flash/4245 (viitattu 20. 12. 2024).

[23] Serhii Flash. Joulukuu 2024. URL: https://t.me/serhii_flash/4575 (viitattu 22. 12. 2024).

[24] Pooja Gupta ja S.P. Kar. ”MUSIC and improved MUSIC algorithm to estimate direction of arrival”. *2015 International Conference on Communications and Signal Processing (ICCSP)*. Huhtikuu 2015, ss. 0757–0761. DOI: 10.1109/ICCSP.2015.7322593. URL: https://ieeexplore.ieee.org/document/7322593 (viitattu 18. 12. 2024).

[25] Xuemei Huang ym. ”Unmanned Aerial Vehicle Hub Detection Using Software-Defined Radio”. *2019 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB)*. ISSN: 2155-5052. Kesäkuu 2019, ss. 1–6. DOI: 10.1109/BMSB47279.2019.8971851. URL: https://ieeexplore.ieee.org/document/8971851/?arnumber=8971851 (viitattu 13. 09. 2024).

[26] Abid Hussain ym. ”Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks”. *Journal of Communications and Networks* 16.4 (elokuu 2014). Conference Name: Journal of Communications and Networks, ss. 397–406. ISSN: 1976-5541. DOI: 10.1109/JCN.2014.000069. URL: https://ieeexplore.ieee.org/document/6896563/?arnumber=6896563 (viitattu 19. 11. 2024).

[27] *Ingress Protection (IP) ratings*. en. URL: https://www.iec.ch/ip-ratings (viitattu 11. 12. 2024).

[28] *It's About Time: The Pressing Need to Evolve The Kill Chain*. en-US. Toukokuu 2017. URL: https://warontherocks.com/2017/05/its-about-time-the-pressing-need-to-evolve-the-kill-chain/ (viitattu 11. 12. 2024).

[29] Jyri Kosola. *Digitaalinen taistelukenttä : informaatioajan sotakoneen tekniikka*. fi. D5 Oppikirja, ammatillinen käsi- tai opaskirja taikka sanakirja. Accepted: 2014-01-15T08:48:39Z ISBN: 9789512525034 ISSN: 1796-4059 Publisher: Maanpuolustuskorkeakoulu. 2013. URL: https://www.doria.fi/handle/10024/94298 (viitattu 07. 10. 2024).

[30] Kvertus. *Advanced development of EW tools | Kvertus LTEJ Mirage | Ukraine*. en-US. URL: https://kvertus.ua/en/product/ltej-mirage/ (viitattu 06. 12. 2024).

[31] Kvertus. *Kvertus AD Counter FPV :* en-US. URL: https://kvertus.ua/en/product/kvertus-ad-counter-fpv-backpack/ (viitattu 06. 12. 2024).

[32] Johtamisen ja sotilaspedagogiikan laitos ym. *Taistelijan fyysinen toimintakyky 2020 : tieteellinen katsaus*. fi. C2 Toimitettu kirja, kokoomateos, konferenssijulkaisu tai lehden erikoisnumero. Accepted: 2021-04-28T08:14:44Z ISBN: 9789512531851 Publisher: Maanpuolustuskorkeakoulu. 2021. URL: https://www.doria.fi/handle/10024/180906 (viitattu 08. 10. 2024).

[33] M2fpv. Lokakuu 2024. URL: https://t.me/M2fpv/2406.

[34] Abdullahi Mohammad ym. "Learning-Based RF Fingerprinting for Device Identification using Amplitude-Phase Spectrograms". en. *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*. Hong Kong, Hong Kong: IEEE, lokakuu 2023, ss. 1–6. ISBN: 9798350329285. DOI: 10.1109/VTC2023-Fall60731.2023.10333639. URL: https://ieeexplore.ieee.org/document/10333639/ (viitattu 08. 10. 2024).

[35] Wei Nie ym. "UAV Detection and Localization Based on Multi-Dimensional Signal Features". *IEEE Sensors Journal* 22.6 (maaliskuu 2022). Conference Name: IEEE Sensors Journal, ss. 5150–5162. ISSN: 1558-1748. DOI: 10.1109/JSEN.2021.3105229. URL: https://ieeexplore.ieee.org/document/9514865 (viitattu 13. 09. 2024).

[36] Dan O'Shea. *Drone defense firm DroneShield lands $33M U.S. government deal | Fierce Electronics*. en. Section: Fierce Electronics Homepage,Electronics,Sensors. Heinäkuu 2023. URL: https://www.fierceelectronics.com/sensors/drone-defense-firm-droneshield-lands-33m-us-government-deal (viitattu 28. 10. 2024).

[37] *On the Detection of Unauthorized Drones - Techniques and Future Perspectives: A Review*. URL: https://ieeexplore.ieee.org/document/9765451 (viitattu 19. 09. 2024).

[38] Richard Poisel. *Modern Communications Jamming Principles and Techniques, Second Edition*. Norwood, MA, UNITED STATES: Artech House, 2011. ISBN: 978-1-60807-166-1. URL: http://ebookcentral.proquest.com/lib/tampere/detail.action?docID=676301 (viitattu 20. 11. 2024).

[39] Karel Pärlin, Muhammad Mahtab Alam ja Yannick Le Moullec. "Mehitamata õhusõidukite juhtimiseks kasutatavate hajaspekter sidesüsteemide segamine" (kesäkuu

2017). URL: https://digikogu.taltech.ee/et/item/401d55b6-c003-4c7a-8d6a-7aea6ac83271 (viitattu 20. 11. 2024).

[40] *RfPatrol Mk2: Counterdrone (C-UAS) Protection*. en-US. URL: https://www.droneshield.com/c-uas-products/rfpatrol-mk2 (viitattu 26. 11. 2024).

[41] Roy [@GrandpaRoy2]. en. Heinäkuu 2024. URL: https://x.com/GrandpaRoy2/status/1809638911943299327 (viitattu 07. 11. 2024).

[42] Savio Sciancalepore ym. ”PiNcH: An effective, efficient, and robust solution to drone detection via network traffic analysis”. *Computer Networks* 168 (helmikuu 2020), s. 107044. ISSN: 1389-1286. DOI: 10.1016/j.comnet.2019.107044. URL: https://www.sciencedirect.com/science/article/pii/S1389128619311764 (viitattu 30. 09. 2024).

[43] Skyfend. *Shop Skyfend Tracer P Drone Detector - Skyfend Online Store*. en. URL: https://store.skyfend.com/products/tracer (viitattu 01. 11. 2024).

[44] Skyfend-Europe. *SFE-Tracer-S V2 - drone detector via spectrum analysis*. en. URL: https://www.skyfend-europe.com/product-page/sfe-tracer-s-v2-drone-detector-via-spectrum-analysis (viitattu 19. 12. 2024).

[45] Skyowl. uk. URL: https://skyowl.com.ua/ (viitattu 07. 11. 2024).

[46] *ST-C-UAS Technology Guide | Homeland Security*. en. URL: https://www.dhs.gov/publication/st-c-uas-technology-guide (viitattu 11. 12. 2024).

[47] G. Sucharitha, Mettu Srinivas ja Anjanna Matta. *Machine learning algorithms and applications*. eng. Hoboken, New Jersey: John Wiley & Sons, 2021. ISBN: 978-1-119-76925-5.

[48] Angesom Ataklity Tesfay ym. ”Smart Jamming: Deep Learning-Based UAVs Neutralization System”. *2024 International Symposium on Electromagnetic Compatibility – EMC Europe*. ISSN: 2325-0364. Syyskuu 2024, ss. 380–384. DOI: 10.1109/EMCEurope59828.2024.10722367. URL: https://ieeexplore.ieee.org/document/10722367/?arnumber=10722367&tag=1 (viitattu 19. 11. 2024).

[49] Jacopo Tosi ym. ”Performance Evaluation of Bluetooth Low Energy: A Systematic Review”. en. *Sensors* 17.12 (joulukuu 2017), s. 2898. ISSN: 1424-8220. DOI: 10.3390/s17122898. URL: https://www.mdpi.com/1424-8220/17/12/2898 (viitattu 29. 10. 2024).

[50] *Wearable Drone Detector Handheld Multi-Mission Detection Tool Support English Russian 2km*. en. URL: https://www.tatusky.com/products/wearable-drone-detector-handheld-multi-mission-detection-tool-support-english-russian-2km (viitattu 29. 10. 2024).