Tampereen yliopisto

Miikka Mäenpää

RADIOHÄIRINTÄ IMPROVISOITUJEN RÄJÄHTEIDEN JA KAUKO-OHJATTAVIEN LENNOKKIEN TORJUNNASSA

Informaatioteknologian ja viestinnän tiedekunta
Tarkastaja: TkT Taneli Riihonen
Kandidaatintyö
Helmikuu 2019

TIIVISTELMÄ

Miikka Mäenpää: Radiohäirintä improvisoitujen räjähteiden ja
kauko-ohjattavien lennokkien torjunnassa
Kandidaatintyö
Tampereen yliopisto
Tieto- ja sähkötekniikan kandidaatin tutkinto-ohjelma
Tarkastaja: TkT Taneli Riihonen
Helmikuu 2019

Tämän kandidaatintyön aiheena on radiohäirintä improvisoitujen räjähteiden ja kauko-ohjattavien lennokkien torjunnassa. Radiohäirintä on ajankohtainen tutkimusaihe varsinkin lennokkien torjunnassa. Vielä toistaiseksi radiohäirinnän merkittävimmät sovelluskohteet ovat olleet sotilastoiminnassa esimerkiksi improvisoitujen räjähteiden torjunnassa, mutta erityisesti lennokkien tapauksessa radiohäirinnästä olisi hyötyä myös siviiliviranomaiselle. Radiohäirintää on kirjallisuudessa käsitelty yleisellä tasolla paljon, mutta lennokkien torjunnassa melko vähän. Kaupallisia laitteita löytyy hyvinkin paljon, mutta useimmat käyttävät yksinkertaisia häirintätekniikoita, joilla saavutetaan heikko energiatehokkuus.

Työ koostuu teoreettisesta ja kokeellisesta osuudesta. Teoriaosuudessa tarkastellaan yllä mainittujen laitteiden radioprotokollia sekä vertaillaan niiden torjunnassa käytettäviä radiohäirintätekniikoita. Protokollan tunnistus on tärkeä edellytys tehokkaalle radiohäirinnälle, koska improvisoiduissa räjähteissä voidaan käyttää melkein mitä tahansa radiolaitteita ja lennokkien ohjaukseen tarkoitetuissa laitteissa käytetään satoja erilaisia radioprotokollia. Lisäksi tutkitaan full-duplexin hyödyntämistä radiohäirinnässä, analysoidaan häirinnän tehokkuutta sekä tehdään lyhyt markkinakatsaus kaupallisiin häirintälaitteisiin.

Kokeellisessa osuudessa rakennetaan mittauslaitteisto AFHDS-protokollaa (engl. Automatic Frequency Hopping Digital System) käyttävälle radiovastaanottimelle häirinnän tehokkuuden toteamista varten sekä testataan kahta eri häirintätekniikkaa kyseistä radiolaitetta käyttävän improvisoidun räjähteen torjunnassa. Testeissä saavutettiin laajakaistahäirinnällä häirintälähettimen ympärille yli 10 metrin säteinen häirinnän peittoalue, jossa häirintä todettiin toimivaksi. Tiedettäessä kohteen käyttämät kanavat, voidaan käyttää monikanavahäirintää, jolla saavutettiin testeissä jopa lähes 40 metrin säteinen häirinnän peittoalue. Käytetyt tehotasot olivat melko pieniä, joten oikeissa sovelluksissa voitaisiin saavuttaa moninkertaiset häirintäkantamat vain kasvattamalla häirintätehoa.

Kohteen käyttämät kanavat voidaan tunnistaa kuuntelemalla taajuuskaistaa. Käyttämällä full-duplex-tekniikkaa voidaan taajuuskaistan kuuntelu suorittaa häirinnän kanssa samanaikaisesti, mikä mahdollistaa myös tehokkaampien häirintätekniikoiden hyödyntämisen. Testeistä todettiin, kuinka suuri vaikutus radiohäirinnässä on kohteen protokollan tunnistuksella, mutta jos ei haittaa, että häirintä kohdistuu kaikkiin kyseisellä taajuuskaistalla toimiviin laitteisiin ja oman lähettimen helppo havaittavuus ei ole ongelma, voidaan yksinkertaisellakin häirinnällä saavuttaa toimivia tuloksia tehotasoja kasvattamalla.

Avainsanat: radiohäirintä, radio-ohjattavat improvisoidut räjähteet, RCIED, tienvarsipommi, lennokki, drone, monikopteri, kuvauskopteri, full-duplex, AFHDS, protokollatietoisuus, adaptiivinen häirintä, mikrokontrolleri

ALKUSANAT

Työ on tehty Maanpuolustuksen tieteellisen neuvottelukunnan (MATINEn) rahoittamassa ”Full-duplex radioteknologia sotilaskäytössä” -tutkimushankkeessa. Koko projekti oli erittäin mielenkiintoinen ja opin paljon uutta. Varsinkin kiinnostukseni full-duplex tekniikkaan sekä radiohäirintään kasvoi projektin aikana. Työn ohjaajana sekä tarkastajana toimi tekniikan tohtori Taneli Riihonen.

Haluaisin kiittää etenkin Taneli Riihosta suuresta avusta ja ohjauksesta kandidaatintyön toteuttamiseen. Haluan kiittää myös kaikkia muita hankkeeseen osallistuneita, keiden kanssa olen saanut työskennellä. Lisäksi myös kiitokset kihlatulleni suuresta tuesta.

Tampereella, 1.2.2019

Miikka Mäenpää

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

A/D-muunnin	analogia-digitaalimuunnin
ACCST	Advanced Continuous Channel Shifting Technology
AFHDS	Automatic Frequency Hopping Digital System
AFHSS	Adaptive Frequency Hopping Spread Spectrum
BER	bit error ratio
BPSK	binary phase-shift keying
CB	citizens' band
CRC	cyclic redundancy check
CSS	chirp spread spectrum
DMSS	Dual Modulation Spectrum System
DSM	Digital Spectrum Modulation
DSSS	direct-sequence spread spectrum
FASST	Futaba Advanced Spread Spectrum Technology
FHSS	frequency-hopping spread spectrum
FM	frequency modulation
FSK	frequency-shift keying
GFSK	Gaussian frequency-shift keying
GMSK	Gaussian minimum shift keying
IED	improvised explosive device
IEEE	Institute of Electrical and Electronics Engineers
ISM	industrial, scientific and medical
JR	Japan Remote Control
JSR	jam to signal ratio
LA	lyhytaalto
OFDM	orthogonal frequency-division multiplexing
PBIED	personel-borne IED
PER	packet error ratio
PMR446	personal mobile radio, 446 MHz
PR	personal radio
PSK	phase-shift keying
PWM	pulse width modulation
RCIED	radio controlled improvised explosive device
RSSI	received signal strength indication
SINR	signal-to-interference-plus-noise ratio
SLT	Secure Link Technology
SNR	signal-to-noise ratio
UAV	unmanned aerial vehicle
VBIED	vehicle-bourne IED
VOIED	victim-operated IED
WLAN	wireless local area network

1. JOHDANTO

Nykyaikana radiolaitteet ovat yleistyneet kuluttajaelektroniikassa. Niiden hankkiminen, käyttäminen sekä soveltaminen on helppoa ja edullista. Radiolaitteita käytetään esimerkiksi kauko-ohjausjärjestelmissä, televisio- ja radiolähetyksissä, mobiililaitteissa ja monissa muissa langattoman datansiirron sovelluksissa. Radiolaitteita voidaan valitettavasti myös väärinkäyttää, jolloin niistä voi koitua esimerkiksi turvallisuusuhkia. Varsinkin radio-ohjattavat lennokit ovat lisääntyneet viime vuosina. Lennokilla tarkoitetaan tässä työssä kiinteäsiipisten lennokkien lisäksi droneja. Lennokkeja voidaan käyttää esimerkiksi rikoksiin, kuten salakuvaamiseen, yritysvakoiluun tai salakuljettamiseen [1]. Etenkin Rikosseuraamuslaitokselle sekä Rajavartiolaitokselle on tullut ongelma droneilla suoritettavista salakuljetuksista [2, 3]. Piittaamattomalla lentämisellä voidaan myös vaarantaa ilmatila, yleisön turvallisuus tai häiritä viranomaisten tehtäviä. Näistä syistä lennokkien lennättäminen onkin kielletty monissa paikoissa, mutta niiden valvonta ja rikoksiin puuttuminen on hankalaa viranomaisten toimesta. [4]

Lennokkien käyttö on yleistynyt myös sotilasympäristössä, jossa ne luokitellaan yleensä miehittämättömiin ilma-aluksiin (engl. Unmanned Aerial Vehicle, UAV). Miehittämättömiä ilma-aluksia käytetään jo nyt monipuolisesti hyödyksi, eikä niiden kaikkia mahdollisuuksia vielä edes tiedetä. Miehittämättömillä ilma-aluksilla voidaan esimerkiksi tiedustella vihollisen toimintaa tai tutkia ympäristöä. Lisäksi ne voidaan jopa varustaa erilaisilla asejärjestelmillä. Tämän vuoksi radiohäirintä on merkittävässä roolissa, jotta sotilaat pystyisivät vastaamaan vihollisen toimintaan. Toinen ongelmakategoria sotilasnäkökulmasta on radio-ohjattavat improvisoidut räjähteet, joita on helppo rakentaa kaupallisista radiolaitteista. Pommiuhat ovat yleistyneet myös siviiliympäristössä, joten radiohäirinnästä olisi hyötyä yhtä lailla terrorismin torjunnassa.

Tämän työn aiheena on selvittää radiohäirinnän keinoja etenkin radio-ohjattavia improvisoituja räjähteitä ja lennokkeja vastaan. Työn tavoitteena on tutustua yleisesti edellä mainittujen laitteiden käyttämiin radioprotokolliin ja häirintätekniikoihin sekä vertailla niiden toimivuutta ja tehokkuutta. Työssä keskitytään tarkemmin AFHDS-protokollaan (engl. Automatic Frequency Hopping Digital System) ja sen häirintään sekä testataan käytännössä kahta eri häirintätekniikkaa kyseistä protokollaa käyttävän improvisoidun räjähteen torjunnassa. Testeillä osoitetaan, että yksinkertaisellakin häirinnällä voidaan saavuttaa tehokkaita tuloksia, mutta tunnistamalla kohteen protokolla voidaan moninkertaistaa häirinnän tehokkuus.

Työn rakenne on seuraavanlainen. Toisessa luvussa tutustutaan yleisimpiin kaupallisiin radiolaitteisiin sekä radioprotokolliin, joita käytetään yllä mainituissa sovelluksissa. Kolmannessa luvussa käydään läpi yleisimpiä häirintätekniikoita sekä ns. full-duplex-teknii-

kan hyödyntämistä häirinnässä. Lisäksi perehdytään häirinnän tehokkuuden analyysiin sekä esitellään lyhyesti kaupallisia häirintälaitteita. Neljännessä luvussa kerrotaan työn kokeellisesta osuudesta, jossa rakennetaan mittalaitteisto häirinnän tehokkuuden toteamista varten, testataan kahden eri häirintätekniikan toimivuutta improvisoidun räjähteen torjunnassa sekä vertaillaan tuloksia teoriaan. Viimeisenä lukuna on työn yhteenveto, jossa pohditaan työn tärkeimpiä tuloksia ja johtopäätöksiä.

2. KULUTTAJAELEKTRONIIKAN RADIOLAITTEET

Radiolaitteet lähettävät ja/tai vastaanottavat sähkömagneettisia aaltoja jotain tiettyä tarkoitusta varten [5]. Tällaisiin radioaaltoihin voidaan moduloida informaatiota, mikä tarkoittaa aallon ominaisuuksien muuttamista esimerkiksi bittijonon mukaan digitaalisessa tiedonsiirrossa. Radioaaltoa, johon moduloidaan informaatiota, kutsutaan kantoaalloksi, ja sillä on monia eri ominaisuuksia, kuten amplitudi, taajuus, vaihe sekä spektri. Spektrillä tarkoitetaan signaalin energian taajuusjakaumaa. Myös erilaisia modulointitapoja on useita. [6] Jotta radiolaitteet pystyisivät kommunikoimaan keskenään, niiden pitää käyttää samoja kantoaallon ominaisuuksia, samaa modulointitapaa sekä muita tiedonsiirtoon liittyviä käytäntöjä. Näitä yhdessä kutsutaan radioprotokollaksi. Työssä keskitytään radio-ohjattavissa improvisoiduissa räjähteissä sekä kauko-ohjattavissa lennokeissa käytettäviin radiolaitteisiin sekä niiden protokolliin, joista kerrotaan tarkemmin tässä luvussa.

2.1 Radio-ohjattavat improvisoidut räjähteet

Improvisoidulla räjähteellä (engl. improvised explosive device, IED) tarkoitetaan "itsetehtyä pommia" [7]. Ne koostuvat yleensä räjähdysaineesta, sytyttimestä, säiliöstä sekä sytytys- ja turvakytkimistä [8]. Niitä on paljon erilaisia ja ne voidaan luokitella moniin eri luokkiin niiden ominaisuuksien perusteella. Esimerkiksi kuljetustavan perusteella ne voidaan luokitella seuraavanlaisesti:

- ajoneuvoon asetetut räjähteet (engl. vehicle-borne IED, VBIED),
- ihmiseen asetetut räjähteet (engl. personel-borne IED, PBIED),
- ohjustyyppiset räjähteet,
- passiiviset räjähteet, kuten miinat. [8]

Myöskin sytytystapoja improvisoiduilla räjähteillä on hyvin monia, mutta yleisimmin ne jaetaan seuraavaan kolmeen pääluokkaan:

- ajastetut räjähteet,
- käskystä aktivoidut räjähteet (engl. command-initiated IED),
- uhrin laukaisemat räjähteet (engl. victim-operated IED, VOIED). [8]

Tässä työssä keskitytään radio-ohjattaviin improvisoituihin räjähteisiin (engl. radio controlled IED, RCIED). Ne kuuluvat käskystä aktivoitaviin improvisoituihin räjähteisiin ja niiden sytytyskytkimenä käytetään radiolähetintä ja -vastaanotinta. [7, 8] Kun radiolähettimestä lähetetään sytytyskäsky radiovastaanottimelle, se aktivoi sytyttimen, joka räjäyttää räjähdysaineen.

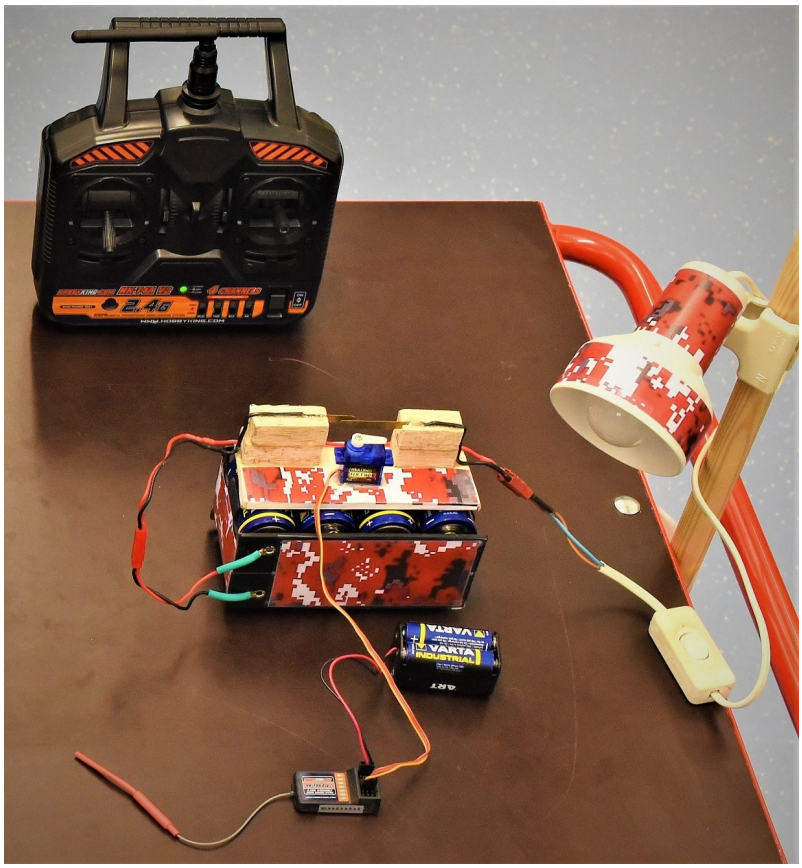
Radiolaitteella yleensä aktivoidaan pelkästään räjäytystapahtuma, mikä tarkoittaa vain yhden bitin informaatiota tiedonsiirron näkökulmasta. Tämän takia improvisoidun räjähteen toteuttamiseen voidaan käyttää hyvinkin yksinkertaisia, helposti saatavilla olevia radiolaitteita, kuten langatonta ovikelloa, itkuhälytintä, auton keskuslukituksen kauko-ohjainta tai oikeastaan mitä tahansa kauko-ohjainta [7]. Lisäksi monimutkaisempia, mutta mahdollisesti radioyhteyden kannalta parempia laitteita, kuten matkapuhelinta, radiopuhelinta tai satelliittipuhelinta voidaan käyttää RCIED:ssä [9].

Koska laitteita on paljon, voivat improvisoidun räjähteen käyttämät taajuudet ja radioprotokollat vaihdella hyvinkin paljon riippuen käytössä olevasta radiolaitteesta. Yleisimmin käytetyt radiolaitteet ovat kuluttajaelektroniikkaa, jotka toimivat ISM-taajuuskaistoilla (engl. industrial, scientific and medical), koska ne ovat edullisia ja niitä on paljon saatavilla. Taulukkoon 1 on kerätty muutamia esimerkkejä improvisoiduissa räjähteissä mahdollisesti käytettävistä radiolaitteista ja niiden taajuusalueista Suomessa.

Taulukko 1. *RCIED:hen soveltuvien radiolaitteiden toimintataajuuksia [7, 9, 10].*

Taajuus (MHz)	Tyypilliset laitteet
27	Pienoismallien analoginen kauko-ohjaus, LA-, CB-, ja PR-27-radiopuhelimet
35	Pienoismallien analoginen kauko-ohjaus
68	Harrastus- ja työyhteyksien radiolähettimet
100	Pienitehoiset FM- lähettimet
433	Yleiset lyhyen kantaman radiolähettimet (auton keskuslukitus, autotallin ovi, ovikello)
446	PMR446-radiopuhelimet
700, 800, 900, 1800, 2100, 2600	Matkapuhelimet
1600	Satelliittipuhelimet
2400	WLAN, Bluetooth, autohälyttimet, Pienoismallien digitaalinen kauko-ohjaus
5800	WLAN, kuvauskopterien videosignaali, pienoismallien digitaalinen kauko-ohjaus

Kuvassa 1 näkyy esimerkkinä radio-ohjattava improvisoitu räjähde, jota käytetään myös kokeellisessa osiossa. Räjähteen kauko-ohjaus on rakennettu 2,4 GHz:n taajuudella toimivan lennokin radiolähettimestä (HK-T4A-V2 [11]) ja radiovastaanottimesta (HK-TR6A-V2 [11]). Improvisoidun räjähteen sähkönalli on turvallisuussyistä vaihdettu led-valoon, joka kuvaa onnistunutta räjäytystapahtumaa. Kyseisellä radio-ohjauslinkillä välitetään vastaanottimelle neljä pulssinleveysmoduloitua (engl. pulse width modulation, PWM) kanavaa, jotka normaalisti säätävät lennokin servomoottoreita. Servomoottoreilla ohjataan normaalisti lennokin liikkumista, mutta tässä tapauksessa servomoottorilla väännetään kahta metallilevyä yhteen, jolloin 12 V:n patteristo kytkeytyy sähköisesti led-valoon ja pommi "räjähtää".



Kuva 1. *Radio-ohjattava improvisoitu räjähde*

2.2 Radio-ohjattavat lennokit

Lennokin määritelmä riippuu hieman asiaympäristöstä. Ilmailulain mukaan lennokilla tarkoitetaan *"lentämään tarkoitettua laitetta, jonka mukana ei ole ohjaajaa ja jota käytetään harraste- tai urheilutarkoitukseen"*. Jos laitetta käytetään johonkin muuhun tarkoitukseen, se luokitellaan miehittämättömäksi ilma-alukseksi. [12]

Tässä työssä lennokilla tarkoitetaan kiinteäsiipisten lennokkien lisäksi droneja. Dronella tarkoitetaan radio-ohjattavaa monimoottorikopteria, jota hyödynnetään usein ilmakuvaukseen. Dronet eroavat muista lennokeista niiden autonomisen ohjausjärjestelmän takia, jonka vuoksi ne ovat helppoja lennättää. Sen vuoksi ne ovat yleistyneet ja niitä hyödynnetään monissa eri sovelluksissa sekä harrastus- että ammattikäytössä. Tässä työssä keskitytään lennokkien radio-ohjaukseen, joka on yleensä samankaltainen riippumatta lennokkityypistä. Sotilasympäristössä lennokit luokitellaan yleensä miehittämättömiin ilma-aluksiin (engl. unmanned aerial vehicle, UAV), joka kattaa pienien lennokkien lisäksi myös paljon isommat lennokit.

Suomessa mahdolliset taajuudet lennokkien ohjaukseen kuluttajakäytössä ovat: 35 MHz, 2,4 GHz ja 5,8 GHz [13]. Vanhat analogiset ohjausjärjestelmät käyttivät 35 MHz:n taajuutta, mutta nykyään ohjausjärjestelmät ovat digitaalisia ja toimivat 2,4 GHz:n tai 5,8 GHz:n taajuudella. Analogisissa järjestelmissä on rajallinen määrä taajuuskanavia, joilla lähetin-

vastaanotin pari voi toimia, kun taas digitaalisissa järjestelmissä käytetään taajuusjakoista kanavointia. Myös antennit ovat paljon suurempia analogisissa järjestelmissä verrattuna digitaalisiin, johtuen suuremmasta aallonpituudesta. Suuremmilla taajuuksilla kantama on luontaisesti lyhyempi, joten 5,8 GHz:n taajuutta käytetään yleensä videon lähetykseen lennokista maahan ja 2,4 GHz:n taajuutta puolestaan radio-ohjaukseen. Tässä työssä keskitytään pääasiassa 2,4 GHz:n taajuudella toimiviin digitaalisiin radio-ohjausprotokolliin, johtuen niiden yleisyydestä sekä testilaitteiston valinnasta.

2.3 Modulaatio

Informaation moduloimiseksi kantoaaltoon on monia eri tekniikoita, mutta yleisimmät digitaaliset modulointitekniikat ovat taajuusavainnus (engl. frequency-shift keying, FSK) ja vaiheavainnus (engl. phase-shift keying, PSK). Taajuus- ja vaiheavainnuksista on monia eri variaatioita, riippuen esimerkiksi symbolien määrästä, suodatuksesta tai signaalin jatkuvuudesta. Symboli kuvaa tiedonsiirrossa bittikombinaatiota. Esimerkiksi, jos järjestelmä käyttää kahta symbolia, sitä kutsutaan yleensä binääriseksi, jossa jokainen symboli kuvaa yhtä bittiä, mutta jos järjestelmässä käytetään enemmän symboleita, voivat symbolit kuvata useita bittejä. [6]

Yksinkertaisin vaiheavainnus on nimeltään binäärinen vaiheavainnus (engl. binary phase-shift keying, BPSK), jossa vakioamplitudisen kantoaallon vaihe saa kahta eri arvoa, riippuen onko datasignaali yksi vai nolla. Lähetettävät signaalit, joilla on 180 asteen vaihe-ero, voivat olla esimerkiksi muotoa:

$$s_1(t) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t) \tag{1}$$

$$s_2(t) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t + \pi) = -\sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t), \tag{2}$$

jossa E_b on bitin energia, T_b bitin kesto ja f_c kantoaallon taajuus. Yhdistämällä eri vaiheiset signaalit, saadaan lähetettävän signaalin muodoksi

$$s_d(t) = d(t)\sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t), \tag{3}$$

jossa $d(t)$ on datasignaali, mikä koostuu arvoista ± 1. [14]

Taajuusavainnuksessa puolestaan kantoaallon taajuutta vaihdellaan datasignaalin mukaan. Yksinkertaisin taajuusavainnus on binäärinen taajuusavainnus (engl. binary frequency-shift keying, BFSK), johon usein viitataan pelkästään taajuusavainnuksena tai FSK:na [15]. Lähetettävä signaali taajuusavainnuksessa voidaan kuvata esimerkiksi seuraavasti

$$s_m(t) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t + \pi m \Delta f t), \tag{4}$$

jossa m on symbolin indeksi, joka binäärisessä taajuusavainnuksessa koostuu arvoista ± 1, riippuen mitä bittiä halutaan esittää ja Δf on lähetettävien symbolien taajuupoikkeama eli deviaatio [6].

Moduloitaessa signaalia on yleensä toivottua, että signaali pysyy mahdollisimman kapeana taajuustasossa. Eri modulointitavoissa voidaan hyödyntää erilaisia keinoja pulssin muokkaamiseksi, jotta signaali ei leviä taajuustasossa [14]. Esimerkiksi taajuusavainnuksessa käytetään usein Gaussista suodinta datasignaalille, jotta taajuusvaihtelu olisi pehmeämpi ja kaistanleveys pysyisi pienempänä. Tällöin modulaatiota kutsutaan GFSK:ksi (engl. Gaussian frequency shift keying) [14].

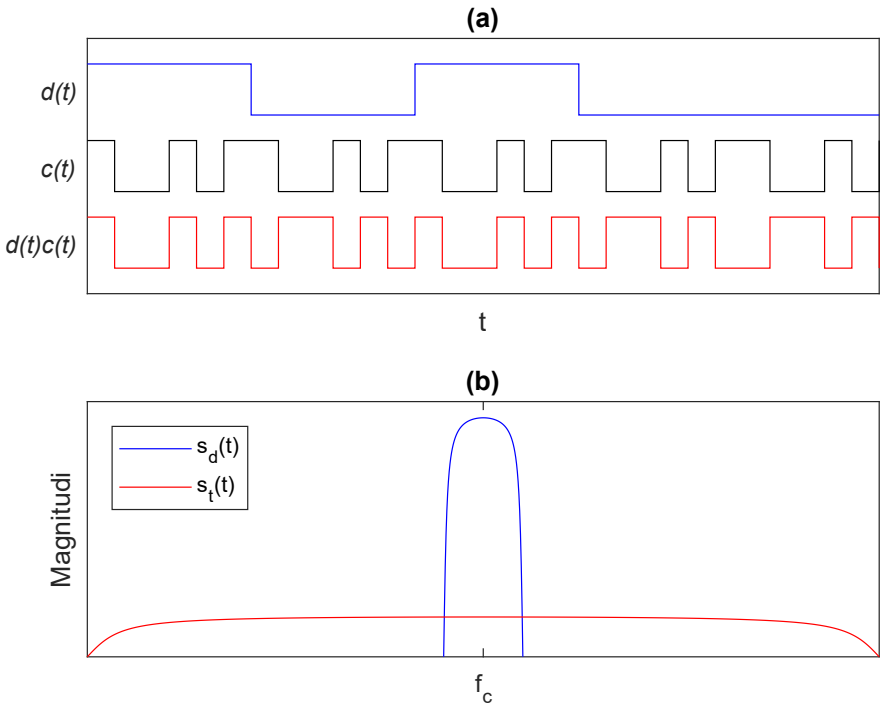
2.4 Hajaspektritekniikat

Käytettäessä 2,4 GHz:n taajuuskaistaa, on otettava huomioon sen häiriöllisyys ja ruuhkaisuus. Esimerkiksi mikroaaltouunit aiheuttavat kyseiselle taajuuskaistalle häiriöitä ja lisäksi taajuuskaistaa käyttää monet radiolaitteet, kuten WLAN- ja Bluetooth-laitteet. Tämän vuoksi signaali pitää pystyä erottamaan päällekkäisistä signaaleista sekä häiriöistä. Tätä varten signaaleissa käytetään hajaspektrilähetystä kuten taajuushyppelevää hajaspektriä (engl. frequency hopping spread spectrum, FHSS) tai suorasekvenssi hajaspektriä (engl. direct-sequence spread spectrum, DSSS). Osassa järjestelmissä hyödynnetään myös molempia yhdessä. Muutamia poikkeuksiakin löytyy, kuten Parrot AR2-drone, joka käyttää WLAN:ia tiedonsiirtoon, missä käytetään OFDM-tekniikkaa (engl. orthogonal frequency-division multiplexing). [16] Hajaspektrijärjestelmissä käytetään suurempaa taajuuskaistaa, mitä datan lähettämiseen tarvittaisiin, jotta datasignaali sietäisi paremmin kohinaa, interferenssiä sekä häirintää. Hajaspektrin tuomaa etua (engl. processing gain) voidaan arvioida esimerkiksi hajaspektrin kaistanleveyden suhteena alkuperäiseen bittinopeuteen tai alkuperäiseen kaistanleveyteen. [17]

2.4.1 DSSS

DSSS-tekniikassa datasignaali kerrotaan signaalilla, jolla on paljon suurempi bittinopeus. Kun bittinopeutta kasvatetaan, myös signaali taajuustasossa levenee ja siksi signaalia, jolla datasignaali kerrotaan, kutsutaan levityskoodiksi (engl. spreading code). Kuvassa 2 (a) näkyy aikatasossa datasignaali $d(t)$, levityskoodi $c(t)$ sekä niiden tulosignaali $d(t)c(t)$. Levitetty datasignaali $d(t)c(t)$ voidaan vastaanottimessa palauttaa alkuperäiseksi datasignaaliksi vain kertomalla samalla levityskoodilla $c(t)$. [18]

Yleisin modulointitapa DSSS-järjestelmissä on vaiheavainnus. Kantoaalto, johon on moduloitu data BPSK:ta käyttäen, voi olla esimerkiksi kaavan (3) muotoista. Taajuustasossa tällainen kantoaalto vastaa kuvan 2 (b) sinistä signaalia, jonka pääasiallinen teho on levittynyt hyvin kapealle alueelle.



Kuva 2. *DSSS-järjestelmän datasignaali, levityskoodi ja niiden tulo aikatasossa (a) sekä BPSK:lla moduloidut kantoaallot taajuustasossa ennen ja jälkeen levitystä (b)*

Kantoaalto kerrotaan levityskoodilla $c(t)$, joka saa arvoja ± 1, jonka jälkeen kantoaalto on muotoa:

$$s_t(t) = d(t)c(t)\sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t). \tag{5}$$

Nyt kantoaallon vaihe muuttuu levityskoodista riippuen paljon useammin mitä ennen levityskoodilla kertomista ja tällöin taajuustasossa signaali levenee, kuten nähdään kuvassa 2 (b) punaisella. [17]

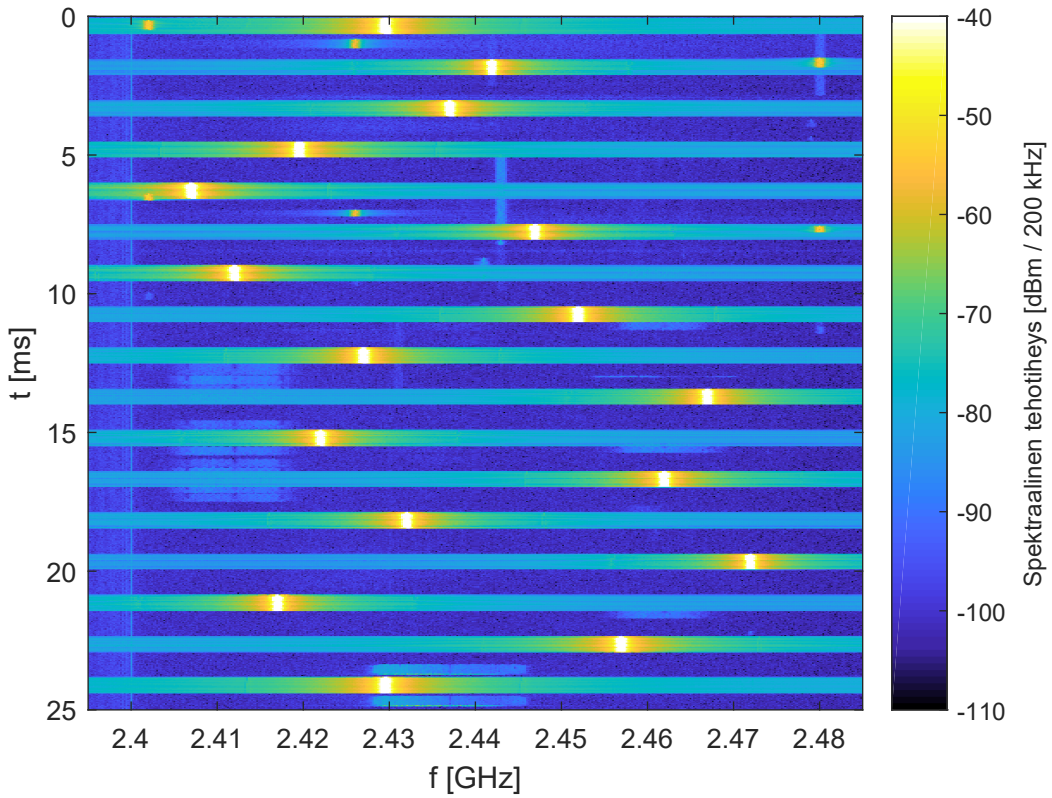
2.4.2 FHSS

Taajuushyppelevässä hajaspektritekniikassa käytössä oleva taajuuskaista jaetaan kapeisiin kanaviin ja hetkellisesti käytettävää keskitaajuutta vaihdetaan ennalta määritellyn hyppysekvenssin mukaan, jokaisen tai muutaman datapaketin lähetyksen jälkeen [16]. Yleisin modulointitapa FHSS-järjestelmissä on taajuusavainnus [6]. Taajuushyppelevän hajaspektritekniikan tärkeimpiä ominaisuuksia ovat muun muassa:

- kanavien määrä
- kanavien leveys
- kanavien hyppynopeus eli kuinka usein vaihdetaan kanavaa
- hyppysekvenssi eli kanavien hyppimisjärjestys
- kanavan päälläoloaika.

Jos hyppynopeus on yhtä suuri tai suurempi kuin symbolinopeus, järjestelmä katsotaan yleensä nopeaksi FHSS-järjestelmäksi ja muulloin hitaaksi FHSS-järjestelmäksi [6]. Lennokkien radio-ohjausjärjestelmät käyttävät yleensä hitaita FHSS-järjestelmiä ja tyypilliset arvot hyppynopeudelle ovat 90 - 300 hyppyä/s, kanavan leveydelle 300 - 2500 kHz ja kanavan päälläoloajalle 0,5 - 5 ms [19].

Kuvassa 3 näkyy kokeellisessa osuudessa käytettävän AFHDS-järjestelmän taajuushyppelevän signaalin ilman yli mitattu spektrogrammi. Järjestelmän lähetys näkyy kuvassa kirkkaina alueina, joissa spektraalinen tehotiheys on yli −40 dBm. Kyseinen AFHDS-järjestelmä käyttää 16 kanavaa, joiden leveys on 500 kHz. Kanavien vaihtoaika on noin 1,48 ms eli hyppynopeus on noin 675 hyppyä/s ja kanavan lähetys on päällä noin 0,6 ms. Koska spektri on mitattu ilman yli, kuvassa näkyy myös muita lähetyksiä, kuten 20 MHz:n levyinen WLAN lähetys ainakin kahdella eri kanavalla (2412 MHz ja 2437 MHz). Tässä työssä FHSS-järjestelmän yhdellä kanavalla lähettämää dataa kutsutaan usein kehykseksi tai paketiksi.



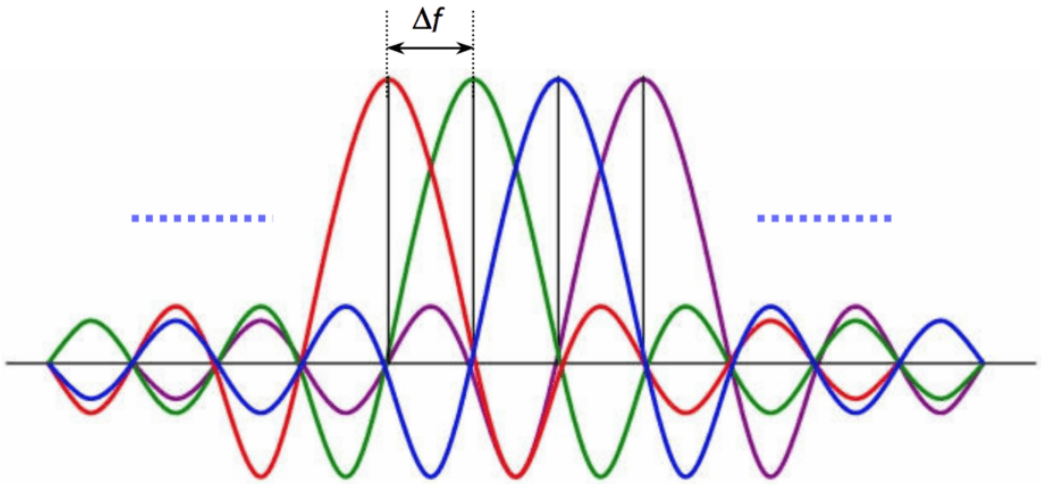
Kuva 3. *FHSS-signaalin spektrogrammi*

Usein FHSS-tekniikan kanssa käytetään myös DSSS-tekniikkaa. Lähetyksen spektri saadaan levitettyä ja piilotettua DSSS:n avulla ja FHSS puolestaan tarjoaa monimuotoisen taajuusjakauman, joka auttaa esimerkiksi taajuusselektiivistä häipymistä vastaan. [17] Jos samalla taajuuskaistalla on muita FHSS-hajaspektriä käyttäviä laitteita, voivat lähetykset välillä törmätä. Törmäyksessä kaksi laitetta käyttää hetkellisesti samaa taajuutta, jol-

loin bittivirhesuhde todennäköisesti kasvaa huomattavasti. FHSS-järjestelmät on pyritty suunnittelemaan niin, ettei törmäyksiä tapahtuisi, mutta aina niitä ei voida välttää. [18] Hybridi-järjestelmällä on paremmat mahdollisuudet tunnistaa vastaanotettu signaali törmäyksen sattuessa, koska data on koodattu levityskoodilla.

2.4.3 OFDM

Lennokkien ohjauksessa harvemmin käytetyssä OFDM-tekniikassa kantoaalto jaetaan moneen alikantoaaltoon (engl. subcarrier), jotka sijoitellaan taajuustasossa ortogonaalisesti limittäin, jotta ne eivät häiritse toisiaan. Kuvassa 4 näkyy taajuustasossa OFDM-signaalin neljä alikantoaaltoa. Alikantoaaltojen keskitaajuuksilla, muiden alikantoaaltojen magnitudi on nolla, jolloin ideaalisesti ne eivät häiritse toisiaan, vaikka ne ovatkin päällekkäin. Tekniikka sietää myös paremmin taajuusselektiivistä häipymistä, koska jaettaessa taajuuskanava useisiin alikantoaaltoihin, näkyy häipyvä kanava yksittäisille kantoaalloille lähes tasaisena kanavana, joka helpottaa tiedonsiirtoa. [6]



Kuva 4. *OFDM signaalin alikantoaallot taajuustasossa [20]*

Alikantoaaltoihin moduloitu informaatio lähetetään rinnakkain, joka mahdollistaa suuret datanopeudet ja taajuuskaistan tehokkaan käytön. [16] Tämän vuoksi OFDM-tekniikka on valittu standardiksi esimerkiksi digitaalisiin televisiolähetyksiin (DVB-T) sekä IEEE 802.11 mukaisiin WLAN verkkoihin [6]. Lennokkien ohjauksessa ei ole tärkeintä datanopeus vaan luotettavuus, joten OFDM:ata käytetään yleisemmin videolinkeissä lennokista maahan.

2.5 Protokollat ja radiopiirit

Taulukkoon 2 on koottu yleisimpien lennokkivalmistajien käyttämiä radioprotokollia, radiopiirejä, hajaspektritekniikoita sekä datan modulaatiomenetelmiä. Taulukkoon on kerätty vain muutaman valmistajan käyttämiä protokollia. Lisäksi samalla valmistajalla saat-

Taulukko 2. *Lennokkivalmistajien käyttämiä protokollia [16, 19, 21–45]*

Valmistaja	Protokolla	Hajaspektri-tekniikka	Radiopiiri	Modulaatio
FlySky	AFHDS	FHSS	Amiccom A7105/A7106	GFSK
Hubsan	X4	-	Amiccom A7105	GFSK
Parrot	WLAN	OFDM	BROADCOM BCM43526	-
Airtronics/Sanwa	FHSS-4	FHSS,DSSS	Cypress CYRF6936	GFSK
Spectrum	DSM/DSM2/DSMX	FHSS,DSSS	Cypress CYRF6936	GFSK
Walkera	DEVO	DSSS	Cypress CYRF6936	GFSK
Futaba	FASST/FASSTest	FHSS,DSSS	Micro Linear ML2724/ML2730	FSK
Bayang	Bayang	FHSS	Nordic Semiconductor NRF24L01	GFSK
Cheerson	CX10/YD717	FHSS/-	Nordic Semiconductor NRF24L01	GFSK
Eachine	Bayamg/MJXq	FHSS	Nordic Semiconductor NRF24L01	GFSK
HiSky	HiSky	FHSS	Nordic Semiconductor NRF24L01	GFSK
Syma	Symax/YD717	FHSS/-	Nordic Semiconductor NRF24L01	GFSK
Tactic	AnyLink SLT	FHSS	Nordic Semiconductor NRF24L01	GFSK
Hitec	AFHSS	FHSS	Texas Instruments CC2500	GFSK
Graupner	HoTT	FHSS	Texas Instruments CC2500	GFSK
FrSky	ACCST	FHSS	Texas Instruments CC2500	GFSK
JR	DMSS	FHSS,DSSS	Texas Instruments CC2520	O-QPSK
Yuneec	ZigBee	DSSS	Texas Instruments CC2530	-
DJI	OcuSync, LightBridge	FHSS, OFDM	-	-

taa olla useita protokollia ja niistä kehitetään jatkuvasti uusia versioita. Tietoja on pyritty keräämään luotettavista lähteistä, mutta tuotesalaisuuksien takia valmistajat ilmoittavat hyvin vähän tarkempia tietoja laitteistaan. Myöskin laitteiden takaisinmallinnus voi olla haastavaa, joten saatavilla olevat tiedot vaihtelevat hyvin paljon. Protokollat voivat erota toisistaan monella eri tapaa, mutta tässä työssä keskitytään erityisesti protokollien käyttämiin hajaspektritekniikoihin. Suurin osa protokollista perustuu joko pelkästään FHSS-tekniikkaan tai sen ja DSSS:n hybriditekniikkaan. Myöskin eri valmistajien FHSS-tekniikat voivat vaihdella monella tapaa, kuten mainittiin luvussa 2.4.2.

Tyypillisesti valmistajat käyttävät laitteissaan yleisiä kaupallisiin tarkoituksiin valmistettuja yksinkertaisia radiopiirejä, koska ne ovat hyvin edullisia. Yleisiä radiopiirejä on rajoitetusti markkinoilla, joten moni valmistaja käyttää laitteissaan samoja radiopiirejä. Käytettävä radiopiiri asettaa rajaehdot protokollalle, joten samaa radiopiiriä käyttävät protokollat ovat yleensä hyvin samankaltaisia. Radiopiiri voi tukea esimerkiksi vain FHSS-tekniikkaa, vain DSSS-tekniikkaa tai molempia. Lisäksi radiopiiri määrittelee, paljonko kanavia voidaan käyttää, kuinka nopeasti lähetin asettuu uudelle taajuudelle, miten data moduloidaan kantoaaltoon, sekä paljon muita ominaisuuksia. Seuraavissa aliluvuissa on esitelty muutamia yleisimpiä lennokkien käyttämiä radiopiirejä, niiden tärkeimpiä ominaisuuksia, sekä niitä käyttäviä protokollia.

2.5.1 Amiccom A7105/A7106

Amiccom A7105 ja A7106-radiopiirit ovat lähes identtiset. Radiopiirit tukevat nopeaa (130 µs) taajuuden asettumisaikaa sekä teoriassa jopa 255 kanavaa, mitkä mahdollistavat FHSS:n käytön. Radiopiirit käyttävät FSK/GFSK-modulaatiota ja niiden tiedonsiirtonopeus on asetettavissa 2 – 500 Kbps:n välillä. Näitä radiopiirejä käyttävät muun muassa FlySkyn AFHDS-protokolla sekä Hubsanin X4-protokolla. [26, 27]

Hubsanin X4-protokolla ei käytä hajaspektritekniikkaa, vaikka radiopiiri sitä tukee. Protokolla käyttää 12 kanavaa, joita lähetin aluksi kuuntelee ja valitsee niistä kanavan, jolla on vähiten interferenssiä eli vastaanotettu teho on pienin. Lähetin ja vastaanotin pysyvät kyseisellä kanavalla, kunnes ne käynnistetään uudelleen. [45] FlySkyn AFHDS-protokollia käsitellään tarkemmin luvussa 4.1.

2.5.2 Cypress CYRF6936

Cypressin CRYF6936-radiopiiri tukee DSSS- ja FHSS-tekniikkaa. Radiopiiri tukee pelkällä GFSK-modulaatiolla 1 Mbps:n tiedonsiirtonopeutta ja DSSS-tekniikalla maksimissaan 250 kbps:n tiedonsiirtonopeutta. Radiopiiriä käytetään muun muassa Airtronicsin, Walkeran ja Spectrumin protokollissa. [30]

Spectrumin ensimmäinen DSM-protokolla (engl. Digital Spectrum Modulation) käyttää DSSS-tekniikkaa ja vain yhtä taajuutta lähetykseen. Kun lähetin käynnistetään se kuuntelee käytössä olevaa taajuuskaistaa ja valitsee 79 kanavan joukosta kanavan, jossa ei ole muita lähetyksiä eli interferenssi on tarpeeksi pieni. Spectrumin uudempi DSM2-protokolla on yhteensopiva DSM-protokollan kanssa ja se käyttää DSSS-tekniikan lisäksi FHSS-tekniikkaa. Kun lähetin käynnistetään, se valitsee kaksi kanavaa 79 kanavan joukosta, joilla ei ole muita lähetyksiä ja vaihtelee niitä jatkuvasti. Valmistajan uusin DSMX-protokolla on yhteensopiva DSM2-protokollan kanssa ja hyödyntää myös DSSS-tekniikkaa, mutta kahden "satunnaisen" kanavan sijasta käyttää 23 kiinteän kanavan FHSS-tekniikkaa, jossa kanavat ja hyppysekvenssi valitaan 79 kanavan joukosta laitteen sarjanumeron perusteella. [43, 21, 30, 44]

2.5.3 Micro Linear ML2724/ML2730

Micro Linearin ML2724- ja ML2730-radiopiirit tukevat DSSS- sekä FHSS-tekniikkaa. Radiopiirit ovat samankaltaisia, mutta ML2730 tarjoaa hieman enemmän ominaisuuksia kuin ML2724. Kyseisiä radiopiirejä käytetään Futaban uudemmissa FASST- ja FASSTest-protokollissa (engl. Futaba Advanced Spread Spectrum Technology), kun taas vanhemmat S-FHSS- ja T-FHSS-protokollat käyttävät Texas Instrumentsin CC2500-radiopiiriä. Futaban FASST-protokolla käyttää 36 kanavaa, joita se hyppii joko seitsemän tai kahdeksan millisekunnin välein ja FASSTest-protokolla käyttää puolestaan 22 kanavaa, joita se hyppii joko 6,3 ms:n tai 15 ms:n välein. [28, 29, 40]

Myöskin DJI käyttää vanhemmissa lennokeissaan Futaban FASST-protokollaa, jota DJI nimittää DESST-protokollaksi (DJI Enhanced Spread Spectrum Technology) [39, 41]. DJI:n uudemmat mallit käyttävät kuitenkin OcuSync- tai LightBridge-protokollaa, jotka radio-ohjauksen lisäksi tarjoavat videolinkin lennokista maahan. OcuSync- ja Lightbridge-protokollat käyttävät OFDM-tekniikkaa videolinkkiin ja FHSS-tekniikkaa ohjaukseen. OcuSync- ja Lightbridge-protokollat käyttävät kehittyneempiä radiopiirejä, jotka mahdollistavat vapaamman määrittelyn protokollalle verrattuna muihin radiopiireihin. [39, 42]

2.5.4 Nordic Semiconductor NRF24L01

Nordic Semiconductorin NRF24L01-radiopiiri on hyvin yleinen ja edullinen radiopiiri. Radiopiiri käyttää GFSK-modulaatiota ja datanopeudeksi voidaan valita joko 1 Mbps tai 2 Mbps ja radiopiirin uudempiversio NRF24L01+ tukee myös 250 kbps:n datanopeutta. Radiopiiri tukee nopeaa taajuuden asettumisaikaa $(130\,\mu s)$ ja 126 kiinteätä kanavaa, jotka mahdollistavat FHSS-tekniikan käytön. [34]

Radiopiiriä käyttää hyvin monet valmistajat, kuten Bayang, Cheerson, Eachine, HiSky, Syma, Tactic ja monet muut kiinalaiset valmistajat. Radiopiiriä käytetään erityisesti edullisissa lennokeissa. Useat radiopiirin protokollat käyttävät neljän kanavan FHSS-tekniikkaa, mutta esimerkiksi YD717 protokolla käyttää vain yhtä kiinteää kanavaa lähetykseen. [25]

2.5.5 Texas Instruments CC2500/CC2520/CC2530

Texas instrumentsin CC2520 ja CC2530 ovat IEEE 802.15.4-standardin mukaisia radiopiirejä, jotka tukevat etenkin standardin mukaista DSSS-tekniikkaa, kun taas CC2500 on yleinen ja edullinen 2,4 GHz:n radiopiiri, joka tukee vain FHSS-tekniikkaa. Texas instrumentsin CC2500 käytetään ainakin FrSkyn, Graupnerin ja HiTecin protokollissa sekä Futaban vanhemmissa S-FHSS- ja T-FHSS-protokollissa. [32, 31, 33, 24, 21]

Entinen Japan Remote Control (JR), jonka toiminta on siirtynyt Konishi Mokei-yritykselle, käytti vanhemmissa laitteissaan Spectrumin DSM-protokollaa, mutta uudemmissa laitteissa käytetään Texas instrumentsin CC2520-radiopiiriä ja JR:n omaa DMSS-protokollaa (engl. Dual Modulation Spectrum System). Kyseinen protokolla käyttää hybriditekniikkaa ja 23 taajuushyppelevää kanavaa. [36] Texas instrumentsin uudempaa CC2530-radiopiiriä käytetään muun muassa Yuneecin lennokeissa, jotka käyttävät IEEE 802.15.4 mukaista ZigBee-protokollaa [16].

3. RADIOLAITTEIDEN HÄIRINTÄMENETELMÄT

Radiohäirinnän tarkoituksena on vaikeuttaa tai estää kohteen sähkömagneettisen spektrin käyttöä ja häirintä kohdistetaan aina radiovastaanottimiin. [46] Yksinkertainen häirintä näkyy vastaanottimelle yleensä kohinatason nousuna. Tällöin bittivirheiden todennäköisyys vastaanottimessa kasvaa ja vastaanottimen on vaikeampi tulkita hyötysignaalia. Kasvatettaessa häirintäsignaalin tehoa bittivirheiden todennäköisyys kasvaa lopulta niin suureksi, että radioyhteys katkeaa. [18]

Seuraavissa alaluvuissa käydään läpi häirintätekniikoita improvisoitujen räjähteiden ja kauko-ohjattavien lennokkien torjunnassa sekä pohditaan full-duplexin hyödyntämistä häirinnässä. Lisäksi perehdytään häirinnän tehokkuuden analyysiin sekä esitellään myös lyhyesti muutamia kaupallisia häirintälaitteita.

3.1 Häirintätekniikat

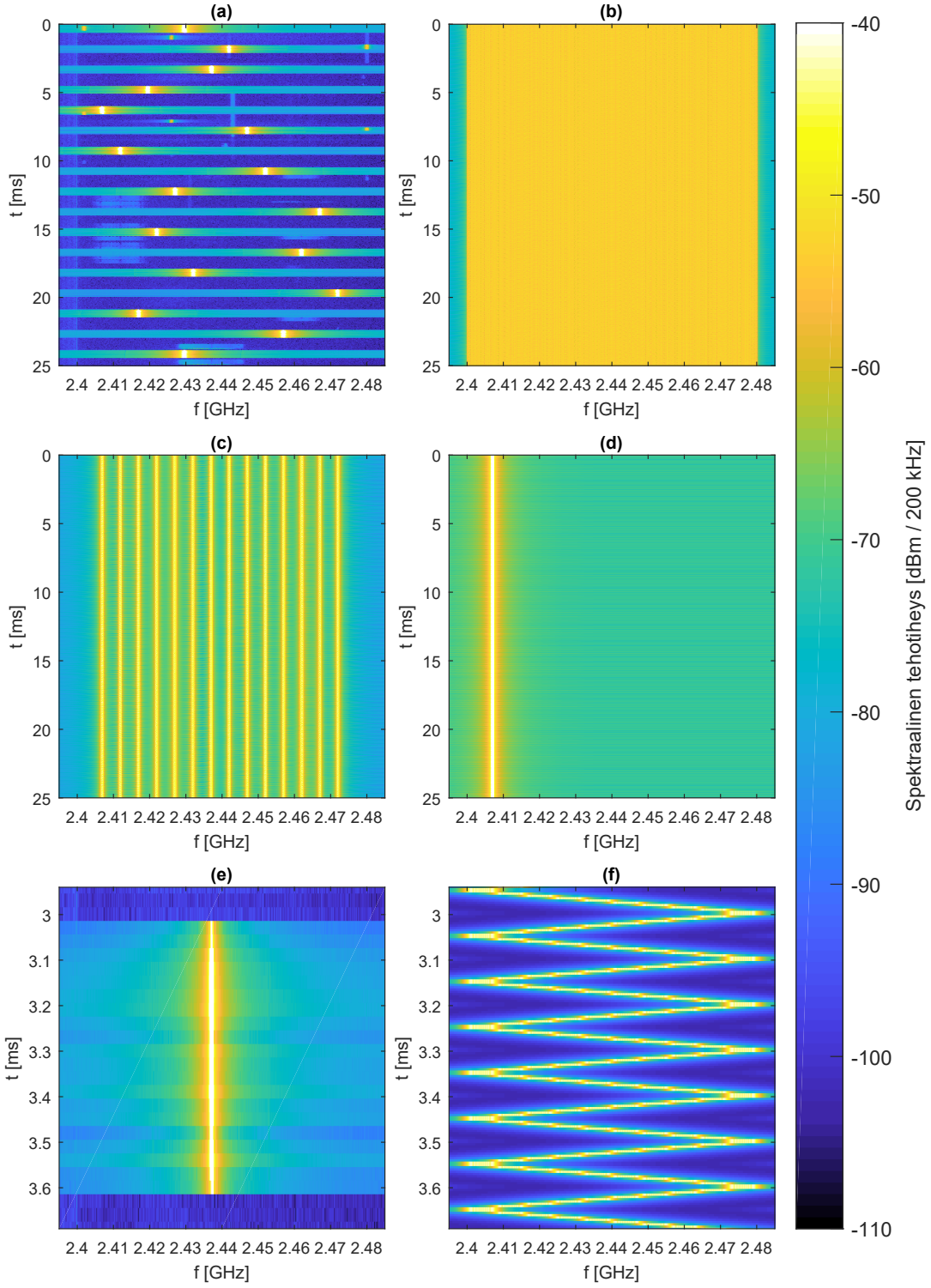
Radiohäirintätekniikoita on useita ja niiden toimivuus riippuu olennaisesti siitä, kuinka hyvin ne on sovitettu kohteen radioprotokollaan. Häirintä on yleensä tehokkaampaa, mitä enemmän häirintäsignaalin tehosta osuu hyötysignaaliin aika- ja taajuustasossa. [47] Yleisimpiä häirintätekniikoita on esitelty tarkemmin seuraavissa alaluvuissa.

Koska suurin osa lennokkien radio-ohjausjärjestelmistä käyttää FHSS-tekniikkaa, keskitytään myös seuraavaksi käsiteltävissä häirintätekniikoissa sen häirintään. Häirintätekniikat ovat kuitenkin yleispäteviä ja niitä voidaan soveltaa yhtä hyvin muitakin järjestelmiä, kuten esimerkiksi radio-ohjattavia improvisoituja räjähteitä vastaan. Tekniikoiden vertailussa on käytetty signaalien spektrogrammikuvia, jotka näkyvät kuvassa 5. Kuvassa 5 (a) näkyy kokeellisessa osuudessakin käytettävän kohteen FHSS-signaalin spektrogrammi. Kuvissa 5 (b, c, d ja f) näkyvät häirintäsignaalit, joiden keskimääräinen teho on yhtä suuri kuin kuvassa 5 (a) mitatun FHSS-signaalin keskimääräinen teho. Kuvassa 5 (e) näkyy sama FHSS-signaali, mutta rajattuna samaan aikaskaalaan kuvan 5 (f) kanssa.

3.1.1 Laajakaistahäirintä

Yksinkertaisin häirintätekniikka on jatkuva yhtenäinen laajakaistahäirintä (engl. barrage jamming). Häirintäsignaali on yleensä kohinaa muistuttava signaali, joka levittyy tasaisesti koko käytettävälle taajuuskaistalle. Kohteelle laajakaistahäirintä näkyy taustakohinan kasvuna. [18]

Kuvassa 5 (b) näkyy laajakaistasignaalin spektrogrammi. Laajakaistahäirinnällä on huono energiatehokkuus, koska häirintäsignaalin teho on jatkuvaa sekä levittynyt koko käytettävälle taajuuskaistalle [18]. Verrattaessa laajakaistasignaalia kuvassa 5 (a) näkyvään



Kuva 5. *FHSS-signaalin (a & e) sekä häirintäsignaalien (b, c, d & f) spektrogrammit*

kohteen FHSS-signaaliin, nähdään, kuinka suurin osa laajakaistahäirinnän tehosta on taajuuksilla ja ajanhetkillä, joita kohteen FHSS-signaali ei käytä.

Laajakaistahäirintää ei voida myöskään kohdistaa tiettyyn vastaanottimeen vaan se vaikuttaa yhtäläisesti kaikkiin taajuuskaistalla toimiviin laitteisiin. Tällöin häirinnällä voidaan esimerkiksi menettää myös omien radioyhteyksien toiminta. [47] Jatkuvan laajakaistahäirinnän huonona puolena on myös erittäin helppo havaittavuus spektristä [49]. Jatkuva laajakaistainen häirintäsignaali on kuitenkin tehokkain häirintämenetelmä, jos ei tiedetä mitään kohteen käyttämästä signaalista [47].

3.1.2 Kanavahäirintä

Kanavahäirintä tai kapeakanavahäirintä (engl. tone jamming) tarkoittaa hyvin kapeakaistaista jatkuvaa häirintää ja voi sisältää joko yhden tai useamman kanavan, joilla samanaikaisesti lähetetään häirintäsignaalia [18]. FHSS-tekniikan torjunnassa yhdellä häirintäkanavalla voidaan häiritä yhtä FHSS-kanavaa, kahdella kahta ja niin edelleen, mutta vain jos tiedetään, mitä taajuuksia FHSS-järjestelmä käyttää [47].

Kuvassa 5 (d) näkyy yksikanavainen häirintäsignaali, joka on kohdistettu yhdelle FHSS-järjestelmän kanavalle. Yhden kanavan häirinnällä saavutetaan paljon suurempi häirinnän tehotiheys kyseiselle FHSS-järjestelmän kanavalle, verrattuna kuvan 5 (b) laajakaistahäirintään. FHSS-järjestelmä voi kuitenkin edelleen toimia muilla kanavilla normaalisti, joten yhden kanavan häirinnällä ei saavuteta yleensä merkittävää vaikutusta FHSS-järjestelmiä vastaan.

Häirintänä voidaan käyttää myös monikanavahäirintää, kuten nähdään kuvassa 5 (c), jossa häirintäsignaali on kohdistettu FHSS-järjestelmän käyttämille kanaville. Häirintäsignaalin tehotiheys FHSS-signaalin käyttämillä kanavilla on noin kymmenkertainen laajakaistahäirintään verrattuna. Tällöin yhtä tehokkaan häirinnän saavuttamiseksi voidaan käyttää paljon pienempiä häirintätehoja. Häirintäsignaalissa käytetään vain 14 taajuuskanavaa, koska käytettävässä järjestelmässä vastaanotin ei käytä kahta taajuutta, joita lähetin käyttää.

Ajallisesti monikanavahäirintä on silti energiatehoton FHSS-signaalin torjunnassa. Tämä johtuu siitä, että monikanavahäirintäsignaali lähettää jatkuvasti häirintäsignaalia kaikilla kanavilla, kun taas kyseinen FHSS-järjestelmä käyttää yhtä kanavaa noin 0,6 ms ja palaa samalle kanavalle vasta noin 24 ms:n kuluttua, eli koko ajasta se käyttää yhtä kanavaa vain noin 2,5 %.

3.1.3 Pyyhkäisyhäirintä

Pyyhkäisyhäirinnällä (engl. sweep jamming) tarkoitetaan kapeakaistaista häirintäsignaalia, joka pyyhkäistään jatkuvasti laajakaistaisen taajuusalueen läpi. Pyyhkäisyhäirinnän

tärkeimpänä parametrina on pyyhkäisynopeus, joka vaikuttaa merkittävästi häirinnän tehokkuuteen. Pyyhkäisyhäirintä osuu jokaisella pyyhkäisyllä FHSS-signaaliin, kunhan pyyhkäisynopeus on suurempi kuin FHSS-signaalin hyppynopeus. Pyyhkäisynopeutta ei voida kasvattaa kuitenkaan liian suureksi, ettei kanavan päällä vietettävä aika laskisi niin pieneksi, että häirinnän tehokkuus laskee [18].

Kuvassa 5 (f) näkyy edestakainen pyyhkäisyhäirintäsignaali, joka on pyritty sovittamaan käytettävän FHSS-järjestelmän torjuntaan. Häirintäsignaalin pyyhkäisynopeus on noin 20000 pyyhkäisyä sekunnissa eli noin 30-kertainen verrattuna FHSS-järjestelmän hyppynopeuteen (675 hyppyä/sekunti). Verrattaessa häirintäsignaalia kuvassa 5 (e) näkyvään FHSS-signaalin yhteen kehykseen, nähdään kuinka häirintäsignaali pyyhkäisee FHSS-signaalin kehyksen päältä noin 11 kertaa kyseisen kanavan päälläoloaikana.

Pärlinin diplomityössä [23] on simuloitu eri pyyhkäisynopeuksilla häirintää hybridi-järjestelmää vastaan ja todettu kymmenkertaisen pyyhkäisynopeuden suhteessa järjestelmän hyppynopeuteen olevan tehokkain. Koska eri FHSS-järjestelmien ominaisuudet vaihtelevat hyvin paljon, myös paras pyyhkäisynopeus eri järjestelmien torjunnassa vaihtelee, joten tehokkaan häirinnän saavuttamiseksi on laskennallisesti, simuloimalla tai kokeellisesti selvitettävä paras pyyhkäisynopeus kohteen järjestelmää vastaan [23].

3.1.4 Reaktiivinen häirintä

Reaktiivisella häirinnällä tarkoitetaan ajallisesti kohteen signaaliin synkronoitua häirintää. Reaktiivisessa häirinnässä ei välttämättä tarvitse tietää kohteen protokollaa, mutta järjestelmässä on oltava vastaanotin, jolla pystytään kuuntelemaan kohteen signaaleita. [47] Reaktiivinen järjestelmä yleensä kuuntelee taajuuskaistaa jatkuvasti ja pyrkii reagoimaan kohdesignaalin muutoksiin mahdollisimman nopeasti.

Järjestelmä voi esimerkiksi tutkia vastaanotettua spektriä ja havaitessaan energian kasvun jollain taajuudella, se pyrkii tunnistamaan, onko kyseessä kohteen FHSS-signaali. Järjestelmän tunnistaessa kohteen FHSS-signaalin, se voi aloittaa häirinnän kyseisellä kanavalla. Havaitessaan puolestaan energian laskun häirittävällä kanavalla, se voi lopettaa häirinnän kyseisellä kanavalla ja pyrkiä löytämään kanavan, jolle FHSS-signaali seuraavaksi hyppää. [18]

Suurin haaste reaktiivisessa häirinnässä on ajoitus. Järjestelmän pitää pystyä nopeasti havaitsemaan kohdesignaali ja aloittaa häirintä kyseisellä taajuudella. Ajoitukseen vaikuttaa myös se, pystytäänkö kuuntelemaan ja häiritsemään samaa taajuuskaistaa yhtä aikaa vai joudutaanko häirintää ja kuuntelua vuorottelemaan ajallisesti. Luvussa 3.2 kerrotaan tarkemmin full-duplex-järjestelmästä, joka mahdollistaa yhtäaikaisesti taajuuskaistan kuuntelun sekä häirinnän.

Reaktiivisella häirinnällä voidaan säästää huomattavasti energiaa, jos kohdejärjestelmä ei käytä häirittävää kanavaa jatkuvasti [49]. Esimerkiksi luvussa 3.1.2 monikanavahäirintä-

signaalilla häirittiin jatkuvasti kaikkia kanavia, vaikka FHSS-signaali pysyi yhdellä kanavalla vain 2,5 % lähetyksestä. Tällöin häiritsemällä kanavia vain se aika milloin kohde käyttää niitä, voitaisiin ideaalisella reaktiivisella häirinnällä saavuttaa jopa 40-kertainen tehokkuus verrattuna monikanavahäirintään. Lisäksi käyttämällä tehokkaammin spektriä häirinnän havainnointi on vaikeampaa ja samalla voidaan vähentää muiden samalla taajuuskaistalla toimivien laitteiden häirintää. Käytännössä järjestelmissä on kuitenkin viiveet, minkä ajan kuluttua signaali pystytään havaitsemaan ja minkä ajan kuluttua häirintä pystytään aloittamaan.

Reaktiivinen häirintä voi olla myös adaptiivista, jolloin järjestelmä voi esimerkiksi kuunnella taajuuskaistaa ja pyrkiä tunnistamaan kohteen FHSS-järjestelmän käyttämät kanavat, hyppysekvenssin ja hyppynopeuden. Tunnistettuaan FHSS-järjestelmän parametrit, se voi synkronoitua kohdejärjestelmän FHSS-signaaliin ja aloittaa häiritsemään kohteen hyppysekvenssin ja hyppynopeuden mukaan kohteen käyttämiä taajuuksia. [48] Jos järjestelmä ei kykene ajallisesti pysymään FHSS-signaalin perässä, voidaan adaptiivisessa häirinnässä käyttää monikanavahäirintää, kun kohteen käyttämät kanavat on tunnistettu. Koska lennokkien ohjaukseen käytettävissä protokollissa FHSS-tekniikan parametrit ovat yleensä kiinteitä eivätkä vaihdu, riittäisi adaptiivisessa häirinnässä aluksi kyseisen järjestelmä tunnistaminen, jonka jälkeen voidaan käyttää samoja parametrejä koko häirinnän ajan. Adaptiivisen häirinnän etuna normaaliin reaktiiviseen häirintään verrattuna on helpompi synkronointi kohdejärjestelmään, koska tiedetään mihin taajuudelle ja milloin järjestelmä hyppää.

3.1.5 Protokollatietoinen häirintä

Protokollatietoisessa häirinnässä tiedetään kohdejärjestelmän käyttämä protokolla tai osa siitä ja käytetään tietoja hyväksi häirinnässä [47]. Protokollatietoista häirintää on tutkittu paljon WLAN-verkkojen torjunnassa [47–51]. Sillä voidaan saavuttaa paljon suurempi häirintätehokkuus kohdistamalla häirintä älykkäästi kohdesignaalin heikkouksiin. Tällöin voidaan myös minimoida häirinnän vaikutus muihin kuin kohdejärjestelmään sekä vähentää häirintäsignaalin havaittavuutta [49].

Lennokkien tapauksessa heikkoutena voidaan hyödyntää esimerkiksi järjestelmissä usein käytettyä CRC-tarkistussummaa (engl. cyclic redundancy check), jota käytetään tarkistamaan onko vastaanotetussa datapaketissa virheitä. Lähetettäessä datapakettia sen biteistä lasketaan CRC-summa, joka lähetetään datan perässä. Vastaanotin laskee vastaavasti CRC-summan vastaanotetuista biteistä. Jos yksi tai useampi bitti on vaihtunut myöskin CRC-numerot todennäköisesti eroavat toisistaan, jolloin datapaketti useimmiten hylätään. Tällöin häirintä voitaisiin kohdistaa vain muutamaan databittiin tai vastaavasti CRC-bitteihin, joiden ollessa virheellisiä, vastaanotin hylkää paketin. Häiritsemällä jokaista lähetettyä pakettia vastaavasti, vastaanotin joutuisi hylkäämään kaikki paketit [49].

Jos tiedetään kohteen käyttämä protokolla ja käytetään hyväksi reaktiivista häirintää, voidaan toimia adaptiivisen häirinnän tavoin, mutta hypätä tunnistusvaiheen ohi suoraan

häirintävaiheeseen. Häirintäsignaaliin voidaan myös moduloida kohinan sijasta kohteen käyttämiä paketteja, joilla pyritään vaikuttamaan kohteen toimintaan. Kohteen toimintaan vaikuttamista matkimalla kohteen protokollaa kutsutaan huijaushäirinnäksi (engl. spoofing). [47] Huijaushäirinnällä on mahdollista kaapata kohdejärjestelmä. Lennokkien tapauksessa voidaan lähettää oikeita ohjaukseen käytettäviä komentoja ja pakottaa kohde laskeutumaan. Jotta pystyttäisiin kaappaamaan kohdejärjestelmä, on kohteen vastaanottimessa häirintäsignaalin tehotason oltava suurempi kuin kohteen oman lähettimen signaalin tehotaso. Lisäksi häirintäsignaalin on oltava kohteen protokollan mukainen ja oikein ajoitettu.

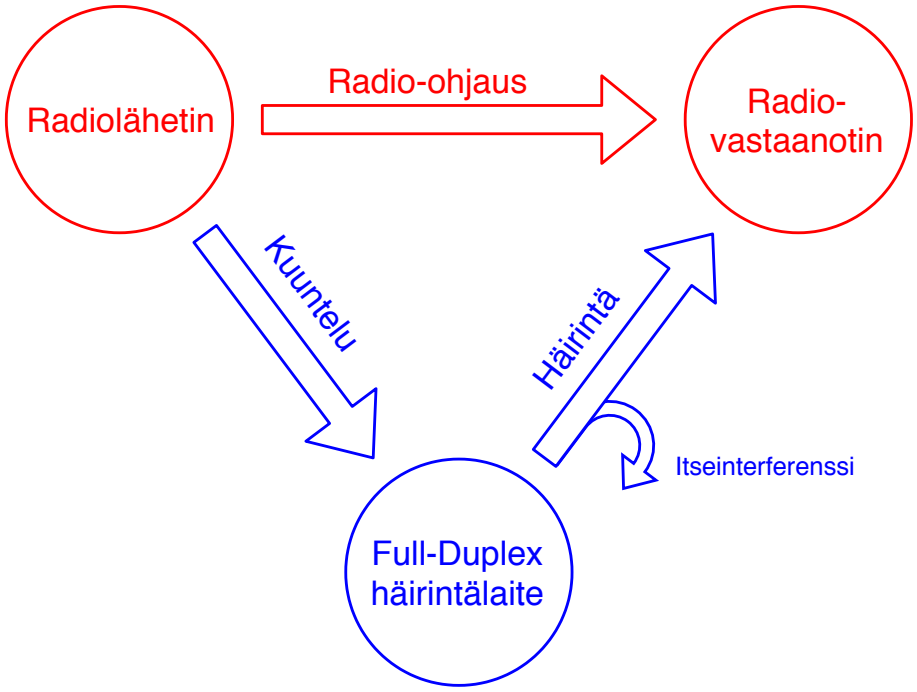
Protokollatietoisen häirinnän haasteina ovat kohdesignaaliin tarkka synkronoituminen sekä kohdejärjestelmästä vaadittava tarkka tietämys, varsinkin jos halutaan kaapata kyseinen järjestelmä [23, 44]. Lisäksi jos halutaan tehdä yleispätevä häirintälaite, joka esimerkiksi tunnistaa kohteen ja käyttää sitä vastaan protokollatietoista häirintää, pitäisi järjestelmän tuntea useita protokollia. Kuten luvussa 2.5 mainittiin, jo pelkästään lennokkien ohjauksessa käytetään hyvin paljon erilaisia protokollia. Lisäksi protokollista on hyvin vähän tietoa saatavilla, koska valmistajat eivät paljasta tietoja ja laitteiden takaisinmallinnus voi olla hyvin työlästä. Tästä syystä eri protokollia käyttävien kohteiden kaappaukseen tarkoitetun laitteen suunnittelu ja toteutus voi olla haastavaa, vaikka teoriassa mahdollista.

3.2 Full-duplexin hyödyntäminen häirinnässä

Full-duplexilla tarkoitetaan tiedonsiirtotekniikkaa, jossa vastaanotetaan sekä lähetetään signaalia samanaikaisesti. Sillä voidaan viitata taajuusjaettuun full-duplex-järjestelmään, joka lähettää ja vastaanottaa signaaleita samanaikaisesti, mutta eri taajuuskaistoilla. Tässä työssä tarkoitetaan kuitenkin full-duplexilla järjestelmää, joka lähettää ja vastaanottaa signaaleita saman aikaisesti samalla taajuuskaistalla (engl. in-band full-duplex). Full-duplex järjestelmässä täytyy käyttää itseinterferenssin kansellointia eli vastaanotetusta signaalista poistetaan oma lähetetty signaali, jotta lähetetty signaali ei häiritse signaalien vastaanottamista. [52]

Full-duplex-järjestelmää voitaisiin käyttää esimerkiksi kuvan 6 skenaariossa, jossa järjestelmä kuuntelee samanaikaisesti samalla taajuudella kohteen radio-ohjaus signaalia sekä häiritsee kohteen vastaanotinta [53, 54, 55]. Full-duplex järjestelmällä voidaan saavuttaa huomattava etu esimerkiksi reaktiivisissa ja protokollatietoisissa häirintäjärjestelmissä, koska lähetettävä häirintäsignaali voitaisiin synkronoida kohdejärjestelmään samanaikaisesti vastaanotettavan radio-ohjaussignaalin avulla. Jos häiritään esimerkiksi FHSS-signaalin yhtä kanavaa ilman full-duplexia, ei voida tietää, onko kohde jo vaihtanut kanavaa keskeyttämättä häirintää.

Myöskin adaptiivisessa häirinnässä voitaisiin hyödyntää full-duplex-järjestelmää häiritsemällä kohdetta esimerkiksi laajakaistahäirinnällä, kunnes kohteen signaali on tunnistettu,



Kuva 6. *Full-Duplexin hyödyntäminen radiohäirinnässä*

jonka jälkeen voidaan vaihtaa tehokkaampaan häirintään, kuten monikanavahäirintään tai ideaaliseen reaktiiviseen häirintään. Kyseisestä sovelluksesta olisi hyötyä etenkin improvisoitujen räjähteiden torjunnassa, jossa kohteen vastaanotin on luultavasti jo vastaanottanut räjäytyskäskyn, kun häirintälaite vasta analysoi kohteen käyttämää radioprotokollaa.

3.3 Häirinnän tehokkuuden analyysi

Jotta pystytään arvioimaan häirinnän toimivuutta, tarvitaan tietoa vastaanotetun signaalin laadusta. Vastaanotetun signaalin tehoa kuvataan RSSI:llä (engl. received signal strength indication), joka on summa kaikesta vastaanottimen vastaanottamasta tehosta. Paremmin signaalin laatua kuvaa signaali–kohinasuhde eli SNR (engl. signal-to-noise ratio), joka voidaan esittää kaavalla

$$SNR = \frac{P_S}{P_N}, \tag{6}$$

jossa P_S on hyötysignaalin teho ja P_N kohinateho. Suure SINR (engl. signal-to-interference-plus-noise ratio) on vastaava, mutta se ottaa huomioon myös interferenssiä aiheuttavien signaalien, kuten häirintäsignaalin tehon P_J [56]

$$SINR = \frac{P_S}{P_J + P_N}. \tag{7}$$

Häirinnän tehokkuutta kuvataan yleensä suureella JSR (engl. jam to signal ratio), joka kuvaa häirintäsignaalin tehoa suhteessa hyötysignaaliin:

$$JSR = \frac{P_J}{P_S}. \tag{8}$$

Häirintäsignaalin tehokkuus JSR mitataan aina vastaanottimesta. Useimmissa häirintätapauksissa vastaanotetun häirintäsignaalin teho P_J on paljon suurempi verrattuna vastaanotettuun kohinatehoon P_N. Tällöin JSR vastaa SINR:in käänteisarvoa. [18]

Signaalin laatua voidaan kuvata myös bittivirhesuhteella BER (engl. bit error ratio), joka kuvaa virheellisten bittien määrää suhteessa lähetettyihin bitteihin. Pakettivirhesuhde PER (engl. packet error ratio) kuvaa puolestaan virheellisten pakettien määrää vastaanottimessa suhteessa lähetettyihin paketteihin.

Eri järjestelmillä on eri raja-arvot bittivirheiden ja pakettivirheiden sietämisessä, riippuen niiden virheenkorjausmenetelmistä ja järjestelmävaatimuksista. Tämän vuoksi BER ja PER on yleisesti käytetty arvioimaan häirinnän tehokkuutta. Häirintä katsotaan yleensä onnistuneeksi, kun BER tai PER nousee järjestelmän raja-arvoa suuremmaksi. Yleensä 10^{-2} tai suurempi BER-arvo riittää onnistuneeseen häirintään, mutta arvo riippuu paljon järjestelmästä [18].

Signaalin modulointi yleensä määrittää, millä SINR:in arvolla järjestelmä voi vastaanottaa signaalin tietyllä BER arvolla. Tästä johtuen järjestelmän käyttämä modulaatio vaikuttaa suoraa siihen, kuinka suuri JSR-arvo vaaditaan saavuttamaan tietty BER arvo. Esimerkiksi BPSK:n tapauksessa vaaditaan vähintään -8,9 dB:n JSR-arvo, jotta saavutettaisiin 10^{-2} BER-arvo. [18] Puolestaan siihen, kuinka suuri JSR-arvo saavutetaan tietyllä häirintäsignaalin lähetysteholla, vaikuttaa se, kuinka hyvin häirintäsignaali on sovitettu kohteen signaaliin aika- ja taajuustasossa ja paljonko kohteen lähettämä hyötysignaali sekä lähetetty häirintäsignaali vaimentuvat edetessään lähettimiltä vastaanottimelle.

Signaalin vaimenemiseen vaikuttaa moni asia, mutta sitä voidaan arvioida esimerkiksi vapaan tilan vaimennusmallilla:

$$\frac{P_L}{P_V} = \left(\frac{4\pi f l}{c}\right)^2, \tag{9}$$

jossa P_L on lähetetty teho, P_V vastaanotettu teho, f käytetty taajuus, c valonnopeus ja l etäisyys [56]. Vapaan tilan vaimennusmallista voidaan ratkaista, paljonko etäisyys muuttuu suhteessa lähetetyn tehon muutokseen, jos vastaanotettu teho pidetään samana:

$$\frac{l_2}{l_1} = \sqrt{\frac{P_2}{P_1}}, \tag{10}$$

jossa P_2 on uusi lähetysteho, P_1 vanha lähetysteho, l_2 uusi etäisyys ja l_1 vanha etäisyys. Esimerkiksi tehon kaksinkertaistuessa saavutetaan noin 40 % pidempi kantama.

Häirintäsignaalien sovitusta kohteen signaaliin voidaan arvioida esimerkiksi vertailemalla signaalien spektrejä. Kuvassa 5 (a) näkyy kohteen FHSS-signaalin mitattu spektri ja kuvissa 5 (b, c, d ja f) eri häirintäsignaalien spektrit. Signaalien keskimääräiset tehot ovat yhtä suuria, joten jos spektrit olisivat kohteen vastaanottimen mittaamia, voisi tilanne vastata asetelmaa, jossa kohteen oma lähetin ja häirintälähetin ovat yhtä kaukana kohteen vastaanottimesta ja lähettävät signaalia samalla teholla.

Kohteen FHSS-signaali käyttää 16 kanavaa, joilla se viipyy jokaisella noin 0,6 ms. Signaalin käyttämät kanavat ovat 500 kHz:n levyisiä. Kuvan 5 (b) laajakaistahäirintäsignaali puolestaan käyttää jatkuvasti 80 MHz:n taajuuskaistaa, jolloin hyötysignaalin sekä häirintäsignaalin keskimääräisten tehojen ollessa yhtä suuret, laajakaistahäirinnällä saavutetaan vain noin -26 dB:n JSR-arvo, joka todennäköisesti ei riittäisi tehokkaaseen häirintään.

Kuvan 5 (c) monikanavahäirintä on laajakaistahäirinnän tapaan jatkuvaa, mutta taajuustasossa teho on kohdistettu FHSS-signaalin kanaville. Häirintäsignaalissa käytetään vain 14 häirintäkanavaa, koska käytettävä vastaanotin ei sattumoisin käytä kahta taajuutta, joita lähetin käyttää. Kanavat ovat kuitenkin hieman leveämpiä kuin FHSS-signaalin kanavat, jolloin taajuustasossa teho on levittäytynyt lähes yhtä suurelle alueelle kuin FHSS-signaalilla. Tällöin FHSS-signaalin käyttämillä kanavilla saavutetaan noin -16 dB:n JSR-arvo eli noin kymmenkertainen häirintäteho verrattuna laajakaistahäirintään. Jos käytetään vapaantilan vaimenemismallia, kymmenkertaisella teholla saadaan kaavan (10) avulla noin kolminkertainen kantama. Tällöin vapaassa tilassa monikanavahäirintäsignaalilla saavutetaan vielä kolme kertaa pidemmällä etäisyydellä sama häirintäteho FHSS-signaalin kanavilla kuin laajakaistahäirintäsignaalilla.

Kuvan 5 (d) yhden kanavan häirinnällä saavutetaan yhdelle kanavalle jopa -5 dB:n JSR-arvo, mutta muille kanaville häirintä on erittäin vähäistä. Kuvan 5 (f) pyyhkäisyhäirinnällä saavutetaan FHSS-paketin ajalta sama keskimääräinen teho kuin laajakaistahäirinnällä eli JSR-arvo on myös noin -26 dB, mutta hetkellinen teho on noin kymmenkertainen verrattuna laajakaistahäirinnän tehoon. Tällöin hetkellisesti voidaan saavuttaa jopa -16 dB:n JSR-arvo. Jos käytettäisiin puolestaan ideaalista reaktiivista häirintää, joka seuraa kohteen FHSS-signaalia ajassa sekä taajuudessa ja häirintäsignaalin keskimääräinen teho olisi edelleen yhtä suuri hyötysignaalin kanssa, saavutettaisiin 0 dB:n JSR-arvo, joka vaatisi kohdejärjestelmältä hyvin tehokasta modulointitapaa pystyäkseen toimimaan häirinnästä huolimatta. Ideaalisella adaptiivisella häirinnällä saavutettaisiin jopa 400-kertainen häirinnän tehokkuus laajakaistahäirintään verrattuna. Tällöin kaavan (10) mukaan saataisiin 20-kertainen kantama laajakaistahäirintään verrattuna.

3.4 Kaupalliset häirintälaitteet

Radiohäirintälaitteiden käyttö on yleensä laitonta yksityishenkilöille, mutta viranomaisille tai yrityksille häirintälaitteiden käyttö voi olla sallittua. Tämän vuoksi suurimmat häirintälaitteita markkinoivat yritykset toimivat yhteistyössä joko armeijan, muiden viranomaisten tai turvallisuusalan toimijoiden kanssa. Häirintälaitemarkkinat ovat suuressa nousussa ja laajentuvat eri aloille uusien tarpeiden mukaan. Varsinkin lennokkien lisääntynyt käyttö on lisännyt tarvetta häirintälaitteiden kehitykselle. [57] Vaikka häirintälaitteiden käyttö ja jopa niiden myyminen yksityishenkilöille on monissa maissa kielletty, niiden tarjonta on silti kasvanut markkinoilla. Kuluttajat pystyvät tilaamaan halpoja häirintälaitteita verkkokaupoista ja käyttämään niitä, ymmärtämättä niiden seurauksia [58].

Radiohäirintälaitemarkkinoiden johtavimpia yrityksiä on kerätty Technavionin tekemän

tutkimuksen perusteella taulukkoon 3 [57]. Taulukon yritykset toimivat kaikki armeijan, muiden viranomaisten tai turvallisuusalan toimijoiden kanssa ja kehittävät häirintälaitteita moniin eri sovelluksiin. Koska laitteiden käyttö on laitonta yksityishenkilöille, löytyy niistä hyvin rajoitetusti tietoa. Erilaisia häirintälaitteita kehittäviä ja markkinoivia yrityksiä on hyvin paljon ja seuraavaksi on käyty läpi muutamia eri yritysten häirintäjärjestelmiä, jotka on tarkoitettu lennokkien häirintään.

Taulukko 3. *Suurimmat yritykset radiohäirintälaitemarkkinoilla [57]*

Yritys	Maa
BAE Systems	Iso-Britannia
Northrop Grumman	Yhdysvallat
Raytheon	Yhdysvallat
HSS Development	Yhdysvallat
Harris Corporation	Yhdysvallat
Lockheed Martin	Yhdysvallat
MCTECH TECHNOLOGY	Yhdysvallat
Stratign FZE	Yhdistyneet arabiemiirikunnat
Israel Aerospace Industries	Israel
Wolves fleet Technology Co.	Kiina

Suomalaisella Sensofusion yrityksellä on lennokkien havainnointiin, häirintään ja kaappaukseen kehitetty järjestelmä Airfence 5.0. Yrityksen mukaan järjestelmän yksiköt ovat helposti skaalattavissa ja yksi yksikkö pystyy havaitsemaan lennokin jopa 10 kilometrin päästä. Järjestelmä voi hälyttää havaituista lennokeista esimerkiksi puhelimen ilmoituksella ja voidaan asettaa automaattisesti häiritsemään havaittuja lennokkeja. Lisäksi se pystyy reaaliajassa näyttämään havaittujen lennokkien sijainnin kartalla [59]. Tarkempia järjestelmän teknisiä tietoja ei ole saatavilla, kuten järjestelmän kokoa, tehoa tai käytettyjä häirintämenetelmiä.

Virolaisella Rantelon yrityksellä on monia erilaisia häirintälaitteita, kuten esimerkiksi "Drone Jamming Gun", joka näkyy kuvassa 7. Laite on pienikokoinen ja painaa alle kaksi kiloa. Laitteesta voidaan valita käytettäväksi sekä 2,4 GHz:ä että 5,8 GHz:ä taajuuskaista. Laitteessa käytetään suuntaavia jagiantenneja, joilla saavutetaan lähetyssuuntaan 12 dBi:n antennivahvistus verrattuna ympärisäteilevään antenniin. Laitteen käyttämä maksimilähetysteho on kummallekin taajuuskanavalle 20 W eli noin 43 dBm ja valmistajan mukaan laitteella voidaan saavuttaa toimiva häirintä jopa kilometrin päähän.

Yhdysvaltalainen Department 13 yritys on keskittynyt protokollatietoiseen lennokkien torjuntaan. Yrityksen kehittämä MESMER-järjestelmä perustuu protokollatietoiseen häirintään. Järjestelmä etsii lennokkeja kuuntelemalla eri taajuuskaistoja ja löydettyään lennokin se pyrkii ottamaan sen haltuunsa lähettämällä sille sen käyttämän protokollan mukaista signaalia. Järjestelmä on erityisesti suunniteltu toimivaksi pienillä lähetystehoilla, jotta sen käyttö olisi laillista. Yrityksen markkinointiesitteen mukaan MESMER v1.5 toi-

***Kuva 7**. Drone Jamming Gun PJ-2458 [60]*

mii 2,4 GHz:n, 5,8 GHz:n, 430 MHz:n, sekä 900 MHz:n taajuuksilla ja, että toimintasäde olisi jopa 4 kilometriä 2,4 GHz:n taajuuskaistalla alle yhden watin (30 dBm) lähetysteholla. Järjestelmän teknisistä tiedoista sekä toimivuudesta on saatavilla kuitenkin hyvin rajoitetusti tietoa ja luvatut toimintasäteet vaikuttavat liian optimistisilta häirintätehoon verrattuna. [61]

Häirintälaitemarkkinat ovat kasvussa ja häirintälaitteiden kehitykseen on sijoitettu viime aikoina paljon enemmän kuin ennen. Yksinkertaisten laajakaistahäirintä- ja kanavahäirintälaitteiden lisäksi kehitetään älykkäämpiä reaktiivisia ja protokollatietoisia häirintälaitteita eri sovelluksiin. [57] Älykkäässä häirinnässä kohteiden havainnointi on suuressa merkityksessä. Tulevaisuudessa häirintälaitteissa voitaisiin hyödyntää full-duplexia toteuttamaan yhtäaikaisesti havainnointia sekä häirintää [53, 54, 55].

4. HÄIRINNÄN TESTAAMINEN

Työn kokeellisessa osassa häirittiin improvisoidun räjähteen radio-ohjausta kahdella eri häirintäsignaalilla. Radiolaitteena hyödynnettiin HobbyKing-merkkisiä lennokkien ohjaukseen tarkoitettuja radiolaitteita (HK-T4A-V2 ja HK-TR6A-V2 [11]), jotka käyttävät FlySkyn AFHDS-protokollaa. Häirintäsignaaleina käytettiin laajakaistahäirintäsignaalia sekä FHSS-signaalin kanaviin kohdistettua monikanavahäirintäsignaalia. Radiovastaanotinta varten tehtiin mittalaitteisto, jolla selvitettiin häirinnän toimivuus. Mittauksissa selvitettiin häirintäsignaaleille eri häirintätehoilla häirinnän peittoalueet. Häirinnän peittoalueella tarkoitetaan aluetta häirintälaitteen ympärillä, jossa kohteen vastaanotin ei toimi.

4.1 AFHDS-protokolla

FlySkyn AFHDS-protokollasta (engl. Automatic Frequency Hopping Digital System) on tällä hetkellä kolme versiota: AFHDS, AFHDS-2A ja AFHDS 3. Tässä työssä on käytetty vanhinta AFHDS-protokollaa. Kyseinen protokolla käyttää Amiccom A7105 radiopiiriä, joka on yleinen 2,4 GHz lyhyen kantaman laitteisiin suunniteltu radiopiiri [26]. Radiopiiri tukee GFSK sekä FSK modulaatiota, joista AFHDS protokollassa käytetään GFSK:ta. Radiopiiri ei tue hybridi-tekniikkaa, vaan AFHDS-protokollassa käytetään vain FHSS-hajaspektritekniikkaa.

Kuvan 3 mittauksen avulla ja protokollan kanavataulukon [35] perusteella on todettu testijärjestelmän lähettimen käyttävän taulukon 4 mukaisia kanavia sekä hyppysekvenssiä. Protokolla käyttää 500 kHz:n levyisiä kanavia. Alun perin protokollassa käytettiin $2400,5 - 2480,0$ MHz:n taajuuskaistaa, joka oli jaettu 160 kanavaan. Yhden laitteen käyttämät 16 kanavaa olivat alun perin valittu tasavälein 160 kanavan joukosta. Myöhemmin kymmenen alinta ja kymmenen ylintä kanavaa poistettiin, jolloin taajuuskaistaksi jäi $2405,5 - 2475,0$ MHz ja vain 140 kanavaa. Uusissa laitteissa kahden poistuneen kanavan tilalle valittiin kanavat käytettyjen kanavien välistä, kuten nähdään taulukosta 4, jossa uudet kanavat ovat 49 ja 29. Testijärjestelmän vastaanotin on vanhempi kuin käytetty lähetin, joten vastaanotin kuulee vain 14 lähettimen käyttämää taajuutta, koska se ei kuuntele kanavia 49 ja 29.

Kuten nähdään kuvasta 3, kanavien vaihtoaika on noin 1,48 ms:a ja kanavan lähetys on päällä noin 0,6 ms. Lisäksi kahden käytettävän kanavan minimi etäisyydeksi on määrätty vähintään yksi megahertsi. [35] Lähettimeen ohjelmoidut kanavat ja hyppysekvenssi määräytyvät laitteen sarjanumeron perusteella ja näitä eri vaihtoehtoja protokollalle on määritelty 160, jotta laitteet eivät häiritsisi toisiaan, jos niitä on paljon samalla alueella. [35]

Taulukko 4. *Testissä käytetyn AFHDS-järjestelmän kanavien hyppyjärjestys [35]*

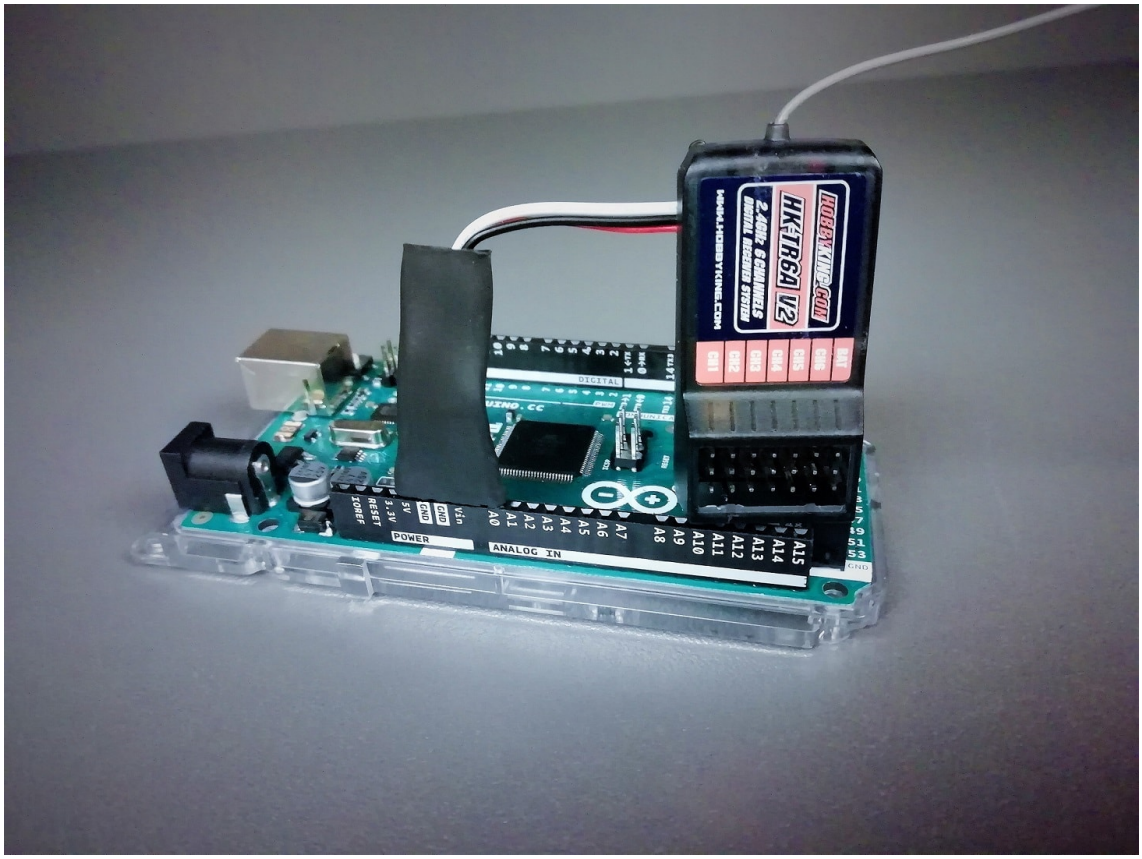
Järjestys	Kanava	Taajuus (MHz)
1	49	2429,5
2	74	2442
3	64	2437
4	29	2419.5
5	4	2407
6	84	2447
7	14	2412
8	94	2452
9	44	2427
10	124	2467
11	34	2422
12	114	2462
13	54	2432
14	134	2472
15	24	2417
16	104	2457

Ensimmäistä kertaa otettaessa vastaanotinta käyttöön se täytyy sitoa lähettimeen. Vastaanotin käynnistetään ensin ns. bind-tilassa, jonka jälkeen vastaavasti lähetin käynnistetään bind-tilassa. Bind-tilassa lähetin kertoo vastaanottimelle sarjanumeronsa, jonka perusteella vastaanotin osaa valita käytettävät kanavat ja hyppysekvenssin. Vastaanottimessa on bind-tilan lisäksi kaksi tilaa, jotka ovat normaalitila sekä tila kantoaallon etsimiseen. Normaalitilassa vastaanotin on synkronoitu lähetyksen hyppysekvenssiin ja hyppii samoja taajuuksia lähettimen kanssa vakioaikavälein. Normaalin kehyksen pituus on noin 1,48 ms, joten 16 kanavan hyppysekvenssi kestää noin 24 ms. Kun vastaanotin käynnistetään tai se hukkaa signaalin noin 100 kehystä peräkkäin, sen täytyy synkronoitua lähettimeen uudelleen. Tällöin vastaanotin siirtyy kantoaallon etsimistilaan, jossa kuunnellaan vuorotellen kuutta eri lähettimen käyttämää kanavaa, jotka testijärjestelmässä ovat: 4, 24, 74, 94, 34, 134. Jokaista kanavaa kuunnellaan noin 50 ms, jotta lähetin kävisi kyseisellä taajuudella kaksi kertaa. Löydettyään lähetyksen, vastaanottimen kello synkronoidaan lähettimen hyppysekvenssiin ja siirrytään normaalitilaan eli aloitetaan hyppimään taajuuksia lähettimen mukana.

Flyskyn seuraavan sukupolven AFHDS-2A-protokolla on hyvin samankaltainen, kun vanhempi AFHDS-protokolla, mutta ne eivät ole yhteensopivat. Uudempi protokolla käyttää uudempaa Amiccom A7106 radiopiiriä [27], mutta samaa modulointia, samoja taajuuskanavia sekä yhtä montaa taajuushyppelevää kanavaa kuin AFHDS-protokollakin. Suurin ero on, että AFHDS-2A tukee kahdensuuntaista radioyhteyttä eli myös ohjattava radiolaite voi lähettää informaatiota radio-ohjaimeen eikä vain toisinpäin. [63, 64] FlySkyn kolmannen sukupolven protokolla käyttää puolestaan 32 kanavan FHSS-signaalia ja kanavat on valittu 63 kanavan taulukosta. Modulointina se ei käytä GFSK:ta vaan chirp-hajaspektri modulaatiota (engl. chirp spread spectrum, CSS) tai GMSK-modulaatiota (engl. Gaussian minimum shift keying). [62]

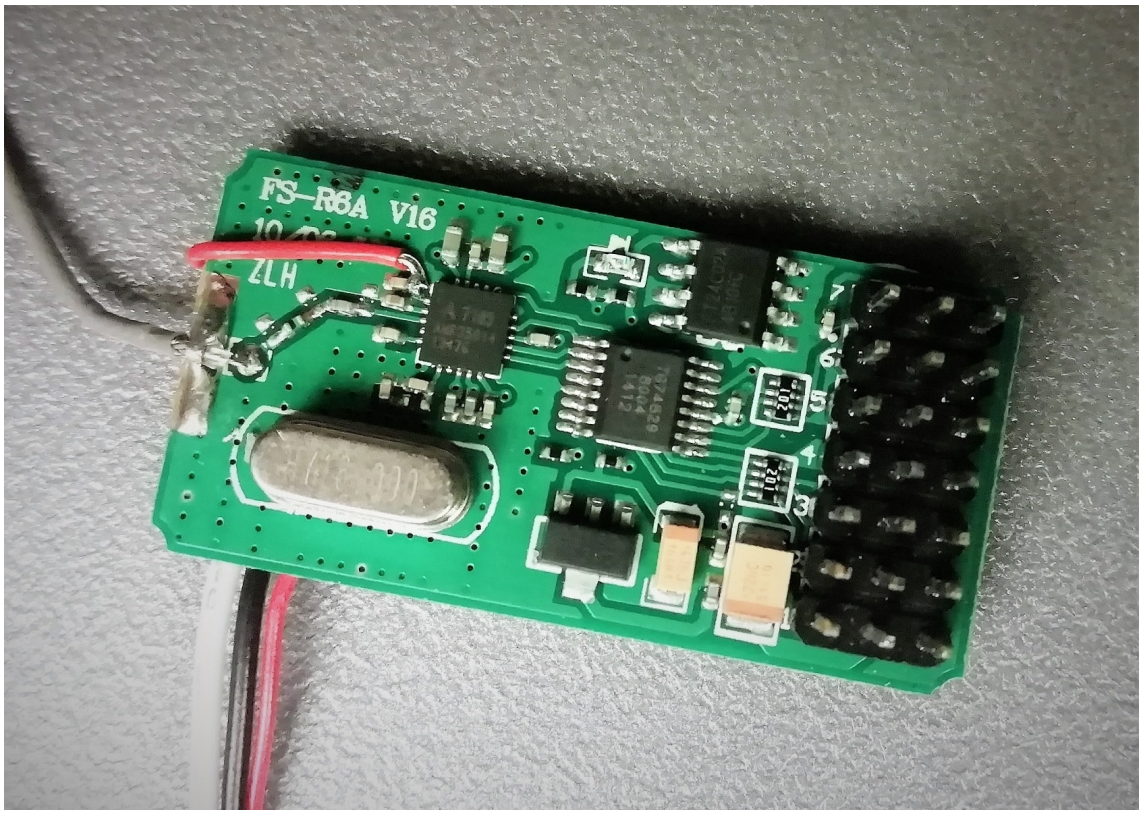
4.2 Mittaukseen käytetty laitteisto

Käytetystä HobbyKing TR6A-V2 vastaanottimesta ei saada suoraan tietoa vastaanotetun signaalin laadusta, joten häirinnän toimivuuden testaamiseksi vastaanottimeen kytkettiin mikrokontrollerijärjestelmä, joka näkyy kuvassa 8. Kuvassa 9 näkyy puolestaan vastaanotin purettuna, josta nähdään tarkemmin vastaanottimeen tehdyt kytkennät. Vastaanottimen radiopiirin RSSI-pinni kytkettiin punaisella johtimella mikrokontrollerin A/D-muuntimeen (Analogia-digitaali-muunnin), jolla mitattiin RSSI-pinnin jännitettä. Mitatut jännitteet lähetettiin tietokoneelle, jossa datasta laskettiin eri arvoja, joiden avulla voitiin arvioida häirinnän toimivuutta. Valkoisella ja mustalla johtimella kytkettiin vain mikrokontrollerijärjestelmästä käyttöjännite vastaanottimelle, ettei tarvinnut käyttää erillistä akkua.



Kuva 8. *Mikrokontrollerijärjestelmä kytkettynä radiovastaanottimeen*

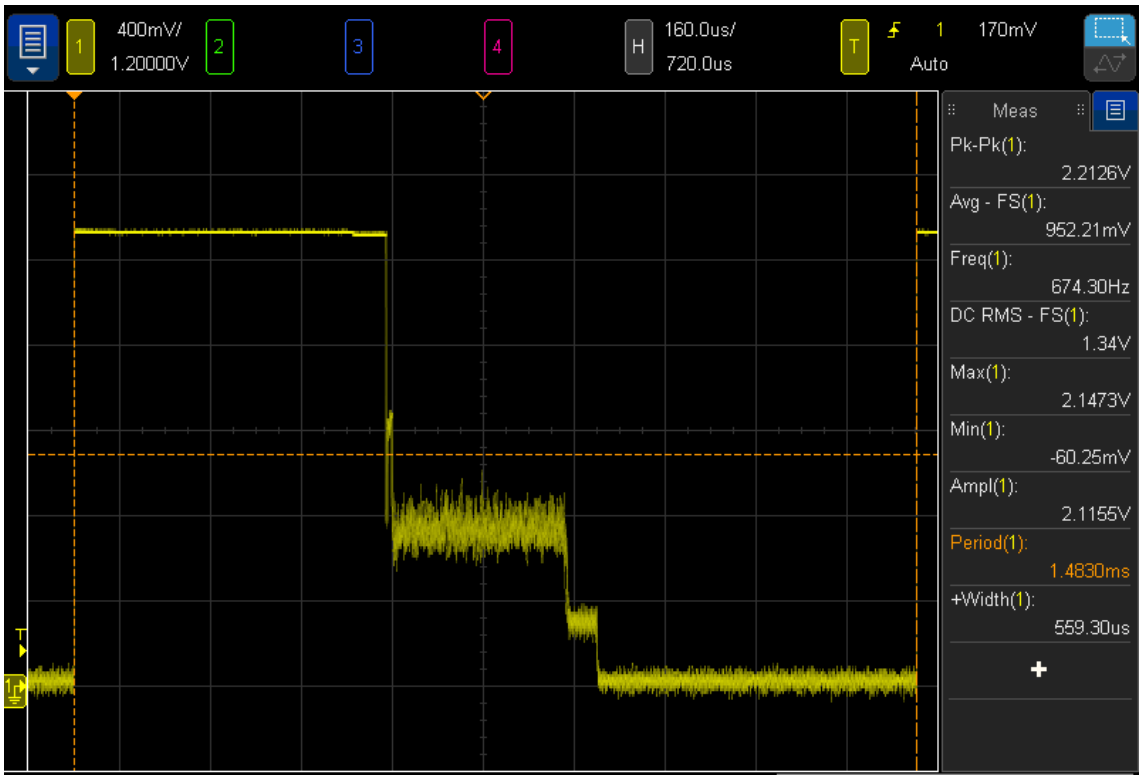
Mikrokontrollerijärjestelmänä käytettiin Arduino Mega 2560 R3:a ja A/D-muuntimen näytteistystaajuudeksi valittiin 19 231 Hz, jotta saadaan tarpeeksi tarkka tieto RSSI-pinnin jännitteestä. Tämä jännite kuvaa vastaanotetun signaalin tehoa valitulla kanavalla. RSSI-pinni voi saada arvoja väliltä $0-2{,}2\,\mathrm{V}$. Jännitteen ollessa noin $2{,}2\,\mathrm{V}$, vastaanotin ei kuuntele mitään kanavaa. Jännitteen laskiessa vastaanotin siirtyy kuuntelemaan valittua kanavaa ja mitä pienempi jännite on, sitä tehokkaampi vastaanotettu signaali on kyseisellä kanavalla. Radiopiirin datalehden [26] mukaan arvioitiin, mitä tehoa mikäkin A/D-muuntimen arvo vastasi ja vastaavuudet ovat laskettu liitteessä A.4.



Kuva 9. *Radiovastaanottimen etupuoli ilman koteloa*

Kuvassa 10 näkyy vastaanottimen radiopiirin RSSI-pinnin jännite oskilloskoopilla mitattuna yhden kehyksen ajalta. Mittauksessa radiolähetin oli päällä ja yhdistettynä vastaanottimeen eli radiovastaanotin oli normaalitilassa. Kuvaajassa yksi ruutu vastaa 0,4 V ja 160 µs. Kuvaajan alussa vastaanotin siirtyy käsittelemään edelliseltä kanavalta saatua informaatiota ja vaihtaa vastaanottimen taajuuden uudelle kanavalle. Tällöin vastaanotin ei kuuntele kanavaa, jolloin RSSI-pinnin jännite pysyy noin 2,2 V:ssa. Noin 400 µs ennen kuin lähetys alkaa uudella kanavalla, alkaa vastaanotin kuuntelemaan kanavaa. Silloin vastaanotettu teho on vain kohinaa, jolloin jännite laskee kohinatehoa vastaavaan arvoon, joka kuvassa on noin 0,8 V:n kohdalla. Kun lähetys alkaa kanavalla, vastaanotettu teho kasvaa ja jännite laskee signaalin tehoa vastaavaan arvoon. Kun kanavan data on saatu vastaanotettua, vastaanotin lopettaa kanavan kuuntelun, käsittelee vastaanotetun informaation sekä vaihtaa uudelle kanavalle.

Kehyksen pituus eli aika kanavan kuuntelun aloituksesta seuraavan kanavan kuuntelun alkuun on vakio. Jos kanavalta ei löydy lähetystä, niin kanavaa kuunnellaan pidempi aika. Tällöin aika, jolloin kanavaa ei kuunnella lyhenee eli jännite on vähemmän aikaa ylhäällä eli maksimi arvossaan. RSSI-pinnin jännitteen ylhäällä olon ajasta voidaan siis päätellä, onko kehys saatu luettua ja voidaan muodostaa arvio pakettivirhesuhteesta. RSSI-pinnin jännitteestä saadaan myös laskettua kanavan kohinateho sekä signaaliteho, jolloin kaavalla (6) saadaan laskettua signaalin SNR. Näiden avulla voidaan arvioida häirinnän toimivuutta.

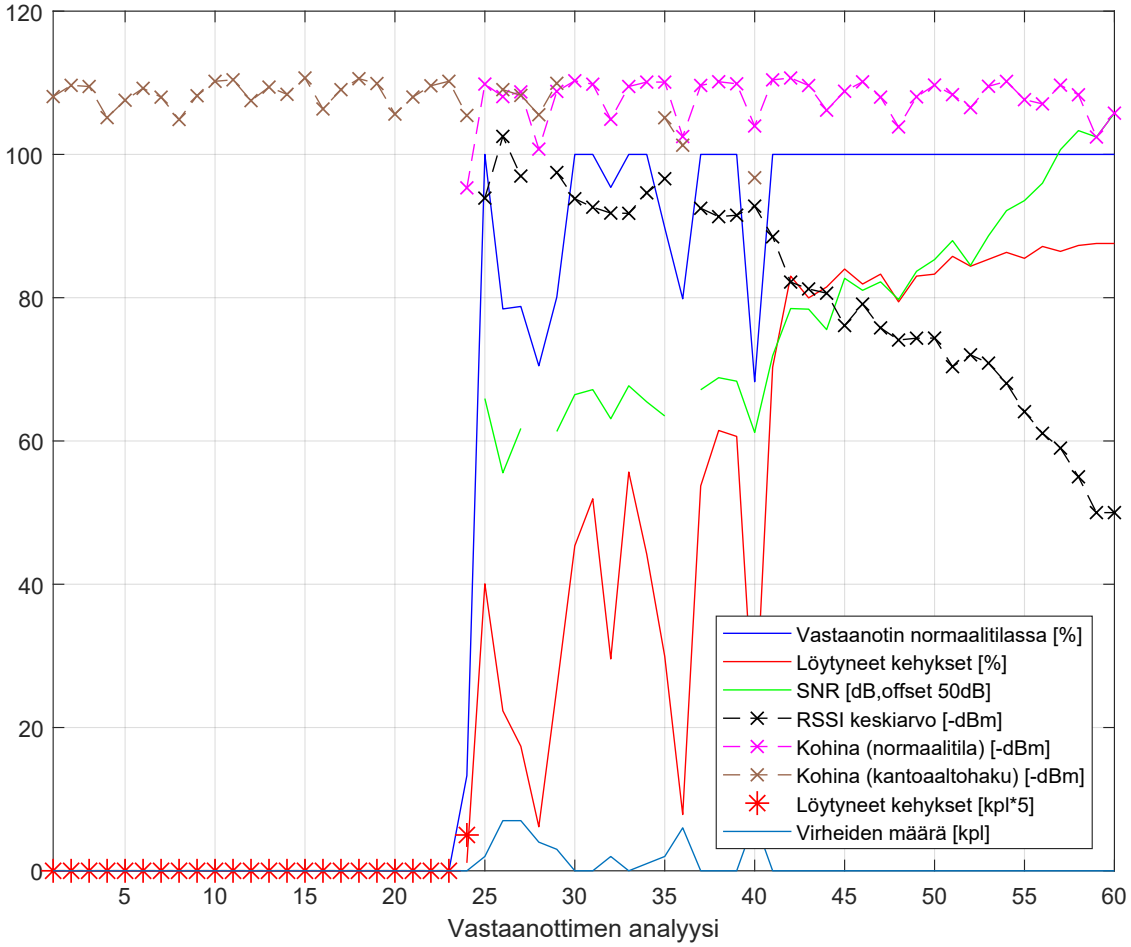


Kuva 10. *RSSI pinnistä oskilloskoopilla mitattu jännite*

Mikrokontrollerin mittaama jännite siirretään USB-kaapelilla sarjaliikennettä käyttäen tietokoneelle, jossa MATLAB-ohjelmalla prosessoidaan data ja selvitetään häirinnän toimivuus. Arduino- ja MATLAB-ohjelmakoodit löytyvät liitteestä A, jossa LOOP.m niminen MATLAB-ohjelma toimii pääohjelmana, joka käyttää muita MATLAB-ohjelmia funktioinaan.

LOOP.m-ohjelma toimii ikuisen silmukan sisällä, jossa aluksi lähetetään arduinolle käsky, jolloin arduino aloittaa A/D-muunnoksen. A/D-muunnos suoritetaan 19 231 kertaa eli noin sekunnin ajan. Arduino lähettää jokaisen mitatun arvon yksitellen A/D-muunnosten välissä sarjaliikennettä käyttäen tietokoneelle, jossa LOOP.m-ohjelma tallentaa arvot. Kun kaikki 19 231 arvoa on vastaanotettu, jaetaan data kehyksiin ja lasketaan kehyksistä eri arvoja, kuten signaali- ja kohinatehoja sekä onnistuneesti vastaanotettujen kehysten määrä. Arvot piirretään kuvaajaan, jonka jälkeen aloitetaan silmukassa uusi kierros eli toistetaan mittaukset ja laskenta sekä piirretään uudet arvot kuvaajaan.

Kuvassa 11 näkyy mittaus tilanteesta, jossa lähetintä viedään hitaasti kauemmaksi vastaanottimesta. Kuvaajassa näkyy aina viimeiset 60 mittausta eli noin 60 sekuntia ja viimeisin mittaus päivittyy vasemmalle puolelle. Kuvaajan on laskettua monia eri arvoja, joilla voidaan arvioida vastaanottimen hetkellistä toimintaa, mutta varsinaisen häirinnän määritystä varten tarkkaillaan löytyneiden kehysten määrää. Mallikuvaajassa aluksi lähetin ja vastaanotin ovat olleet lähellä toisiaan, joten löytyneitä kehyksiä on ollut noin 88 % kaikista vastaanotetuista kehyksistä. Tämä johtuu siitä, että vastaanotin kuulee vain 14 lähettimen käyttämästä 16 kanavasta. Siirrettäessä lähetintä kauemmaksi vastaanottimesta

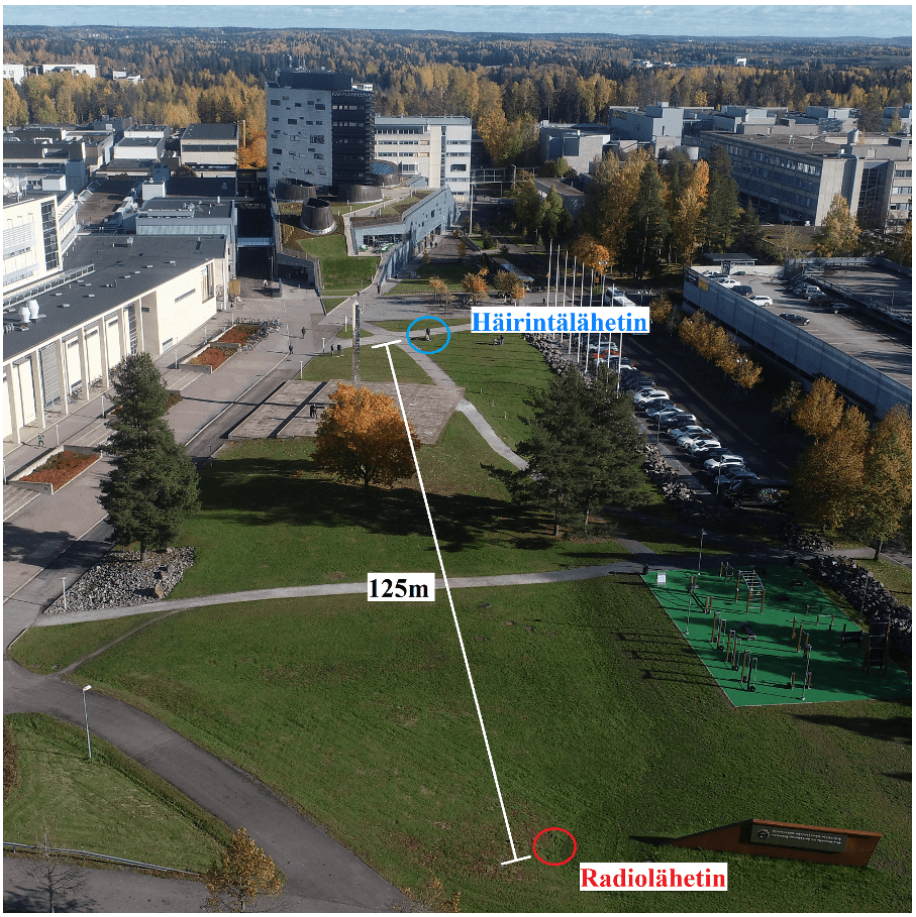


Kuva 11. *Matlab-kuvaaja RSSI-pinnin jännitteestä lasketuista tuloksista*

vastaanotetun signaalin teho laskee ja samalla SNR laskee. Kun lähetin viedään tarpeeksi kauas, SNR laskee niin pieneksi, ettei vastaanotin enää pysty tulkitsemaan vastaanotettuja paketteja. Tällöin löytyneiden kehysten määrä lähtee laskuun ja lopulta vastaanotin löytää vain yhden kehyksen yhden sekunnin ajalta. Tämän jälkeen lähetin ei enää löydä kehyksiä ja pysyy kantoaallon etsimistilassa.

4.3 Mittaukset

Mittauksissa määritettiin häirinnän peittoalueet kahdelle eri häirintäsignaalille viidellä eri tehotasolla. Häirintäsignaaleina käytettiin laajakaistahäirintäsignaalia, joka näkyy kuvassa 5 (a) ja monikanavahäirintäsignaalia, joka näkyy kuvassa 5 (c). Häirintätehoina käytettiin 0-20 dBm, 5 dBm:n välein. Mittaukset suoritettiin ulkona ja mittausasetelma näkyy kuvassa 12. Radiolähetin asetettiin noin 125 metrin päähän häirintälähettimestä, noin 1,5 metrin korkeudelle, joka vastaa tilannetta, jossa se olisi vihollisen käsissä. Peittoalueita varten radiovastaanotinta siirreltiin häirintälähettimen ympärillä ja mitattiin häirintälähettimestä 12 suuntaan 30°:n välein maksimietäisyydet eri häirintätehoilla ja -signaaleilla, joissa häirintä todettiin toimivaksi.

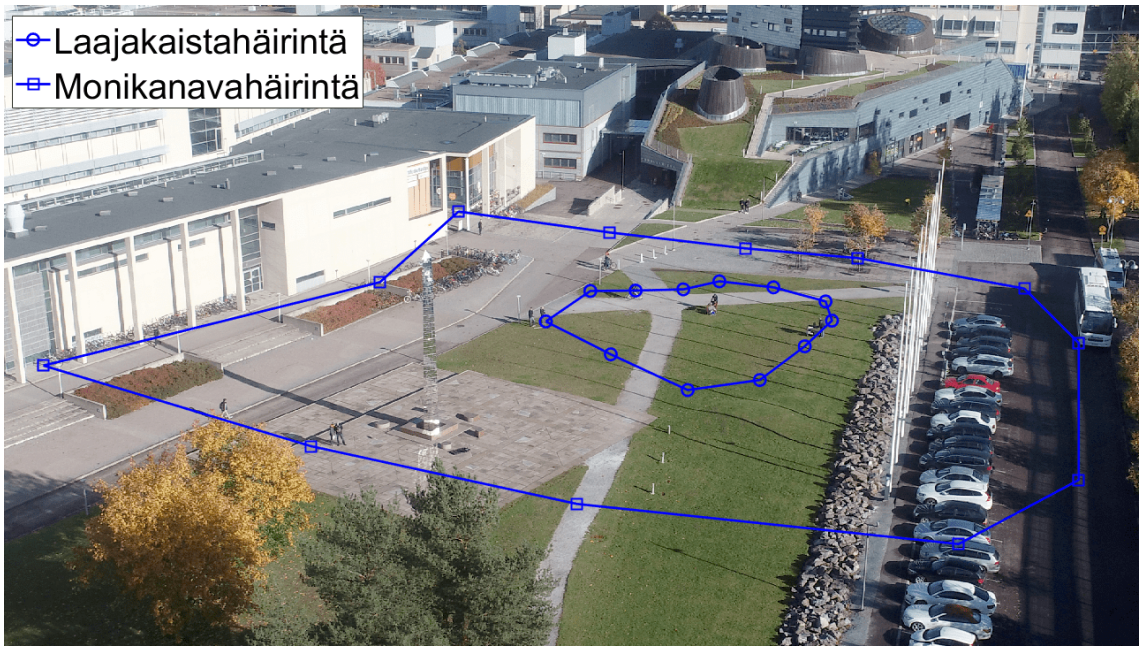


Kuva 12. *Radiolähettimen ja häirintälähettimen sijainti suhteessa toisiinsa*

Mittauksissa vastaanotin asetettiin maahan, koska tarkoituksena oli torjua improvisoituja räjähteitä. Häirintä katsottiin toimivaksi, kun radiovastaanotin ei löytänyt yhtään kehystä viiden peräkkäisen mittauksen eli viiden sekunnin aikana, koska yksikin onnistunut kehys saattaa riittää vastaanottimelle laukaisemaan räjähde. Tässä ajassa normaalisti kehyksiä olisi saatavilla yli 3000. Jos häirinnässä olisi keskitytty lennokkien häirintään, olisi häirinnän toimivuuden raja-arvoa voitu muuttaa, koska lennokkien hallinta olisi luultavasti menetetty paljon ennen kuin häirintä saavuttaa tilan, jossa vastaanotin ei löydä yhtään kehystä viiden mittausjakson aikana.

4.4 Tulokset

Kuvassa 13 näkyy mitatut peittoalueet laajakaista- sekä monikanavahäirinnälle 20 dBm:n lähetysteholla. Mitatut peittoalueet eivät ole täysin ympyröitä. Tämä johtuu esimerkiksi maaston muodoista, jotka vaikuttavat signaalien etenemiseen ja monitiehäipymiseen etenkin, koska vastaanotin oli maassa. Lisäksi häirintälähetin ei ole täysin ympärisäteilevä vaan se säteilee hieman paremmin radiolähettimen suuntaan. Taulukkoon 5 on laskettu eri lähetystehoille keskimääräiset häirintäpeittoalueiden säteet 12 eri suunnan keskiarvona. Tuloksia hieman vääristää se, että laajakaistahäirinnälle ei saatu suoritettua luotettavaa mittausta kahdella pienimmällä tehotasolla (*) kaikkiin 12 suuntaan.



Kuva 13. *Häirinnän peittoalueet, joissa häirintälähettimen lähetysteho on 20 dBm*

Monikanavahäirintäsignaalilla saavutettiin noin 3–4-kertainen häirintäetäisyys verrattuna laajakaistahäirintään. Suuruusluokaltaan tulos vastaa luvussa 3.3 saatua teoreettista tulosta, jonka mukaan monikanavahäirintäsignaalilla saataisiin noin kolminkertainen häirintäetäisyys laajakaistahäirintään verrattuna. Teoreettinen tulos on kuitenkin laskettu vapaantilan vaimenemismallia käyttäen, mikä ei vastaa maan pinnalla esteisessä maastossa etenevän signaalin vaimenemista. Lisäksi häirintäetäisyyteen vaikuttaa olennaisesti vastaanottimessa häirintäsignaalin tehon lisäksi kohteen radiolähettimen signaalin teho, mikä ei ole vakio vaan saattaa vaihdella eri mittapisteissä huomattavasti, johtuen esimerkiksi etäisyyden, esteiden ja monitiehäipymisen muutoksista.

Taulukko 5. *Keskimääräiset häirintäpeittoalueiden säteet*

	Laajakaista-häirintä	Monikanava-häirintä
0 dBm	3,0 m*	12,8 m
5 dBm	3,3 m*	17,8 m
10 dBm	4,9 m	23,2 m
15 dBm	8,2 m	29,3 m
20 dBm	12,2 m	37,3 m

Häirinnän tarkoituksena oli torjua improvisoituja räjähteitä. Laajakaistahäirinnällä saavutettiin noin 12 metrin häirintäsäde jo melko pienellä 20 dBm:n lähetysteholla. Käyttämällä adaptiivista häirintää, voidaan häirintä vaihtaa monikanavahäirintään heti, kun kohteen käyttämät kanavat on tunnistettu. Monikanavahäirinnällä saavutettiin lähes 40 metrin häirintäsäde vain 20 dBm:n lähetysteholla, joka antaisi jo huomattavan edun räjähteeltä suojautumisessa.

Testeissä käytetyt tehotasot ovat kuitenkin hyvin pieniä (20 dBm eli 0,1 W) ja oikeissa sovelluksissa käytettäisiin paljon suurempia tehoja, kuten kymmenistä wateista jopa tuhansiin watteihin. Jos käytettäisiin esimerkiksi 10 W:n tehoa, kaavan (10) mukaan saavutettaisiin noin kymmenkertainen kantama eli laajakaistahäirinnällä saavutettaisiin teoriassa 120 metrin häirintäsäde ja monikanavahäirinnällä jopa 400 metrin häirintäsäde. Jos tarkoituksena olisi ollut lennokkien häirintä, voitaisiin häirintälähettimessä käyttää suuntavia antenneja, joilla voitaisiin saavuttaa esimerkiksi 100-kertainen vahvistus, eli teoriassa noin kymmenkertainen kantama häirinnälle.

5. YHTEENVETO

Työn tavoitteena oli tutustua radio-ohjattavien improvisoitujen räjähteiden ja lennokkien käyttämiin radioprotokolliin ja niiden torjunnassa käytettäviin häirintätekniikoihin. Työn aihe on erityisen ajankohtainen johtuen lennokkien yleistymisestä sekä siitä seuranneesta ilmailurikkomusten lisääntymisestä. Radiohäirintää vaikeuttaa improvisoitujen räjähteiden tapauksessa käytettyjen laitteiden laaja kirjo. Lennokkien tapauksessa puolestaan käytettävä taajuuskaista ja usein myös hajaspektritekniikka ovat samoja eri laitteissa, mutta protokollat eroavat silti monin muin tavoin toisistaan. Lennokkien protokollia on satoja erilaisia ja niiden tarkempia tietoja on huonosti saatavilla. Nämä asiat on todettu vaikuttavan merkittävästi radiohäirinnän menetelmiin, koska mitä vähemmän radiohäirinnän kohteen käyttämästä radioprotokollasta tiedetään, sen yksinkertaisempaa ja tehottomampaa häirintämenetelmää joudutaan käyttämään. Tämän vuoksi tutkimukselle varsinkin lennokkien käyttämistä protokollista olisi tarvetta, jotta olisi mahdollista kehittää tehokkaampia häirintälaitteita niiden torjuntaan.

Työn kokeellisessa osiossa testattiin laajakaistahäirintää sekä monikanavahäirintää radio-ohjausjärjestelmää vastaan. Radiohäirintä todettiin toimivaksi improvisoitujen räjähteiden torjunnassa ja samoja keinoja voitaisiin hyödyntää lennokkien torjuntaan. Käytetty monikanavahäirintä eroaa laajakaistahäirinnästä siten, että häirintäsignaali on kohdistettu taajuustasossa kohdejärjestelmän käyttämille kanaville. Testeissä saavutettiin 20 dBm:n lähetysteholla laajakaistahäirinnällä yli 10 metrin ja monikanavahäirinnällä lähes 40 metrin säteinen peittoalue, jossa häirintä todettiin toimivaksi. Käytetyt tehotasot ovat kuitenkin melko pieniä ja oikeissa sovelluksissa voitaisiin helposti käyttää jopa 100-kertaisia tehotasoja, joilla saavutettaisiin teoriassa yhtä kertaluokkaa suuremmat häirintäsäteet.

Tuloksista voidaan todeta myös, miten yksinkertaisellakin tiedolla kohdejärjestelmästä voidaan saavuttaa merkittäviä hyötyjä radiohäirinnässä. Tunnistettaessa kohteen käyttämät taajuudet voidaan siirtyä laajakaistahäirinnästä monikanavahäirintään, jolloin häirinnän tehokkuus kymmenkertaistuu. Tunnistuksessa voitaisiin käyttää hyödyksi full-duplex-tekniikkaa, jolla saavutettaisiin huomattava etu, koska kohteen havainnointi ja häirintä voitaisiin suorittaa yhtä aikaa. Jos käytettäisiin vielä kehittyneempää adaptiivista häirintää, jossa pystyttäisiin seuraamaan täydellisesti kohteen signaalia aika- ja taajuustasossa, saavutettaisiin teoriassa 400 kertaa tehokkaampi häirintä laajakaistahäirintään verrattuna eli 20 dBm:n lähetysteholla jopa 240 metrin häirintäsäde. Tällöin myös spektrin käyttö olisi paljon tehokkaampaa, joten muille järjestelmille aiheutuva häiriö olisi todennäköisesti huomattavasti paljon pienempää ja häirintälähettimen havainnointi olisi paljon vaikeampaa.

LÄHTEET

[1] K. Riihola, Drone-lennokeista tuli ongelmia poliisille, Helsingin uutiset, 2018. Saatavilla: https://www.helsinginuutiset.fi/artikkeli/718889-drone-lennokeista-tuli-ongelmia-poliisille-luonut-uudenlaisia-turvallisuusuhkia, Viitattu 20.12.2018

[2] E. Mäntymaa, Kopteri toi vankilaan sukan täydeltä subutexia – dronella voi salakuljettaa vaikka käsiaseita, Yle Uutiset, 2017. Saatavilla: https://yle.fi/uutiset/3-9867140, Viitattu 16.1.2019

[3] Drone luvatta Venäjältä Suomeen, 2017, Rajavartiolaitos. Saatavilla: https://www.raja.fi/tietoa/tiedotteet/1/0/drone_luvatta_venajalta_suomeen_74709, Viitattu 16.1.2019

[4] A. Torniainen, Drone-uhka! : miehittämättömien lennokkien valvonta ja torjunta, Poliisiammattikorkeakoulu, 2018. Saatavilla: http://urn.fi/URN:NBN:fi:amk-201803293948

[5] Radiolaitteet, Viestintävirasto. Saatavilla: https://www.viestintavirasto.fi/taajuudet/radiolaitteet.html, Viitattu 20.12.2018

[6] J. Proakis, M. Salehi, Digital Communications, 5.th ed. New York, NY: McGraw-Hill, 2008, 1150 p.

[7] K. Wilgucki, R. Urban, G. Baranowski, P. Grądzki, P. Skarżyński, Automated protection system against RCIED, Military Communication Institute, 2011, pp. 593-601. Saatavilla: http://www.wil.waw.pl/art_prac/2011/Automated_Protection_System.pdf, Viitattu 20.12.2018

[8] A. Wilkinson, J. Bevan, I. Biddle, Improvised Explosive Devices (IEDs): An Introduction, in: Conventional Ammunition in Surplus, 2008, pp.136-145. Saatavilla: http://www.smallarmssurvey.org/publications/by-type/book-series/conventional-ammunition-in-surplus.html, Viitattu 20.12.2018

[9] A. Gulyàs, The Radio Controlled Improvised Explosive Device (RCIED) threat in Afghanistan, in: AARMS Vol. 12, No. 1, 2013, pp. 9–23. Saatavilla: archiv.uni-nke.hu/uploads/media_items/aarms-vol-12_-issue-1_-2013.original.pdf, Viitattu 20.12.2018

[10] Taajuusjakotaulukko, Viestintävirasto. Saatavilla: https://www.viestintavirasto.fi/attachments/maaraykset/Taajuusjakotaulukko_suomi_3.1.2018.pdf, Viitattu 20.12.2018

[11] HobbyKing 2.4Ghz 4Ch Tx & Rx V2 (Mode 2). Saatavilla: https://hobbyking.com/en_us/hobby-king-2-4ghz-4ch-tx-rx-v2-mode-2.html, Viitattu 20.12.2018

[12] Ilmailulaki 2014. 2§ (23.11.2018/965). Saatavilla: https://www.finlex.fi/fi/laki/ajantasa/2014/20140864, Viitattu 9.1.2019

[13] Kauko-ohjatut kopterit, Viestintävirasto. Saatavilla: https://www.viestintavirasto.fi/taajuudet/radioluvat/kauko-ohjatutkopterit.html, Viitattu 20.12.2018

[14] L. Ahlin, J. Zander, Principles of Wireless Communications. 2nd ed. Lund: Studentlitteratur, 1998, 525 p.

[15] B. Watson, FSK: Signals and Demodulation, Watkins-Johnson Tech Note, 1980. Saatavilla: http://www.rfcafe.com/references/articles/wj-tech-notes/fsk-signals-demodulation-v7-5.pdf, Viitattu 21.12.2018

[16] G. Goeij, E. Dijken, F.Brouwer, Research into the Radio Interference Risks of Drones, Strict b.v. 2016. Saatavilla: https://www.agentschaptelecom.nl/binaries/agentschap-telecom/documenten/rapporten/2017/december/6/rapport-research-into-the-radio-interference-risks-of-drones/Research_into_radio_interference_risks_of_drones.pdf, Viitattu 20.12.2018

[17] R.Peterson, R. Ziemer, D. Borth, Introduction to Spread-spectrum Communications, Englewood Cliffs, N.J: Prentice Hall, 1995, 695 p.

[18] R. Poisel, Modern Communications Jamming Principles and Techniques, 2nd edn, Artech House, Boston, 2011, 870 p.

[19] Protecting the Sky: Signal Monitoring of Radio Controlled Civilian Unmanned Aerial Vehicles and Possible Countermeasures, Rohde & Schwarz GmbH & Co KG. Saatavilla: https://www.scribd.com/doc/315420957/Protecting-the-Sky, Viitattu 27.12.2018

[20] PHY Basics: How OFDM Subcarriers Work, 2015. Saatavilla: http://www.revolutionwifi.net/revolutionwifi/2015/3/how-ofdm-subcarriers-work, Viitattu 20.12.2018

[21] D. Buxton, RC Spread Spectrum Demystified, 2014. Saatavilla: https://www.rchelicopterfun.com/RC-Spread-Spectrum.html, Viitattu 20.12.2018

[22] J. Andersson, Attackin DSMx with Software Defined Radio, PacSec 2016 Conference. Saatavilla: https://pacsec.jp/psj16/PSJ2016_Andersson_Hacking_DSMx_with_SDR_PacSec_2016_English.pdf, Viitattu 20.12.2018

[23] K. Pärlin, Jamming of Spread Spectrum Communications Used in UAV Remote Control Systems, Tallin University of Technology, 2017. Saatavilla: https://digi.lib.ttu.ee/i/?9378

[24] Supported Models, DeviationWiki. Saatavilla: https://www.deviationtx.com/wiki/supported_models, Viitattu 20.12.2018

[25] Multiprotocol TX Module, GitHub. Saatavilla https://github.com/pascallanger/DIY-Multiprotocol-TX-Module, Viitattu 22.1.2019

[26] A7105 Data Sheet, 2.4GHz FSK/GFSK Transceiver with 2K–500 Kbps data rate Amiccom Electronics Corp. Saatavilla: http://files.banggood.com/A7105%20Datasheet%20v1.4.pdf, Viitattu 20.12.2018

[27] A7106 Data Sheet, 2.4GHz FSK/GFSK Transceiver with 500Kbps data rate Amiccom Electronics Corp. Saatavilla: http://amiccom.weebly.com/uploads/3/9/5/9/3959395/a7106_datasheet_v0.1preliminary.pdf, Viitattu 20.12.2018

[28] ML2724 Data Sheet, 2.4GHz Low-IF 1.5Mbps FSK Transceiver, Micro Linear Corp. Saatavilla: http://doc.chipfind.ru/micro-linear/ml2724.htm, Viitattu 20.12.2018

[29] ML2730 Data Sheet, 2.4GHZ Variable data Rate FSK Transreceiver With Integrated PA, Micro Linear Corp. Saatavilla: http://datasheet.octopart.com/ML2730DM-Micro-Linear-datasheet-8616965.pdf, Viitattu 20.12.2018

[30] CYRF6936 Data Sheet, WirelessUSB™ LP 2.4 GHz Radio SoC, Cypress Semiconductor Corp. Saatavilla: http://www.cypress.com/files/cyrf6936-wirelessusb-lp-24-ghz-radio-soc-datasheetpdf, Viitattu 20.12.2018

[31] CC2520 Data Sheet, 2.4 GHZ IEEE 802.15.4/ZIGBEE® RF TRANSCEIVER, Texas Instruments Inc. Saatavilla: http://www.ti.com/product/CC2520, Viitattu 20.12.2018

[32] CC2500 Data Sheet, Low-Cost Low-Power 2.4 GHz RF Transceiver, Texas Instruments Inc. Saatavilla: http://www.ti.com/product/CC2500, Viitattu 20.12.2018

[33] CC2530 Data Sheet, A True System-on-Chip Solution for 2.4-GHz IEEE 802.15.4 and ZigBee Applications, Texas Instruments Inc. Saatavilla: http://www.ti.com/product/CC2530, Viitattu 20.12.2018

[34] nRF24L01+ Product Specification, Single Chip 2.4GHz Transceiver, Nordic Semiconductor ASA. Saatavilla: https://www.nordicsemi.com/DocLib?Product=nRF24, Viitattu 20.12.2018

[35] FS-i4, FCC Test Report, FlySky Rc Model Technology Co. Ltd. Saatavilla: https://fccid.io/N4ZFLYSKYI4/Test-Report/Test-Report-2285339, Viitattu 20.12.2018

[36] XG6, FCC Test Report, Japan Remote Control Co. Ltd. Saatavilla: https://fccid.io/AXG-RF2TPA/Test-Report/Test-Report-2959446, Viitattu 27.12.2018

[37] OPTIMA 9FCC Test Report, Hitec RCD Inc. Saatavilla: https://fccid.io/IFHOPT9-24G/Test-Report/Test-Report-1170846, Viitattu 27.12.2018

[38] T18MZ-WCFCC Test Report, Futaba Corp. Saatavilla: https://fccid.io/AZPT18MZWC-24G/Test-Report/Test-Report-DTS-2898147, Viitattu 2.1.2019

[39] M. Haluza, J. Čechák, Analysis and decoding of radio signals for remote control of drones, in: New Trends in Signal Processing (NTSP), Demanovska Dolina, 2016, pp. 1-5. Saatavilla: https://ieeexplore.ieee.org/document/7747781

[40] Y. Tian, Z. Wang, Q. Huang, UAV Remote Control Signal Analysis Based on GNU Radio and USRP X310,in: 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Conference (IMCEC), Xi'an, 2018, pp. 2502-2506. Saatavilla: https://ieeexplore.ieee.org/document/8469271

[41] A2 Flight Control System User Manual, SZ DJI Technology Co., Ltd. Saatavilla: https://dl.djicdn.com/downloads/a2/20170425/A2_User_Manual_V1.26_en.pdf, Viitattu 27.12.2018

[42] DJI OcuSync 2.0: What You Need to Know About This FPV Transmission System, 2018. Saatavilla: http://djibestdrones.com/dji-ocusync-2-0/#Benefits_of_OcuSync_over_Lightbridge, Viitattu 14.1.2019

[43] Introducing the New DSM System from Spektrum, Horizon Hobby Inc. 2004. Saatavilla: http://www.spektrumrc.com/Articles/Article.aspx?ArticleID=1423&Page=2, Viitattu: 21.1.2019

[44] D. Mototolea, C. Stolk, Software Defined Radio for Analyzing Drone Communication Protocols, International Conference on Communications (COMM), Bucharest, 2018, pp. 485-490. Saatavilla: https://ieeexplore.ieee.org/document/8484821

[45] R. Lagoy, Intercepting Quad-Copter Spread Spectrum Communications, UMass Amherst ECE 697KK Final Project. Saatavilla: http://www.nhfll.org/doc/lagoy_intercept_comms.pdf, Viitattu 31.12.2018

[46] J. Kosola, J. Jokinen, Elektroninen Sodankäynti: Osa 1, Taistelun Viides Dimensio. Helsinki: Maanpuolustuskorkeakoulu, tekniikan laitos, 2004. 223 s.

[47] M. Lichtman, J. Poston, S. Amuru, C. Shahriar, T. Clancy, R. Buehrer, J. Reed, A Communications Jamming Taxonomy, in: IEEE Security & Privacy, vol. 14, no. 1, 2016, pp. 47-54. Saatavilla: https://ieeexplore.ieee.org/document/7397710

[48] N. Aschenbruck, E. Gerhards-Padilla, P. Martini, Simulative Evaluation of Adaptive Jamming Detection in Wireless Multi-hop Networks, in: IEEE 30th International Conference on Distributed Computing Systems Workshops, Genova, 2010, pp. 213-220. Saatavilla: https://ieeexplore.ieee.org/document/5628838

[49] A. Hussain, N. Saqib, U. Qamar, M. Zia, H. Mahmood, Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks, in: Journal of Communications and Networks, vol. 16, no. 4, 2014, pp. 397-406. Saatavilla: https://ieeexplore.ieee.org/document/6896563

[50] K. Pelechrinis, M. Iliofotou, S. Krishnamurthy, Denial of Service Attacks in Wireless Networks: The Case of Jammers, in: IEEE Communications Surveys & Tutorials, vol. 13, no. 2, 2011, pp. 245-257. Saatavilla: https://ieeexplore.ieee.org/document/5473884

[51] W. Xu, K. Ma, W. Trappe, Y. Zhang, Jamming sensor networks: attack and defense strategies, in IEEE Network, vol. 20, no. 3, 2006, pp. 41-47. Saatavilla: https://ieeexplore.ieee.org/document/1637931

[52] A. Sabharwal, P. Schniter, D. Guo, D. Bliss, S. Rangarajan, R. Wichman, In-Band Full-Duplex Wireless: Challenges and Opportunities, in: IEEE Journal on Selected Areas in Communications, vol. 32, no. 9, 2014,pp. 1637-1652. Saatavilla: https://ieeexplore.ieee.org/document/6832464

[53] T. Riihonen, D. Korpi, M. Turunen, T. Peltola, J. Saikanmäki, M. Valkama, R. Wichman, Military full-duplex radio shield for protection against adversary receivers, submitted for review.

[54] T. Riihonen, D. Korpi, M. Turunen, M. Valkama, Full-duplex radio technology for simultaneously detecting and preventing improvised explosive device activation, Proc. International Conference on Military Communications and Information Systems (ICMCIS), Warsaw, Poland, May 2018. Saatavilla: https://ieeexplore.ieee.org/document/8398707

[55] T. Riihonen, D. Korpi, O. Rantula, H. Rantanen, T. Saarelainen, and M. Valkama, Inband Full-Duplex Radio Transceivers: A Paradigm Shift in Tactical Communications and Electronic Warfare?, IEEE Communications Magazine, vol. 55, no. 10, pp. 30-36, 2017. Saatavilla: https://ieeexplore.ieee.org/document/8067680

[56] A. Carlson, P. Crilly, Communication Systems: An Introduction to Signals and Noise in Electrical Communication, 5., internat. ed. Boston: McGraw-Hill, 2010, 924 pp.

[57] Global Signal Jammer Market 2017-2021, Technavio, 2017. Saatavilla: https://www.technavio.com/report/global-computing-devices-global-signal-jammer-market-2017-2021, Viitattu 20.12.2018

[58] K. Hill, Jamming GPS Signals Is Illegal, Dangerous, Cheap, And Easy, Gizmodo, 2017. Saatavilla: https://www.gizmodo.com.au/2017/07/jamming-gps-signals-is-illegal-dangerous-cheap-and-easy/, Viitattu 10.1.2019

[59] Airfence 5.0, Sensofusion Oy. Saatavilla: https://www.sensofusion.com/, Viitattu 20.12.2018

[60] Drone Jamming Gun PJ-2458, Rantelon Ltd. Saatavilla: https://rantelon.ee/en/toode/drone-jamming-gun/, Viitattu 20.12.2018

[61] MESMER®, Department 13, LLC. Saatavilla: https://department13.com/mesmer-3/, Viitattu 20.12.2018

[62] FGr4S, FCC Test Report, FlySky Rc Model Technology Co. Ltd. Saatavilla: https://fccid.io/N4ZFGRS400/Test-Report/Test-Report-DSS-4082352, Viitattu 3.1.2019

[63] Flysky Transmitters: what to know before you buy, WordPress, 2017. Saatavilla: https://rejectedorigins.wordpress.com/2017/01/03/flysky-transmitters-what-to-know-before-you-buy/, Viitattu 3.1.2019

[64] FS-i6S, FCC Test Report, FlySky Rc Model Technology Co. Ltd. Saatavilla: https://fccid.io/N4ZFLYSKYI6S/Test-Report/Test-Report-2911062, Viitattu 3.1.2019

LIITE A: ARDUINO- JA MATLAB-KOODIT

A.1 Arduino_Mega.c

```
#define F_CPU 16000000UL          // Clock Speed
#define BAUD 250000UL             // UART Baud rate
#define MYUBRR F_CPU/16/BAUD-1    // Value to UART register

#include <avr/io.h>
#include <avr/interrupt.h>
#include <util/delay.h>

volatile char data;

void USART_Init( unsigned int ubrr)
{
  /*Set baud rate */
  UBRR0H = (unsigned char)(ubrr>>8);
  UBRR0L = (unsigned char)ubrr;
  //Enable receiver and transmitter */
  UCSR0B = (1<<RXEN0)|(1<<TXEN0);
  /* Set frame format: 8data, 1stop bit */
  UCSR0C = (0<<USBS0)|(3<<UCSZ00);
}

void ADC_init(void){

  //Voltage reference to Internal 2.56V, Left adjust result, (Ch 0)
  ADMUX = (1 << REFS0) | (1 << REFS1) | (1 << ADLAR);

  //ADC prescaler = 64 -> ADC Clock =  250kHz
  //13 ADC clock cycles per conversion -> ADC SPS 19,231k
  ADCSRA = ((1 << ADPS2) | (1 << ADPS1));

  //Turn on ADC
  ADCSRA |= (1 << ADEN);

  DIDR0 = 0xFF; //Disable digital input registers A0-7

}

int main(int argc, char* argv[])
{ // Flash some LED:s to know when the controller resets
  DDRB = (1 << PB7);
  PORTB &= ~(1 << PB7);    //Turn off LED
  _delay_ms(200);
  PORTB |=  (1 << PB7);    //Turn on LED
  _delay_ms(200);
  PORTB ^=  (1 << PB7);    //Change LED
  _delay_ms(200);
  PORTB ^=  (1 << PB7);    //Change LED
  _delay_ms(200);
  PORTB ^=  (1 << PB7);    //Change LED

  USART_Init(MYUBRR);
  ADC_init();

```

```
54
55    while(1)
56    {
57
58        /* Wait for data to be received */
59        while ( !(UCSR0A & (1<<RXC0)) );
60        data = UDR0;
61
62        if (data == 'y')
63        {
64          //Turn on LED while doing A/D-conversion and sending data
65          PORTB |=  (1 << PB7);
66          ADCSRA |= (1 << ADSC); //Start A/D-conversion
67          uint32_t i = 0;
68
69          //Continue 19231 samples
70          while(i<19231)
71          {
72           while ( !( ADCSRA & (1<<ADIF )) );  //Wait until conversion is ready
73           ADCSRA |= (1 << ADSC);              //Start new conversion
74           while ( !( UCSR0A & (1<<UDRE0)) );  //Wait until DATA register is empty
75           UDR0 = ADCH;                        //Send data
76           i += 1;
77
78          }
79          PORTB &= ~(1 << PB7);                //Turn off LED
80        }
81    }
82  }
```

A.2 Serial_Init.m

```
%Funktio sarjaväylän alustukseen
function [s] = Serial_Init(N)
        instrreset      %Irrota ja poista kaikki vanhat instrumentit
        speed = 250000; %Baudinopeus 250k
        port = 'COM4';  %Portti COM4

        %Sisääntulopuskurin koko 2*N ja aikakatkaisu 6s.
        s=serial(port,'BaudRate',speed,'InputBufferSize',2*N,'Timeout',6);
        fopen(s);       %Avaa sarjaliikenne
end
```

A.3 Serial_READ.m

```
%Funktio datan lukemiseen mikrokontrollerilta
function [fixed_data] = Serial_READ(s,N)
        flushinput(s)         %Tyhjennä sisääntulopuskuri

        %Kirjoita mikrokontrollerille, jotta aloittaa A/D-muunnoksen
        fwrite(s,'y','uchar')
        data = fread(s,N,'uint8');      %Luetaan mikrokontrollerin lähettämä data
        normalized_data=data*1000/max(data);   %Normalisoidaan data 0-1000 välille
        %Siivotaan laskevat ja nousevat reunat
        bad_values = find(normalized_data<1000 & normalized_data>500);
        fixed_data = normalized_data;
        fixed_data(bad_values) = 1000;
end
```

A.4 RSSI_skaalaus.m

```
%Funktio RSSI arvon skaalaukselle dBm arvoksi datalehden mukaan (Amiccom A7105)
%A/D-muuntimelta saadut RSSI-arvot on valmiiksi skaalattu 0-1000
%välille Serial_read-funktiossa datan käsittelyn helpottamiseksi
function RSSI_dBm = RSSI_skaalaus(RSSI_Arvo)
        if RSSI_Arvo < 13
                RSSI_dBm = -40;
                elseif RSSI_Arvo >= 13 && RSSI_Arvo < 14
                RSSI_dBm = -45;
                elseif RSSI_Arvo >= 14 && RSSI_Arvo < 22
                RSSI_dBm = -50;
                elseif RSSI_Arvo >= 22 && RSSI_Arvo < 32
                RSSI_dBm = -55;
                elseif RSSI_Arvo >= 32 && RSSI_Arvo < 40
                RSSI_dBm = -56;
                elseif RSSI_Arvo >= 40
                RSSI_dBm = RSSI_Arvo*-0.1460-52;
         end
end
```

A.5 LOOP.m

```
clc;
clear all;

Fs = 19.231e3;          %A/D-muuntimen näytteistystaajuus
N=Fs;                   %Näytteiden määrä
time = (0:N-1)./Fs;
s = Serial_Init(N); %Sarjaväylän alustus
pause(1)                %Viive, jotta ehditään alustaa sarjaväylä


%Alustetaan rekisteri kuvaajaa varten
nBuffer = 60;
nSamples = 8;
RingBuffer = NaN*ones(nSamples,nBuffer);



keepLooping = true;

tic
%-------------------------------------------------------------------------
%Aloitetaan ikuinen silmukka, jossa luetaan N määrä näytteitä,
%prosessoidaan data ja piirretään kuvaajaan tärkeimmät tiedot
%-------------------------------------------------------------------------
while keepLooping
    tic
    clearvars -except N Fs time s nBuffer nSamples RingBuffer...
                      keepLooping processTime tallennus_kierros

    %MUUTTUJIEN ALUSTUS
    Rx_ON_Index                 = NaN;
    Rx_ON_Frames                = NaN;
    frame_on_or_off             = NaN;
    Kohina_on                   = NaN;
    Kohina_on_ka                = NaN;
    Kohina_on_skaalattu         = NaN;
    Kohina_all                  = NaN;
    Kohina_all_ka               = NaN;
    Kohina_all_skaalattu        = NaN;
    RSSI_on                     = NaN;
    RSSI_on_ka                  = NaN;
    RSSI_on_skaalattu           = NaN;
    Loytyneet_kehykset          = NaN;
    Hukatut_kehykset            = NaN;
    Loytyneet_kehykset_p        = NaN;
    SNR                         = NaN;
    Rx_OFF_Frames               = NaN;
    Rx_OFF_Index                = NaN;
    Kohina_off                  = NaN;
    Kohina_off_ka               = NaN;
    Kohina_off_skaalattu        = NaN;
    drawnow limitrate

    %Luetaan N määrä näytteitä mikrokontrollerilta
    data=Serial_READ(s,N);

    %Indeksoidaan kehykset laskevien reunojen kohdalta ja
    %lasketaan kehyksien pituudet
    laskevat_reunat_i = find(diff(data,1,1)<-500)+1;
    laskevat_reunat_diff = diff(laskevat_reunat_i);


```

```
63      %-------------------------------------------------------------------------
64      %Etsitään kehysrakenteet, jolloin vastaanotin normaali tilassa
65      %(Pituus 20-28 näytettä)
66      %-------------------------------------------------------------------------
67      laskevat_reunat_on_i =find( laskevat_reunat_diff==20 |...
68                                  laskevat_reunat_diff==21 |...
69                                  laskevat_reunat_diff==22 |...
70                                  laskevat_reunat_diff==23 |...
71                                  laskevat_reunat_diff==24 |...
72                                  laskevat_reunat_diff==25 |...
73                                  laskevat_reunat_diff==26 |...
74                                  laskevat_reunat_diff==27 |...
75                                  laskevat_reunat_diff==28);
76      Rx_ON = length(laskevat_reunat_on_i);
77
78      %Jos kehyksiä, joissa vastaanotin normaalitilassa löytyy,
79      %niin prosesoidaan kehykset
80      if Rx_ON > 1
81
82          Rx_ON_Index = laskevat_reunat_i(laskevat_reunat_on_i);
83          Rx_ON_Frames = zeros(Rx_ON-1,35);
84          kierros_on = 1;
85          frame_on_or_off = zeros(Rx_ON,1);
86
87          for i = 1:Rx_ON-1
88              %Välimuuttuja johon tallennetaan yhden kehyksen arvot
89              arvot1 = data(Rx_ON_Index(i):laskevat_reunat_i(...
90                  find(laskevat_reunat_i==Rx_ON_Index(i))+1)-1);
91
92              %Jos RSSI-jännite on "lepotilassa" eli ylhäällä vain lyhyen
93              %aikaa, niin kehyksen lukeminen ei ole onnistunut
94              if length(find(arvot1>999))>5
95                  frame_on_or_off(kierros_on,1) = 1;
96              end
97
98              pituus1 = length(arvot1);
99              Rx_ON_Frames(kierros_on,1:pituus1) = arvot1;
100             kierros_on = kierros_on +1;
101         end
102
103         Rx_ON_Frames( all(~Rx_ON_Frames,2), : ) = [];
104         Rx_ON_Frames( : ,all(~Rx_ON_Frames,1)) = [];
105
106         frame_on_or_off = frame_on_or_off(1:size(Rx_ON_Frames,1),1);
107
108        %Lasketeaan kohinan ja RSSI:n keskiarvot kehyksistä, jolloin data
109        %on saatu luettua onnistuneesti ja lasketaan niistä SNR
110         Kohina_on = mean(Rx_ON_Frames(frame_on_or_off==1,2:4),2);
111         if ~isempty(Kohina_on)
112             Kohina_on_ka = mean(Kohina_on);
113             Kohina_on_skaalattu = RSSI_skaalaus(Kohina_on_ka);
114             Kohina_on_abs = 10^(Kohina_on_skaalattu/10);
115
116             RSSI_on = mean(Rx_ON_Frames(frame_on_or_off==1,9:12),2);
117             RSSI_on_ka = mean(RSSI_on);
118             RSSI_on_skaalattu = RSSI_skaalaus(RSSI_on_ka);
119             RSSI_on_abs = 10^(RSSI_on_skaalattu/10);
120             RSSI_on_korjattu_abs = RSSI_on_abs-Kohina_on_abs;
121
122             if RSSI_on_korjattu_abs <0
123                 RSSI_on_korjattu_abs = 0;
124             end
125             RSSI_on_korjattu = 10*log10(RSSI_on_korjattu_abs);
126            SNR = RSSI_on_korjattu-Kohina_on_skaalattu;
```

```
127         else
128             Kohina_on_skaalattu = NaN;
129             RSSI_on_skaalattu = NaN;
130             SNR = NaN;
131             RSSI_on_korjattu = NaN;
132         end
133
134         %Lasketaan kohina keskiarvot kaikista kehyksistä jolloin
135         %vastaanotin normaalitilassa
136         Kohina_all = mean(Rx_ON_Frames(:,2:4),2);
137         Kohina_all_ka = mean(Kohina_all);
138         Kohina_all_skaalattu = RSSI_skaalaus(Kohina_all_ka);
139
140         %Lasketaan kehysten määrä, jolloin data on saatu luettua
141         %onnistuneesti sekä määrä jolloin ei ole saatu luettua.
142         Loytyneet_kehykset      = nnz(frame_on_or_off);
143         Hukatut_kehykset        = nnz(~frame_on_or_off);
144         Loytyneet_kehykset_p    = Loytyneet_kehykset/...
145                                   (Loytyneet_kehykset+Hukatut_kehykset)*100;
146
147
148        %Tallennetaan arvot kuvaajaa varten
149         RingData(2:5) = [Loytyneet_kehykset_p; SNR+50 ; ...
150                          RSSI_on_korjattu*-1 ; Kohina_on_skaalattu*-1];
151         RingData(7) = Loytyneet_kehykset*5;
152
153     else
154         RingData(2:5) = NaN;
155         RingData(7) = 0;
156     end
157
158     %-------------------------------------------------------------------
159     %Etsitään kehysrakenteet, jolloin vastaanotin etsii lähetintä
160     %(Pituus 886-889 näytettä)
161     %-------------------------------------------------------------------
162     laskevat_reunat_off_i = (find(      laskevat_reunat_diff==886 |...
163                                         laskevat_reunat_diff==887 |...
164                                         laskevat_reunat_diff==888 |...
165                                         laskevat_reunat_diff==889));
166
167     %Jos kehyksiä löytyy, joissa vastaanotin etsintätilassa,
168     %niin prosesoidaan kehykset
169     Rx_OFF = length(laskevat_reunat_off_i);
170
171     if Rx_OFF > 1
172
173         Rx_OFF_Index = laskevat_reunat_i(laskevat_reunat_off_i);
174         Rx_OFF_Frames = zeros(Rx_OFF-1,890);
175         kierros_off = 1;
176
177         for i = 1:Rx_OFF-1
178             %Välimuuttuja johon tallennetaan yhden kehyksen arvot
179             arvot2 = data(Rx_OFF_Index(i):laskevat_reunat_i(...
180                 find(laskevat_reunat_i==Rx_OFF_Index(i))+1)-1);
181
182             pituus2 = length(arvot2);
183             Rx_OFF_Frames(kierros_off,1:pituus2) = arvot2;
184             kierros_off=kierros_off +1;
185
186         end
187
188         Rx_OFF_Frames( all(~Rx_OFF_Frames,2), : ) = [];
189         Rx_OFF_Frames( : , all(~Rx_OFF_Frames,1)) = [];
190
```

```
191         %Lasketaan kohinan keskiarvo etsintätilan kehyksistä ja
192         %talletetaan se kuvaajaa varten
193         Kohina_off = mean(Rx_OFF_Frames(:,2:800),2);
194         if ~isempty(Kohina_off)
195             Kohina_off_ka = mean(Kohina_off);
196             Kohina_off_skaalattu = RSSI_skaalaus(Kohina_off_ka);
197         end
198         RingData(6) = Kohina_off_skaalattu*-1;
199     else
200         RingData(6) = NaN;
201     end
202
203     %-------------------------------------------------------------------
204     %Lasketaan virheellisesti mitattujen kehysten määrä sekä vastaanottimen
205     %aika normaalitilassa verrattuna kokonaisaikaan (kehyksistä)
206     %-------------------------------------------------------------------
207     laskevat_reunat_error_i = laskevat_reunat_i;
208     laskevat_reunat_error_i(...
209         [laskevat_reunat_on_i;laskevat_reunat_off_i]) = [];
210     virheiden_maara = length(laskevat_reunat_error_i)-1;
211     RingData(8) = virheiden_maara;
212
213     Rx_ON_p = Rx_ON/(Rx_ON + Rx_OFF*33)*100;
214     RingData(1) = Rx_ON_p;
215
216     RingBuffer = [RingBuffer(:,2:end) RingData(:)];
217
218     %-------------------------------------------------------------------
219     %Kuvaajan piirto:
220     %-------------------------------------------------------------------
221     figure(1)
222     p = plot(1:nBuffer,fliplr(RingBuffer),'MarkerSize',8,'LineWidth',0.6);
223     axis([1 nBuffer 0 120])
224     grid on
225     legend( 'Vastaanotin normaalitilassa [%]',...
226                 'Löytyneet kehykset [%]',...
227                 'SNR [dB,offset 50dB]',...
228                 'RSSI keskiarvo [-dBm]',...
229                 'Kohina (normaalitila) [-dBm]',...
230                 'Kohina (kantoaaltohaku) [-dBm]',...
231                 'Löytyneet kehykset [kpl*5]',...
232                 'Virheiden määrä [kpl]',...
233                 'Location','southeast')
234
235
236     p(4).LineStyle = '--';
237     p(5).LineStyle = '--';
238     p(6).LineStyle = '--';
239     p(7).LineStyle = 'none';
240     p(1).Color = 'b';
241     p(2).Color = 'r';
242     p(3).Color = 'g';
243     p(4).Color = 'k';
244     p(5).Color = 'm';
245     p(7).Color = 'r';
246     p(6).Color = [0.6 0.4 0.3];
247     p(7).MarkerSize = 10;
248     p(4).Marker = 'x';
249     p(5).Marker = 'x';
250     p(6).Marker = 'x';
251     p(7).Marker = '*';
252
253     xlabel('Vastaanottimen analyysi')
254
```

```
255     %-------------------------------------------------------------------
256     %Tulosta komentoriville laskettu data
257     %-------------------------------------------------------------------
258     disp(['Vastaanotin päällä: ',num2str(round(Rx_ON_p)),' %'])
259     disp(['Virheiden määrä    : ',num2str(virheiden_maara)])
260     if Rx_ON > 1
261         disp(['Löytyneet kehykset: ',num2str(...
262             round(Loytyneet_kehykset_p)),' %'])
263         disp(['Löytyneet kehykset: ',num2str(...
264             Loytyneet_kehykset),' kpl'])
265         disp(['RSSI(korjattu,dBm): ',num2str(...
266             round(RSSI_on_korjattu,2))])
267         disp(['Kohina     (on,dBm): ',num2str(...
268             round(Kohina_on_skaalattu,2))])
269         disp(['Kohina    (all,dBm): ',num2str(...
270             round(Kohina_all_skaalattu,2))])
271     end
272     if Rx_OFF > 1
273         disp(['Kohina(off)  (dBm): ',num2str(...
274             round(Kohina_off_skaalattu,2))])
275     end
276     if Rx_ON > 1
277             disp(['SNR           (dB): ',num2str(round(SNR,2))])
278     end
279     disp(['Aika: ',num2str(toc),' s'])
280     disp(' ');
281 
282 end
283 toc
284 %Suljetaan sarjaväylä
285 fclose(s);
```