jamk

Merivalvontatutkien radioaaltojen eteneminen ja siihen liittyvät kyberturvallisuusuhat

Katri Hallavainio

Opinnäytetyö, AMK
Marraskuu 2025
Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Hallavainio, Katri

Merivalvontatutkien radioaaltojen eteneminen ja siihen liittyvät kyberturvallisuusuhat

Jyväskylä: Jyväskylän ammattikorkeakoulu. Marraskuu 2025, 55 sivua.

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Tutkatekniikan kehitys johti siihen, että tutkajärjestelmien toimintaympäristö monimutkaistui ja niiden uhkakenttä laajeni perinteisestä sähkömagneettisesta spektristä myös ohjelmisto- ja verkkotasolle. Tutkimuksen tavoitteena oli selvittää, miten radioaaltojen etenemiseen vaikuttavat fysikaaliset ilmiöt sekä kyberturvallisuusuhat heikensivät tutkien suorituskykyä merivalvonnassa ja millaisin teknisin ja operatiivisin menetelmin niiden vaikutuksia voitiin torjua tai lieventää.

Tutkimus toteutettiin kirjallisuusanalyysina ja simulaatiopohjaisina kokeina, joissa tutkittiin erilaisten häiriöiden vaikutusta tutkan havaintokykyyn. Simulaatiokokeissa (A-C) mallinnettiin erityisesti tahallisia häiriöitä sekä tutkittiin adaptiivisen signaalinkäsittelyn ja sensorifuusion tehokkuutta niiden torjunnassa.

Tulokset osoittivat, että tutkajärjestelmien häiriönsieto ei ollut yksittäinen tekninen ominaisuus vaan arkkitehtuurinen ja tietoturvallinen kokonaisuus. Fyysisten ja tietoteknisten häiriöiden yhteisvaikutus heikensi järjestelmän toimintakykyä merkittävästi, kun taas adaptiivinen signaalinkäsittely, tekoälypohjainen analyysi ja monilähdefuusio paransivat havaintojen tarkkuutta. Kognitiivisen tutkan havaittiin edustavan tutkateknologian seuraavaa kehitysvaihetta, jossa järjestelmä oppii tunnistamaan ja hallitsemaan samanaikaisia häiriöitä reaaliaikaisesti.

Johtopäätöksenä todettiin, että tutkajärjestelmien luotettavuus perustui fyysisen, digitaalisen ja kognitiivisen tason yhteistoimintaan. Tutkimuksen tuloksia voitiin hyödyntää seuraavan sukupolven merivalvontatutkien suunnittelussa, joissa yhdistetään sähkömagneettinen häiriönsieto, tietoturva sekä tekoälyohjattu päätöksenteko.

Avainsanat (asiasanat)

tutkajärjestelmät, merivalvonta, elektroninen sodankäynti, häiriönsieto, kognitiivinen tutka, kyberturvallisuus, tekoäly

Muut tiedot (salassa pidettävät liitteet)

-

jamk

Description

Hallavainio, Katri

Maritime Surveillance Radar Signal Propagation and Associated Cybersecurity Threats

Jyväskylä: JAMK University of Applied Sciences, November 2025, 55 pages.

Bachelor´s Degree Programme in Information and Communications Technology. Bachelor´s thesis.

Permission for open access publication: No

Language of publication: Finnish

Abstract

The development of radar technology led to an increasingly complex operating environment, where the threat landscape expanded beyond the traditional electromagnetic spectrum to include software- and network-level domains. The objective of the study was to examine how physical phenomena affecting radio wave propagation and cybersecurity threats degraded the performance of radar systems in maritime surveillance, and to identify the technical and operational methods through which their impacts could be mitigated.

The research was carried out as a literature-based analysis and simulation experiments, which investigated how different types of interference affected radar detection capability. The simulations (A–C) modelled deliberate interference and examined the effectiveness of adaptive signal processing and sensor fusion in countering such disruptions.

The results showed that radar system resilience was not a single technical property but an architectural and cybersecurity-related capability. The combined impact of physical and digital interference significantly reduced system performance, whereas adaptive signal processing, AI-based analysis, and multisource fusion improved detection accuracy. Cognitive radar was found to represent the next stage in radar evolution, where the system learns to recognize and manage simultaneous disturbances in real time.

It was concluded that radar system reliability depended on the integration of physical, digital, and cognitive domains. The results of the research could be applied in the design of next-generation maritime surveillance radars that combine electromagnetic countermeasures, cybersecurity, and AI-driven decision-making.

Keywords/tags (subjects)

radar systems, maritime surveillance, electronic warfare, resilience, cognitive radar, cybersecurity, artificial intelligence

Miscellaneous (Confidential information)

-

Sisältö

Kuviot

1 Johdanto

1.1 Tausta ja tutkimusongelma

Merivalvonta on kansallisen turvallisuuden ja merenkulun sujuvuuden kulmakivi. Tässä valvonnassa tutkajärjestelmät ovat keskeisimpiä teknisiä työkaluja, jotka mahdollistavat laajojen merialueiden tapahtumien havaitsemisen ja seuraamisen sääolosuhteista riippumatta. Globalisoituneessa maailmassa, jossa meriliikenteen volyymi sekä geopoliittiset jännitteet kasvavat, reaaliaikaisen ja luotettavan tilannekuvan merkitys on korostunut entisestään. Vaikka tutkat ovat perinteisesti olleet luotettavia, niiden suorituskykyyn vaikuttavien tekijöiden monimutkaisuus on lisääntynyt huomattavasti (Skolnik 2008, 25–27).

Perinteisesti tutkien suorituskykyä on tarkasteltu fysikaalisten rajoitteiden kautta. Erityisesti kaukovalvontatutkien (HF-tutkat) toiminta on riippuvaista radioaaltojen etenemisestä ilmakehän kerroksissa. Ionosfäärin jatkuvat tilanvaihtelut, jotka johtuvat avaruussäästä ja Auringon aktiivisuudesta, voivat aiheuttaa signaalin vaimenemista, taittumista ja odottamattomia etenemisreittejä. Nämä luonnolliset ilmiöt muodostavat jatkuvan ja dynaamisen haasteen tutkajärjestelmien luotettavuudelle.

Samaan aikaan järjestelmien digitalisoituminen sekä verkottuminen ovat avanneet oven täysin uudenlaiselle uhkaympäristölle. Nykyaikaiset tutkajärjestelmät eivät ole enää suljettuja, itsenäisiä laitteita, vaan ne ovat osa laajempaa tietoverkkoa. Tämä altistaa ne tahalliselle, ihmisen aiheuttamille kyberturvallisuusuhille, kuten elektroniselle häirinnälle, signaalin väärentämiselle (spoofing) sekä ohjelmisto- ja verkkotason hyökkäyksille.

Tämän opinnäytetyön tutkimusongelma syntyy näiden kahden, luonteeltaan erilaisen haasteen risteyskohdasta. Ongelmana on, että ympäristön aiheuttamia fysikaalisia häiriöitä sekä ihmisen aiheuttamia kyberuhkia tarkastellaan usein erillisinä ilmiöinä, vaikka ne voivat vaikuttaa järjestelmän toimintaan samanaikaisesti ja jopa pahentaa toistensa vaikutuksia. Tutkimuksen tieteellinen merkitys perustuu siihen, että se yhdistää fysikaalisen signaalinmallinnuksen ja kyberturvallisuuden näkökulmat, joita on aiemmissa suomalaisissa tutkimuksissa tarkasteltu harvoin yhtenä kokonaisuutena.

Tutkajärjestelmien merkitys on kasvanut, erityisesti Itämeren alueella muuttuneen turvallisuustilanteen, avaruussään voimistumisen ja tekoälypohjaisten valvontajärjestelmien käyttöönoton myötä. Näiden kehityskulkujen vuoksi häiriönsieto ja järjestelmien tietoturva muodostavat kriittisen tutkimuskohteen.

1.2 Tutkimuskysymykset ja työn rajaus

Tämän opinnäytetyön tavoitteena on analysoida kokonaisvaltaisesti merivalvontatutkien suorituskykyyn vaikuttavia ympäristötekijöitä ja kyberturvallisuusuhkia. Työssä pyritään luomaan synteesi siitä, miten avaruussään kaltaiset luonnonilmiöt ja tahallinen häirintä yhdessä muovaavat tutkajärjestelmien toimintaympäristöä. Lisäksi tavoitteena on tarkastella teknisiä ja operatiivisia ratkaisuja, jolla järjestelmien häiriönsietokykyä ja turvallisuutta voidaan parantaa.

Tavoitteeseen pääsemiseksi työssä haetaan vastauksia seuraaviin tutkimuskysymyksiin:

- Miten keskeisimmät radioaaltojen etenemiseen vaikuttavat fysikaaliset ilmiöt heikentävät tutkan suorituskykyä merivalvonnassa?
- Millä tavoin nykyaikaisiin tutkajärjestelmiin kohdistuvat kyberturvallisuusuhat vaarantavat järjestelmien luotettavuuden ja tuottaman tilannekuvan eheyden?
- Millä teknisillä ja operatiivisilla menetelmillä sekä luonnollisten että tahallisten häiriöiden vaikutuksia voidaan torjua tai lieventää?

Tämä opinnäytetyö keskittyy fysiikan ja kyberturvallisuuden teknisiin periaatteisiin. Työssä ei oteta kantaa esimerkiksi tutkajärjestelmiin liittyvään lainsäädäntöön, hankintaprosesseihin tai yksityiskohtaiseen laitteistorakenteeseen. Tarkastelun kohteena ovat yleiset periaatteet, ei yksittäisten, operatiivisessa käytössä olevien järjestelmien salaiseksi luokitellut ominaisuudet.

1.3 Työn rakenne

Opinnäytetyö on jaettu kolmeen pääosaan, jotka etenevät loogisesti perusteista haasteisiin ja lopulta ratkaisuihin. Työn ensimmäinen osa luo teoreettisen pohjan esittelemällä tutkatekniikan perusteet ja radioaaltojen etenemisen fysiikan. Erityistä huomiota kiinnitetään ionosfäärin ja avaruussään merkitykseen kaukovalvonnan kannalta.

Toisessa osassa syvennytään työn ytimessä oleviin haasteisiin. Luvussa 3 analysoidaan ympäristön aiheuttamia luonnollisia häiriöitä, kuten ionosfäärin vaihteluita ja anomaalisia etenemismuotoja. Tämän jälkeen luvussa 4 siirrytään tarkastelemaan ihmisen aiheuttamia uhkia, keskittyen elektronisen sodankäynnin menetelmiin, kuten häirintään sekä muihin kyberturvallisuuden uhkakuviin.

Työn kolmas osa keskittyy ratkaisuihin ja soveltamiseen. Luvussa 4 esitellään teknisiä ja operatiivisia suojausmenetelmiä, joilla voidaan parantaa tutkajärjestelmien häiriönsietokykyä. Lopuksi tulokset esitellään sekä analysoidaan, minkä jälkeen kaikki osa-alueet vedetään yhteen pohdinnassa, jossa tehdään johtopäätökset sekä vastataan asetettuihin tutkimuskysymyksiin.

Työssä toteutettiin kolme simulaatiopohjaista koetta (A-C), joilla arvioitiin järjestelmän häiriönsietoa tahallisissa häiriöissä. Tulosten perusteella analysoitiin adaptiivisen ECCM:n ja sensorifuusion vaikutuksia järjestelmän luotettavuuteen.

1.4 Tutkimusasetelma ja tutkimusmenetelmä

Tämä opinnäytetyö toteutettiin kokeellisena simulaatiotutkimuksena, jossa tutkittiin merivalvontatutkien suorituskykyä erilaisissa tahallisissa häiriötilanteissa. Kokeellinen tutkimus on tutkimusmenetelmistä ainoa, joka mahdollistaa syy-seuraussuhteiden systemaattisen arvioinnin manipuloimalla yhtä tai useampaa muuttujaa sekä havainnoimalla näiden vaikutusta mittaavaan vasteeseen. Kokeelliselle menetelmälle tyypillisiä piirteitä ovat kontrolloidut olosuhteet, riippumattoman muuttujan manipulointi ja riippuvan muuttujan mittaaminen. (Hirsjärvi, Remes & Sajavaara 2015, 180–185; Creswell 2014, 168–171.)

Tässä työssä riippumattomina muuttujina toimivat muun muassa

- häirinnän tyyppi ja voimakkuus (DRFM, kohinahäirintä)
- Ionosfäärin tai troposfäärin tila
- GNSS/AIS-signaalin väärentämisen aste,

kun taas riippuvia muuttujia edustivat tutkan havaitsemiskyky, signaali-kohinasuhde ja fuusion tuottaman tilannekuvan virhe. Näiden muuttujien systemaattinen manipulointi tekee menetelmästä luonteeltaan selvästi kokeellisen.

Opinnäytetyö luokitellaan lisäksi soveltavaksi tutkimukseksi, sillä tavoitteena ei ole pelkästään ilmiöiden teoreettinen ymmärtäminen, vaan myös niiden käytännön vaikutusten arviointi merivalvontatutkien operatiiviseen suorituskykyyn. On kuitenkin tärkeää huomata, että soveltava tutkimus ei ole menetelmä itsessään, vaan tutkimuksen tarkoitusta kuvaava luokitus: soveltavassa tutkimuksessa käytetään mitä tahansa menetelmää, joka parhaiten vastaa tutkimuskysymyksiin (Hirsjärvi, Remes & Sajavaara 2015, 155–156). Tässä työssä soveltavan tutkimuksen tavoitteet toteutetaan nimenomaan kokeellisen menetelmän avulla.

Kokonaisuutena tutkimusasetelma muodostuu kolmesta simulaatiokokeesta (A-C), jotka edustavat eritasoisia uhkamalleja: signaalitason häirintää, laaja-alaista ECCM-tarkastelua sekä järjestelmätasoista sensorifuusiota. Tämän rakenteen avulla voidaan analysoida sekä yksittäisten ilmiöiden vaikutuksia että niiden yhteisvaikutusta tutkajärjestelmien resilienssiin. Näin kokeellinen menetelmä toimii primaarisena työkaluna vastattaessa tutkimuskysymyksiin.

2 Tutkateknologiat ja radioaaltojen etenemisen perusteet

2.1 Tutkatekniikan perusteet

Tutka (RADAR, Radio Detection and Ranging) on sähkömagneettiseen säteilyyn perustuva järjestelmä, joka on suunniteltu kohteiden havaitsemiseen, paikantamiseen sekä niiden liikkeiden seuraamiseen. Järjestelmän toiminta perustuu lyhyiden radiopulssien lähettämiseen ja kohteesta heijastuneen kaiun vastaanottamiseen sekä analysointiin (Kingsley & Quegan 1999, 1–2). Merivalvonnassa käytettävät tutkajärjestelmät voidaan jakaa karkeasti kahteen päätyyppiin niiden toimintaperiaatteen ja kantaman perusteella: suoranäköyhteydellä toimiviin tutkiin (Line-of-Sight, LOS) sekä horisontin yli toimiviin kaukovalvontatutkiin (Over-the-Horizon Radar, OTHR).

LOS-tutkat toimivat tyypillisesti mikroaaltotaajuuksilla (UHF- ja SHF-alueet), joiden radioaallot etenevät suoraviivaisesti. Niiden tehokas toiminta edellyttääkin esteetöntä näköyhteyttä tutkan ja kohteen välillä. Tämän vuoksi niiden kantamaa rajoittavat käytännössä aina maan kaarevuus, maastonmuodot sekä ilmakehän olosuhteet, kuten voimakkaat sateet tai poikkeukselliset lämpötilakerrostumat, jotka voivat vaimentaa tai taittaa signaalia (Skolnik 2008, 981, 995–997). Skolnikin (2008, 995–997) mukaan ilmakehän refraktio vaikuttaa tutkahorisonttiin lineaarisesti, kun taas

Kingsley ja Quegan (1999, 127) esittävät vaikutuksen olevan ei-lineaarinen troposfäärin kosteuden vaihtelussa. Tämä ero on merkittävä rannikkotutkien suunnittelussa.

Kaukovalvontatutkat (OTHR) puolestaan hyödyntävät korkeita HF-taajuuksia (3–30 MHz), joiden erityispiirre on kyky heijastua maapallon ionosfäärikerroksista. Tämä heijastuminen mahdollistaa tutkasignaalin etenemisen horisontin taakse jopa tuhansien kilometrien päähän ilman suoraa näköyhteyttä. Toimintaperiaate tekee järjestelmästä kuitenkin erittäin riippuvaisen ionosfäärin jatkuvasti vaihtelevasta tilasta, mikä altistaa sen avaruussään aiheuttamille häiriöille. Näiden ulkoisten tekijöiden ja järjestelmien omien ominaisuuksien välistä suhdetta kuvataan matemaattisesti tutkayhtälöllä, joka on kaikkien tutkajärjestelmien suorituskyvyn analysoinnin perusta. (Hunsucker & Hargreaves 2003, 97; Skolnik 2008, 321–322.)

Tutkayhtälön muoto on:

$$P_r = \frac{(P_t G_t G_r \lambda^2 \sigma)}{(4\pi)^3 R^4 L}$$

missä Pr on vastaanotettu teho, Pt lähetysteho, Gt ja Gr antennien vahvistukset, λ aallonpituus, σ kohteen tutkapoikkipinta-ala, R etäisyys ja L järjestelmän häviötekijä. Yhtälö osoittaa, että vastaanotettu signaali heikkenee neljännen potenssin verran etäisyyden kasvaessa, mikä tekee sekä ympäristöolosuhteista että häiriöistä erityisen kriittisiä pitkän kantaman valvontatutkissa. (Skolnik 2008, 23–25.)

Skolnik (2008) painottaa, että tutkan havaitsemiskyky riippuu yhtä lailla antennijärjestelmän ominaisuuksista kuin ympäristön dynaamisesta vaikutuksesta, kun taas Kingsley ja Quegan (1999) korostavat signaalinkäsittelyn merkitystä häiriönsietokyvyn kannalta. Näiden näkökulmien yhdistäminen on keskeistä nykyaikaisessa merivalvonnassa, jossa fyysiset ja tietotekniset rajoitteet kietoutuvat toisiinsa.

Näin ollen tutkajärjestelmän suorituskyky ei ole pelkästään laitteiston ominaisuus, vaan dynaaminen yhdistelmä ympäristön, signaalinkäsittelyn ja antennitekniikan yhteisvaikutuksia. Tämä korostaa mallinnuksen ja simulaatiopohjaisen analyysin merkitystä erityisesti merivalvontatutkien kehitystyössä.

2.2 Radioaaltojen eteneminen LOS-järjestelmissä

Suoranäköyhteydellä (Line-of-Sight, LOS) toimivat merivalvontatutkat ovat yleisin tutkatyyppi rannikkovalvonnassa sekä alusasennetuissa järjestelmissä. Ne hyödyntävät tyypillisesti mikroaaltotaajuuksia (yli 30 MHz), joiden oletetaan etenevän suoraviivaisesti. Vaikka termi ”suoranäköyhteys” viittaa esteettömään linjaan tutkan ja kohteen välillä, radioaallon todellinen kulkureitti ilmakehässä on monimutkaisempi. Sekä maan pinta että ilmakehän ominaisuudet muokkaavat signaalin kulkua, vaikuttaen siten merkittävästi tutkan suorituskykyyn. (Kingsley & Quegan 1999, 127.)

Toisin kuin kaukovalvontatutkat, LOS-järjestelmät eivät hyödynnä ionosfääriheijastusta, joten niiden toimintaympäristö rajoittuu ilmakehän alaosiin eli troposfääriin ja stratosfääriin. Troposfääri ulottuu noin 10 kilometrin korkeuteen, ja se on kerros, jossa sääilmiöt, kuten lämpötilan, paineen ja kosteuden muutokset, tapahtuvat. Sen yläpuolella, 10–50 kilometrin korkeudessa on stratosfääri, joka sisältää muun muassa UV-säteilyltä suojaavan otsonikerroksen. Nämä kerrokset ovat keskeisiä LOS-tutkien toiminnalle, mutta eivät merkittävästi vaikuta kaukovalvontatutkissa käytettävien HF-taajuuksien etenemiseen. (Radioaallon eteneminen HF-alueella 2020, 19–21.)

LOS-järjestelmissä signaalin etenemistä muokkaavat erityisesti maanpinnan ja ilmakehän vaikutukset, jotka voivat joko parantaa tai heikentää tutkan havaintokykyä. Näistä keskeisimmät ovat monitie-eteneminen sekä signaalin taittuminen ilmakehässä.

2.2.1 Maanpinnan ja ilmakehän perusvaikutukset

Merenpinnan läheisyydessä toimivien tutkien keskeisin haaste on monitie-eteneminen (multipath). Osa tutkan lähettämästä energiasta etenee suoraan kohteeseen, mutta merkittävä osa heijastuu merenpinnasta ja saapuu kohteeseen hieman eri vaiheessa kuin suora aalto. Nämä kaksi signaalia summautuvat kohteessa, mikä aiheuttaa paikoitellen joko vahvistavaa tai heikentävää interferenssiä. Tämä luo tutkan antennin korkeuskuvioon niin sanottuja monitiekeiloja (multipath

lobes) ja niiden välisiä katvealueita, joissa kohteiden havaitseminen on heikkoa tai mahdotonta. (Skolnik 2008, 1001–1003.)

Normaaliolosuhteissa ilmakehän tiheys ja sitä kautta radiotaittokerroin pienenevät korkeuden kasvaessa. Tämä saa radioaallot taipumaan (refraction) hieman alaspäin maan kaarevuuden mukaisesti. Tämän standarditaipumisen ansiosta tutkan havaintoetäisyys eli tutkahorisontti on itse asiassa noin 15 % pidempi kuin geometrinen horisontti. Lisäksi ilmakehän kaasut sekä erityisesti sade ja sumu aiheuttavat signaalin vaimenemista (attenuation), joka on sitä voimakkaampaa, mitä korkeampaa lähetystaajuutta käytetään. (Richards, Scheer & Holm 2010, 169–172.)

Skolnik (2008) sekä Richards ja muut (2010) korostavat, että vaikka nämä vaikutukset ovat luonnollisia ja ennakoitavia, ne voivat yhdessä aiheuttaa merkittäviä paikallisia virheitä kohteiden havaitsemisessa, etenkin rannikkoympäristössä, jossa lämpötilan ja kosteuden vaihtelut ovat suuria.

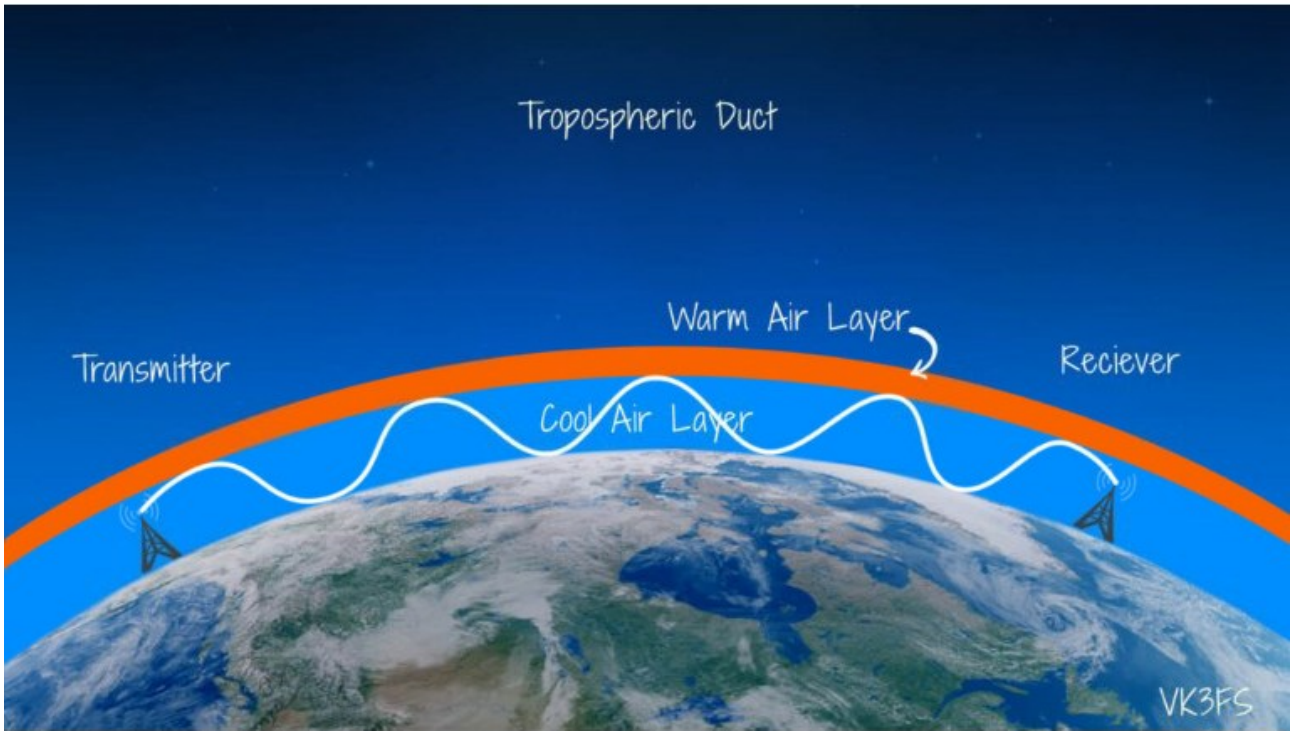
Monitie-eteneminen ja ilmakehän taittovaikutus muodostavat yhdessä merivalvontatutkien keskeisen toimintarajoitteen: niiden havaintokyky voi muuttua merkittävästi jopa paikallisten sääilmiöiden seurauksena. Tämä tekee LOS-tutkista erityisen herkkiä ympäristötekijöiden vaihtelulle verrattuna ionosfääriheijastuksiin perustuvaan OTHR-tekniikkaan. (Skolnik 2008, 1001–1003; Richards ym. 2010, 169–172.)

2.2.2 Anomaalinen eteneminen (kanavoituminen)

Ilmakehän tila ei ole aina vakio, ja erityisesti sääolosuhteet voivat johtaa poikkeuksellisiin etenemisolosuhteisiin (anomalous propagation). Yleisin muoto on superrefraktio, joka voi aiheuttaa ilmakehän kanavoitumista (ducting). Tämä ilmiö syntyy tyypillisesti, kun lämmin ilmakerros asettuu kylmemmän ilmakerroksen päälle muodostaen lämpötilainversion, joka on tyypillinen tilanne suurten merialueiden yllä. Tällöin syntyy troposfäärinen kanava (Tropospheric Duct), joka voi johdattaa radioaaltoja pitkiä matkoja lähes ilman vaimenemista. (Skolnik 2008, 997; Tropospheric Propagation of VHF and UHF radio signals 2024.)

Tähän kanavaan joutuessaan VHF- ja UHF-taajuusalueiden radioaallot voivat jäädä loukkutilaan ja edetä heijastumalla kerrosten ja maan- tai merenpinnan välillä. Näin radioaalto voi kulkea huo-

mattavasti pidemmälle kuin geometrinen horisontti sallisi, joskus satoja kilometrejä. Vaikka kanavoituminen voi lisätä havaintokantamaa, se aiheuttaa tutkajärjestelmille myös virheellisiä havaintoja ja näennäisiä maaleja, sillä signaalit voivat tulla odottamattomista suunnista (Kuvio 1). Harvinaisempi ilmiö on subrefraktio, jossa radioaallot taipuvat ylöspäin, mikä lyhentää havaintokantamaa ja voi aiheuttaa tutkaan ”sokeita” alueita. (Skolnik 2008, 997–999; Tropospheric Propagation of VHF and UHF radio signals 2024.)



Kuvio 1. Troposfäärin kanavoituminen (ducting) (Tropospheric Propagation of VHF and UHF radio signals 2024)

Yhteenvetona voidaan todeta, että anomaalinen eteneminen on kaksiteräinen ilmiö: se voi parantaa tutkan havaintokykyä tietyissä olosuhteissa, mutta samanaikaisesti se heikentää järjestelmän tilannekuvan luotettavuutta. Tämän vuoksi kanavoitumisen tunnistaminen ja kompensointi ovat olennainen osa nykyaikaista signaalinkäsittelyä ja ECCM-suunnittelua.

2.3 Radioaaltojen eteneminen kaukovalvontatutkissa (HF)

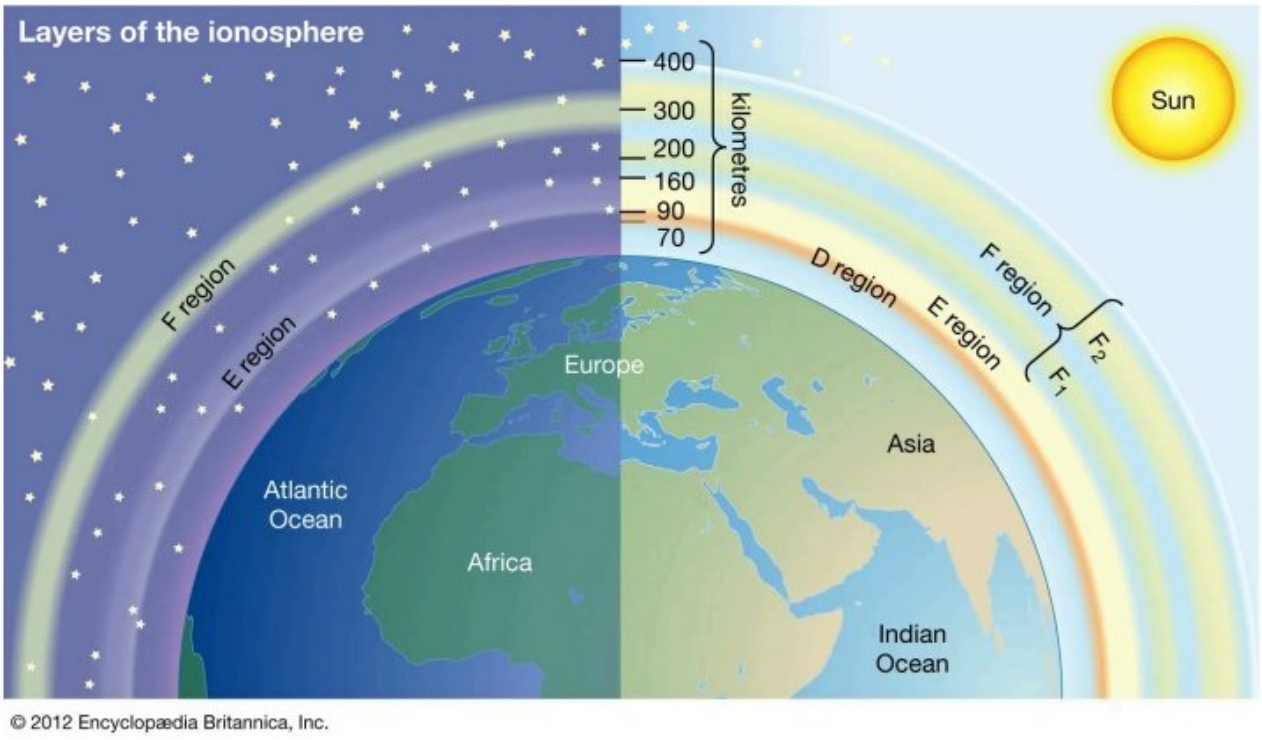
2.3.1 Ionosfäärin rakenne ja kerrokset (D, E, F)

Toisin kuin LOS-tutkat, kaukovalvontatutkat (Over-the-Horizon Radar, OTHR) on suunniteltu havaitsemaan kohteita satojen tai jopa tuhansien kilometrien päässä horisontin takana. Tämä mahdollistetaan hyödyntämällä HF-alueen (3–30 MHz) radioaaltoja, jotka heijastuvat Maan ionosfääristä (Radioaallon eteneminen HF-alueella 2020, 3). Ionosfääri sijaitsee noin 60–1000 km korkeudella ja koostuu Auringon säteilyn ionisoimista kaasukerroksista, jotka taittavat tai heijastavat radioaaltoja takaisin kohti maanpintaa. Ionosfäärin tila on näin ollen ratkaiseva tekijä HF-tutkien suorituskyvylle (Skolnik 2008, 321).

D-kerros (70–90 km) vaimentaa erityisesti alle 10 MHz taajuuksia päiväsaikaan, koska se absorboi energiaa UV- ja röntgensäteilyn ionisoidessa ilmakehää. Yöllä D-kerros katoaa lähes kokonaan, jolloin HF-aallot kantavat kauemmas (Goodman 2010, 97). E-kerros (90–130 km) heijastaa radioaaltoja erityisesti päiväsaikaan ja mahdollistaa yhteydet jopa 2000 km etäisyyksille. E-kerroksen satunnaiset muutokset voivat kuitenkin aiheuttaa signaalin voimakkuuden ja vaiheen vaihtelua, mikä näkyy tutkan epävarmuutena. (Goodman 2010, 98–99.)

E-kerroksen satunnainen muoto, sporadinen Es-kerros, on ohut, mutta erittäin heijastava. Se voi esiintyä paikallisesti ja hetkellisesti, heijastaen jopa VHF-taajuuksia. Tämä tekee siitä merkittävän häiriölähteen tutkajärjestelmille. (Goodman 2010, 114–116.)

F-kerros (130–1000 km) on tärkein pitkien kantamien kannalta. Päivällä se jakautuu F1- ja F2-kerroksiin, joista jälkimmäinen säilyy aktiivisena myös yöllä. F2-kerros on erityisen merkittävä, sillä se mahdollistaa jopa 4000 km kantaman yhdellä hypyllä, mutta on herkkä Auringon aktiivisuudelle ja geomagneettisille häiriöille. (Hunsucker & Hargreaves 2003, 68–72.) Ionosfäärin rakenteen vuorokausivaihtelu on esitetty Kuviossa 2.



Kuvio 2. Ionosfäärin kerrosten vuorokausivaihtelu (Ionosphere and magnetosphere 2024)

Yhteenvetona ionosfäärin kerroksellinen rakenne tekee HF-tutkista samanaikaisesti erittäin tehokkaita ja herkkiä. Luotettava toiminta edellyttää jatkuvaa ionosfäärin seurantaa ja dynaamista taajuudenhallintaa.

2.3.2 Kriittinen taajuus ja sen merkitys

Ionosfäärin heijastusominaisuudet riippuvat taajuudesta. Jokaisella kerroksella on kriittinen taajuus (foE, FoF2), jonka ylittävät signaalit läpäisevät kerroksen palaamatta (Goodman 2010, 97–99). F2-kerroksen kriittinen taajuus vaihtelee voimakkaasti Auringon aktiivisuuden mukaan (tyypillisesti 5–10 MHz, maksimeissa jopa 30 MHz), mikä tekee dynaamisesta taajuudenvalinnasta välttämättömän.

Kriittisten taajuuksien seuranta on keskeinen osa HF-tutkien kalibrointia ja suorituskyvyn hallintaa. Reaaliaikaisia mittauksia varten käytetään ionosondeja, jotka tuottavat ionogrammeja kerrosten tilasta. (Reinisch & Galkin 2011, 377.)

Yhteenvetona, kriittinen taajuus määrittää HF-tutkan tehokkaan toimintaikkunan. Sen jatkuvat vaihtelut tarkoittavat, että automaattinen taajuusoptimointi ja ionosfäärimallit ovat välttämättömiä, jotta tutka pystyy ylläpitämään toimintavarmuutensa.

2.3.3 HF-aaltojen heijastuminen ja taittuminen

HF-tutkien toiminta perustuu aallon taittumiseen, ei täydelliseen heijastumiseen. Kun aalto etenee ionosfääriin, elektronitiheys kasvaa ja aalto alkaa kaartua kohti maata, mikä synnyttää ns. virtuaalisen heijastuksen. (Davies 1990, 45; Hunsucker & Hargreaves 2003, 115.)

Taittumisen voimakkuus riippuu signaalin tulokulmasta ja taajuudesta suhteessa ionosfäärin hetkelliseen tilaan. F2-kerros mahdollistaa pitkän kantaman, mutta D- ja E-kerrokset voivat vaimentaa tai hajottaa signaalia, erityisesti auringon aktiivisuuden ollessa suurta (Impacts: Radio Communications 2024).

Ionosfäärin dynaamisuus tekee HF-tutkien toiminnasta erittäin muuttuvaa. Jatkuva ionosfäärin monitorointi on välttämätöntä, jotta järjestelmät pystyvät säilyttämään luotettavan kantaman ja estämään virheelliset havainnot.

2.3.4 Edistyneemmät etenemismuodot

HF-aallot voivat edetä myös monihyppyisesti (multi-hop) tai kanavoituneina. Jokainen hyppy (ionosfäärin ja maanpinnan välinen heijastus) aiheuttaa vaimennusta, mutta meriveden hyvä johtavuus tekee siitä tehokkaan heijastuspinnan. Tämän vuoksi valtamerialueet tarjoavat OTHR-järjestelmille paremmat edellytykset kuin mantereet. (Davies 1990, 250.)

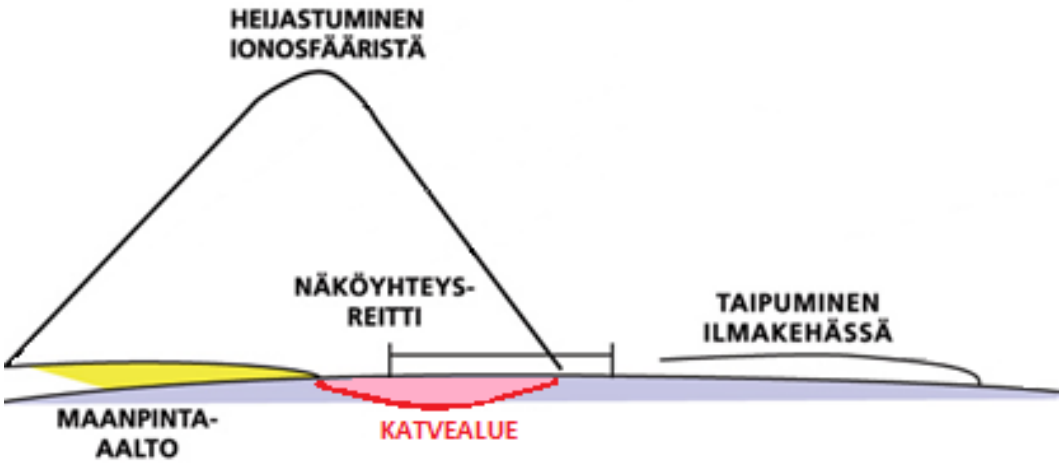
Harvinaisempi etenemismuoto on Chordal Hop, jossa aalto etenee ionosfäärikerroksen sisällä ilman kontaktia maanpintaan. Tämä vähentää häviöitä ja mahdollistaa poikkeuksellisen pitkän kantaman havaintoja, mutta tekee tarkkojen etäisyysarvioiden kalibroinnin vaikeaksi. (Goodman 2005, 201; Davies 1990, 254.)

Nämä monimutkaiset etenemismoodit korostavat, että HF-tutkan suunnittelussa on ymmärrettävä paitsi fysikaaliset rajat myös niiden aiheuttamat virhelähteet. Etenemismoodien vaihtelu on myös

potentiaalinen hyökkäysvektori, jota voidaan hyödyntää esimerkiksi häirintä- tai spoofing-tilanteissa.

2.3.5 Katvealueen (Skip Zone) muodostuminen

Kaukovalvontatutkalle on luonteenomaista, että sen ympärille muodostuu katvealue (skip zone), joka on alue, jolle ei saada havaintoja, koska pinta-aalto ei enää kanna, mutta taivasaalto ei vielä palaudu. Tyypillinen katvealue ulottuu 30–100 kilometrin päähän lähettimestä (Kuvio 3). (Radioaallon eteneminen HF-alueella 2020, 20.)



Kuvio 3. Radioaaltojen etenemisreitit ja katvealue (Radioaallon eteneminen HF-alueella 2020, 4, muokattu)

Katvealue on HF-tutkien merkittävin rakenteellinen rajoite. Se on huomioitava järjestelmäarkkitehtuurissa esimerkiksi sijoittamalla useita asemia päällekkäisiin sektoreihin tai hyödyntämällä sensorifuusiota (tutka + GNSS/AIS), jolloin katveiden vaikutus tilannekuvaan voidaan minimoida.

3 Ympäristön aiheuttamat häiriöt ja niiden vaikutukset

Vaikka tutkajärjestelmien periaatteet ovat selkeät, niiden todellinen suorituskyky riippuu merkittävästi ympäristöstä, jossa ne toimivat. Radioaaltojen matka lähettimestä kohteeseen ja takaisin ei tapahdu tyhjiössä, vaan ilmakehä ja maanpinta muokkaavat signaalia jatkuvasti.

Ympäristön vaikutukset voivat olla sekä ennustettavia että täysin satunnaisia. Ilmakehän kaasut, lämpötilaerot, kosteuden vaihtelut ja avaruussään ilmiöt muuttavat tutkasignaalin kulkua ja voivat aiheuttaa sekä suorituskyvyn heikkenemistä että vääristymiä havaintoihin. Tämän vuoksi tutkatekniikan ymmärtäminen edellyttää sekä fysikaalisten että dynaamisten ympäristötekijöiden huomioon ottamista.

Tässä luvussa käsitellään keskeisimpiä luonnonilmiöiden aiheuttamia häiriöitä ja niiden vaikutuksia sekä suoranäköyhteydellä toimiviin tutkiin että kaukovalvontatutkiin. Luku jakautuu kahteen osaan: ensin käsitellään ilmakehän vaikutuksia LOS-tutkajärjestelmiin ja se jälkeen tarkastellaan avaruussään ja ionosfäärin aiheuttamia häiriöitä kaukovalvontatutkissa.

3.1 Häiriöt LOS-tutkajärjestelmissä

Suoranäköyhteydellä toimivat tutkat eroavat rakenteeltaan ja toimintaperiaatteeltaan merkittävästi HF-taajuuksilla toimivista kaukovalvontatutkista, sillä niiden signaali ei nojaa ionosfäärin heijastukseen vaan etenee suoraan lähettimen ja kohteen välillä. Tämän vuoksi LOS-tutkat ovat luonnostaan immuuneja ionosfäärin tilan ja avaruussään aiheuttamille häiriöille, jotka voivat merkittävästi vaikuttaa HF-signaalien etenemiseen. Tästä huolimatta niiden toimintavarmuus ei ole täysin riippumaton ympäristöolosuhteista. (Skolnik 2008, 981; Radioaallon eteneminen HF-alueella 2020, 4.)

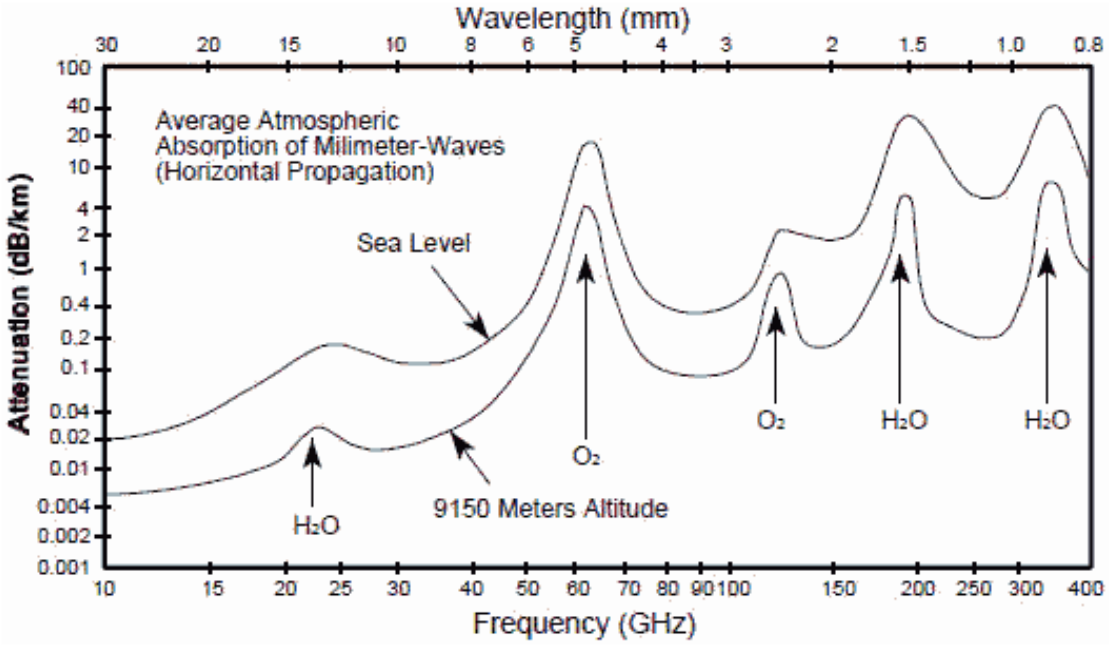
LOS-tutkien etuna on niiden rakenteellinen yksinkertaisuus ja toimintavarmuus ionosfäärin vaihteluista huolimatta, mutta toisaalta niiden suorituskyky on herkkä troposfäärin ja sään vaihtelulle. Ilmiöt, kuten sateen, sumun ja kosteuden aiheuttama signaalin vaimennus, maaston tai vesistöjen pinojen aiheuttamat monitieheijastukset sekä poikkeavat etenemisolosuhteet, kuten troposfäärikanavoituminen (tropospheric ducting), voivat muuttaa signaalin käyttäytymistä olennaisesti.

3.1.1 Ilmakehän vaimennus (sade, sumu, kaasut)

Tutkasignaali menettää aina osan energiastaan edetessään ilmakehän läpi. Tätä energian menetystä kutsutaan vaimennukseksi (attenuation) ja se on yksi merkittävimmistä LOS-tutkien kanta-

maan vaikuttavista tekijöistä. Vaimennus johtuu siitä, että ilmakehän molekyylit ja hiukkaset absorboivat ja sirottavat radioaallon energiaa. Vaimennuksen voimakkuus ilmoitetaan tyypillisesti desibeleinä kilometriä kohden (dB/km). (Skolnik 2008, 995.)

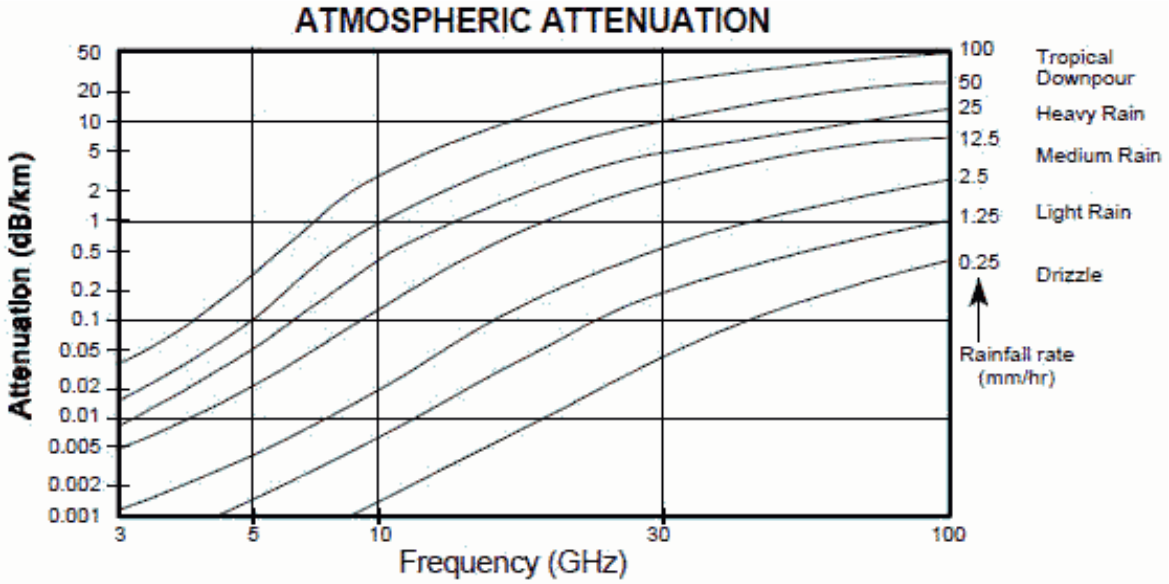
Vaimennuksen aiheuttajat voidaan jakaa kahteen pääryhmään: ilmakehän kaasuihin ja hydrometeoreihin. Ilmakehän kaasut, erityisesti happi (O_2) ja vesihöyry (H_2O), aiheuttavat vaimennusta tietyillä resonanssitaajuuksilla (Skolnik 2008, 995). Kuten kuviosta 4 nähdään, ilmakehän kaasut aiheuttavat vaimennuspiikkejä tietyillä taajuuksilla. Ylempi käyrä kuvaa vaimennusta merenpinnan tasolla ja alempi käyrä 9150 metrin korkeudessa. Vaimennus on korkeammalla vähäisempää, koska ilma on ohuempaa ja siinä on vähemmän vaimentavia molekyylejä, kuten vesihöyryä (Electronic Warfare and Radar Systems Engineering Handbook 2025.)



Kuvio 4. Ilmakehän kaasujen aiheuttama vaimennus eri korkeuksilla (Electronic Warfare and Radar Systems Engineering Handbook 2025)

Usein merkittävämpi vaimennuksen aiheuttaja on kuitenkin hydrometeorit, joilla tarkoitetaan sateen, sumun, pilvien ja lumen sisältämää vettä. Erityisesti sade vaimentaa tutkasignaalia voimakkaasti, koska sadepisarat ovat kooltaan lähellä yleisesti käytettyjen merivalvontatutkien aallonpituuksia. Kuten kuviosta 5 voidaan havaita, vaimennus kasvaa dramaattisesti sekä lähetystaajuuden että sateen voimakkuuden (mm/hr) kasvaessa. Tämä tarkoittaa, että korkealla taajuudella (esim.

X-kaista, > 8GHz) toimivat tutkat ovat alttiimpia sateen aiheuttamalle vaimennukselle, kun taas matalammilla taajuuksilla) kuten L- tai S-kaista) toimivat tutkat ovat sääilmiöille huomattavasti immuunimpia. (Richards ym. 2010, 171–172.)



Kuvio 5. Sateen aiheuttama vaimennus eri taajuuksilla ja sademäärillä (Electronic Warfare and Radar Systems Engineering Handbook 2025)

Vaimennus kasvaa lähes eksponentiaalisesti taajuuden noustessa, erityisesti yli 10 GHz:n alueella, jolloin signaaliin vaikuttavat samanaikaisesti sekä sateen että kaasujen aiheuttamat vaimennusilmiöt. Esimerkiksi vesihöyryllä on selvä absorptiopiikki 22GHz taajuudella, mikä tekee korkeataajuisista järjestelmistä erityisen herkkiä ilmankosteuden vaikutuksille. (Skolnik 2008, 995.)

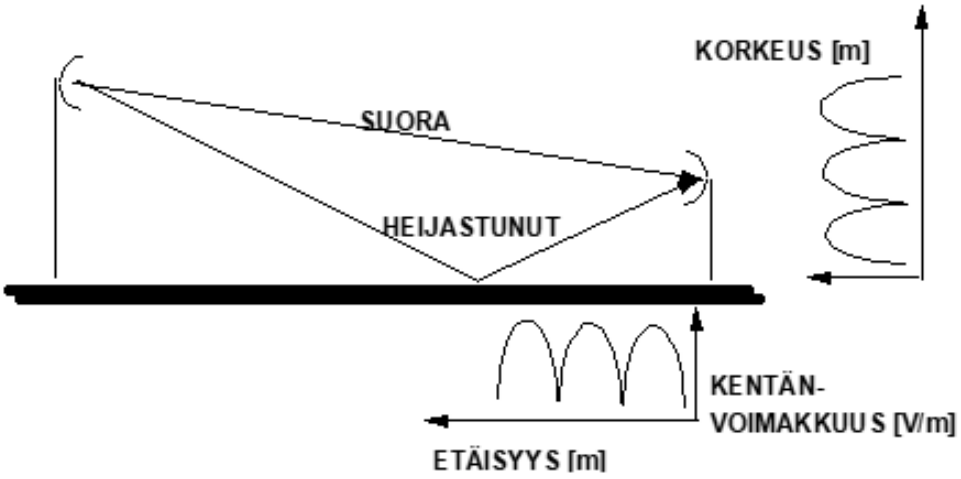
Tämän vuoksi matalataajuiset merivalvontatutkat, kuten S- tai C-kaistalla toimivat järjestelmät, soveltuvat usein paremmin käytettäväksi voimakkaissa sateissa kuin X-kaistalla (>8 GHz) toimivat korkean resoluution järjestelmät. Pilvipisaroiden ja sumun vaikutus korostuu erityisesti silloin, kun pisarakoko on verrannollinen käytettyyn aallonpituuteen, mutta nämä jäävät merkitykseltään selvästi sateen aiheuttamaa vaimennusta vähäisemmiksi. (Richards ym. 2010, 171–172; Skolnik 2008, 1003.)

Lisäksi Pitkäsen (2012, 28) mukaan sade voi aiheuttaa myös ns. varjostusilmiön, jossa voimakas sateen alue tutkan ja kohteen välillä vaimentaa signaalin niin voimakkaasti, että taustalla oleva

kohde ei näy tutkassa lainkaan. Tällöin esimerkiksi voimakkaan sadealueen takana kulkeva laiva voi jäädä täysin näkymättömäksi. Näin ollen tutkasuunnittelussa on välttämätöntä tasapainottaa taajuuden ja resoluution välinen kompromissi siten, että sääolosuhteiden vaikutus pysyy operatiivisesti hyväksyttävänä.

3.1.2 Monitie-etenemisen aiheuttamat katveet

Merenpinnan yllä toimivien LOS-tutkien toinen merkittävä haaste on monitie-eteneminen (multipath). Tutkasignaali etenee kohteeseen kahta reittiä: suoraan sekä merenpinnasta heijastumalla. Nämä kaksi signaalia summautuvat kohteessa ja riippuen niiden välisestä vaihe-erosta, ne joko vahvistavat tai heikentävät toisiaan (Kuvio 6). (Radioaallon eteneminen HF-alueella 2020, 22.)



Kuvio 6. Monitie-etenemisen vaikutus signaalin voimakkuuteen (Radioaallon eteneminen HF-alueella 2020, 22)

Tämä interferenssi-ilmiö luo tutkan pystysuuntaiseen peittoalueeseen sormimaisen rakenteen, joka koostuu voimakkaista havaintoalueista (monitiekeilat) sekä niiden välisistä lähes kuuroista katvealueista. Matalalla lentävä tai liikkuva kohde voi siten ”kadota” tutkan näytöltä ja ilmestyä uudelleen näkyviin edetessään näiden katvealueisen läpi, mikä vaikeuttaa sen jatkuvaa ja luotettavaa seurantaa. (Skolnik 2008, 1001–1003.)

Tämän vuoksi monitie-etenemisen vaikutukset on huomioitava erityisesti rannikkovalvonnassa ja matalilla taajuuksilla toimivissa järjestelmissä. Modernit tutkat hyödyntävät adaptiivisia antennikuvioita ja digitaalista signaalinkäsittelyä, joiden avulla voidaan kompensoida interferenssistä johtuvia peittoaukkoja.

3.1.3 Anomaalisen etenemisen (kanavoitumisen) vaikutukset

Kuten luvussa 2.2.2 kuvattiin, poikkeukselliset sääolosuhteet, kuten inversiokerrokset, voivat aiheuttaa radioaaltojen kanavoitumista (ducting). Tällä ilmiöllä on arvaamattomia vaikutuksia LOS-tutkan suorituskykyyn.

Aallon kanavoituminen voi pidentää tutkahorisonttia sadoilla kilometreillä, mahdollistaen havaintoja kohteista, jotka ovat normaalisti täysin kantaman ulkopuolella (Tropospheric Propagation of VHF and UHF radio signals 2024). Toisaalta tämä ylikantama voi aiheuttaa merkittävää maastokaikua (clutter), kun tutka alkaa nähdä kaukaisia saaria, rannikoita tai jopa toisella puolella merta olevaa liikennettä. Lisäksi kanavan muodostuminen tietylle korkeudelle voi samanaikaisesti aiheuttaa katvealueita lähempänä tutkaa, jolloin normaalin kantaman sisällä olevat kohteet jäävät havaitsematta. (Skolnik 2008, 997–999.)

Koska kanavoituminen on luonteeltaan väliaikaista ja vaikeasti ennustettavaa, se muodostaa merkittävän epävarmuustekijän operatiivisessa merivalvonnassa. Tilannetta voidaan kuitenkin seurata reaaliaikaisesti radioluotausten ja numeeristen säämallien avulla, jolloin poikkeukselliset etenemisolot voidaan tunnistaa sekä huomioida analyysissä. (Skolnik 2008, 997–999.)

3.2 Häiriöt kaukovalvontatutkajärjestelmissä

Kaukovalvontatutkat ovat toimintaperiaatteensa vuoksi immuuneja troposfäärin ilmiöille, kuten sateen aiheuttamalle vaimennukselle, mutta niiden suorituskyky on täysin riippuvainen ionosfäärin tilasta. Ionosfääri on jatkuvassa muutoksessa ja sen aiheuttaman häiriöt ovat merkittävin kaukovalvontatutkan toimintaa rajoittava tekijä. Nämä häiriöt johtuvat pääasiassa avaruussäästä. (Skolnik 2008, 321.)

HF-tutkien toimintaympäristö on siten monikerroksinen ja dynaaminen. Ionosfäärin käyttäytymiseen vaikuttavat auringon aktiivisuus, vuodenaika, maantieteellinen sijainti sekä vuorokaudenaina (Ionosfääri 2015, 12). Näiden ilmiöiden kokonaisuutta kutsutaan avaruussääksi, ja sen ymmärtäminen on keskeistä luotettavien HF-yhteyksien ja kaukovalvontatutkien toiminnan kannalta (Avaruussää 2024).

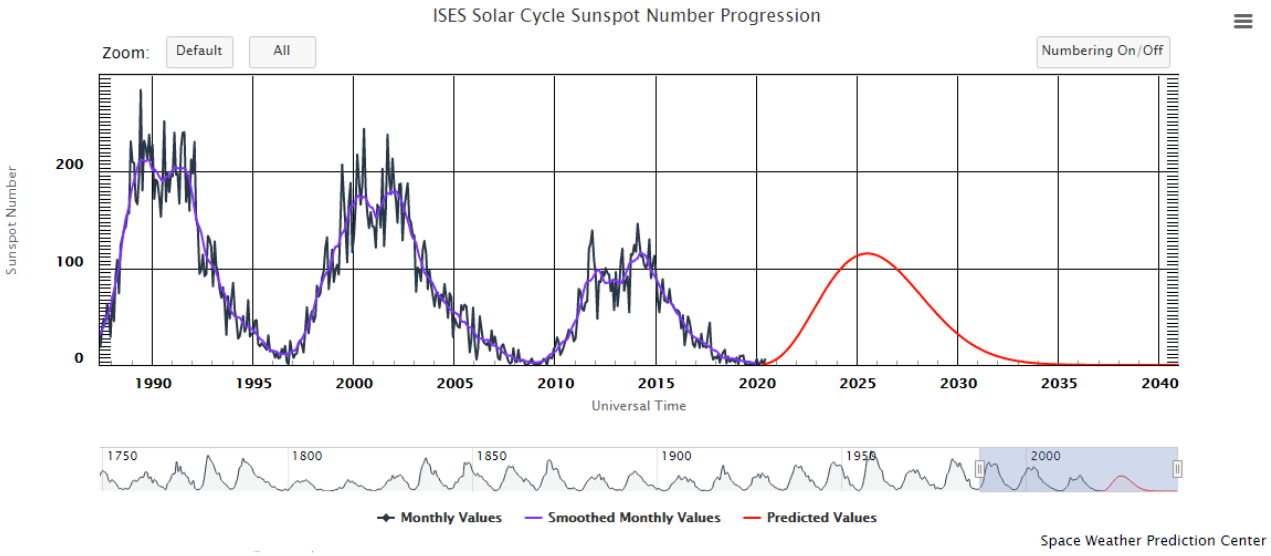
Seuraavissa alaluvuissa tarkastellaan avaruussään vaikutuksia eri mittakaavoissa: ensin Auringon aktiivisuuden aiheuttamia äkillisiä häiriöitä, sen jälkeen paikallisempia ionosfäärisiä ilmiöitä sekä lopuksi niiden kokonaisvaikutusta tutkajärjestelmien suorituskykyyn.

3.2.1 Auringon aktiivisuuden aiheuttamat äkilliset häiriöt

Merkittävin yksittäinen ionosfääriin vaikuttava tekijä on Auringon aktiivisuus, joka ohjaa ionisaatiota ja siten radioaaltojen etenemistä. Auringon aktiivisuutta seurataan useilla indekseillä, joista tärkeimpiä ovat auringonpilkkuluku (SSN, Sunspot Number) ja aurinkovuo (Solar Flux, F10,7). SSN kuvaa Aurinkoon muodostuvien magneettisten aktiivisuusalueiden lukumäärää, kun taas aurinkovuo mittaa Auringosta tulevaa 10,7 cm aallonpituuden (28000 MHz) radiosäteilyä, joka korreloi vahvasti ionosfäärin ionisaatiotason kanssa. (Ionosfääri 2015, 13.)

Auringon aktiivisuus noudattaa noin 11 vuoden jaksoa, jossa pilkkuluku kasvaa minimistä maksimiin ja palaa jälleen minimiin. Tätä syklisyyttä ja nykyisen syklin 25 ennustetta havainnollistaa kuvio 7, joka esittää havaittuja sekä ennustettuja auringonpilkkulukuja ajanjaksolla 1990–2040.

Auringon aktiivisuuden vaihtelut heijastuvat suoraan ionosfäärin heijastus- ja taivutusominaisuuksiin. Korkea pilkkuluku merkitsee voimakkaampaa ionisaatiota, mikä parantaa HF-taajuuksien etenemistä pitkillä kantamilla ja nostaa heijastuskorkeuksia. Vastaavasti matalan aktiivisuuden jaksoina ionosfäärin kantokyky heikkenee, mikä puolestaan vaikeuttaa pitkämatkaista radioliikennettä. (Ionosfääri 2015, 13.)



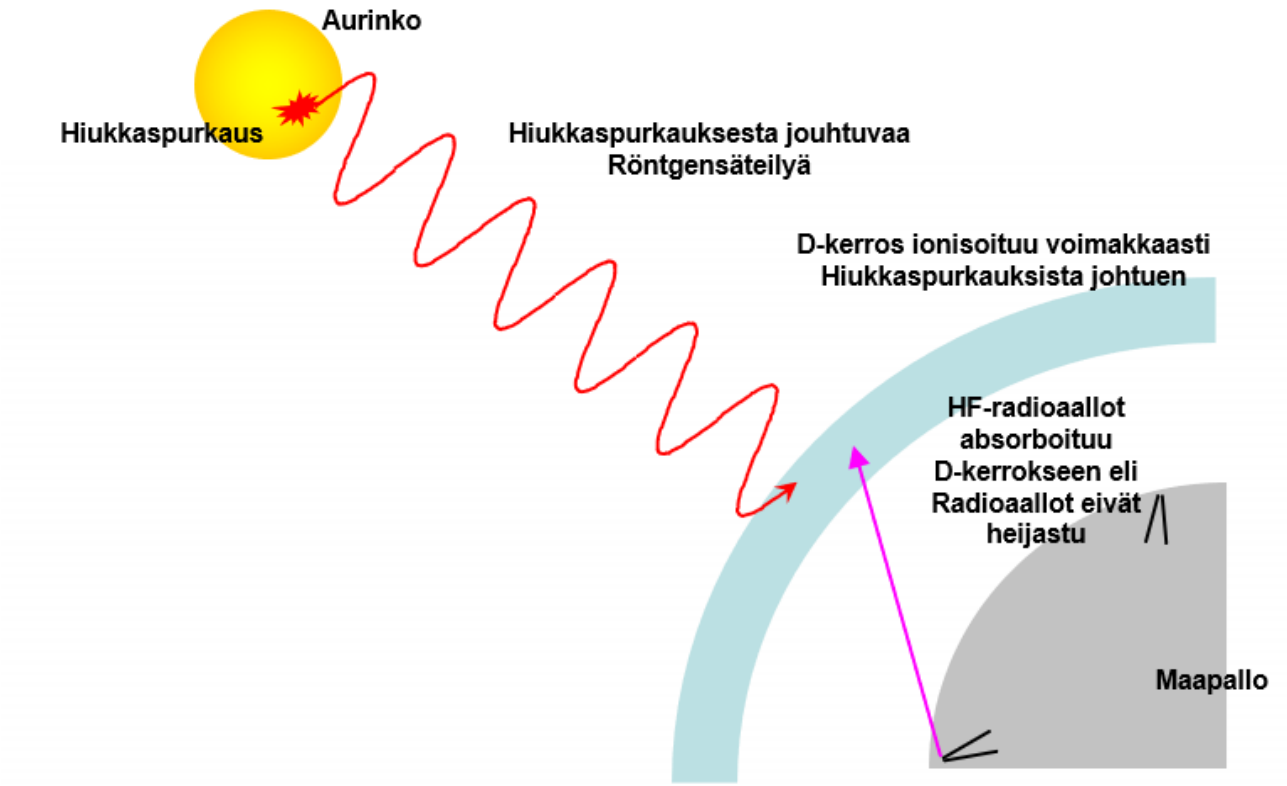
Kuvio 7. Auringonpilkkujen havaittu ja ennustettu vaihtelu 11 vuoden sykleissä (Solar Cycle Progression 2025)

Näiden lisäksi käytetään myös T-indeksiä, joka perustuu Auringon aktiivisuuden lisäksi myös mitattuun tietoon ionosfäärin todellisesta vasteesta Auringon aktiivisuuteen (Ionosfääri 2015, 13).

Auringon aktiivisuuteen liittyy myös äkillisiä, voimakkaita ilmiöitä, kuten auringonpurkauksia (soihdut) ja koronamassapurkauksia (CME). Nämä purkaukset vapauttavat avaruuteen valtavan määrän energiaa ja varautuneita hiukkasia, jotka muokkaavat Auringosta jatkuvasti puhaltavaa hiukkasvirtausta eli aurinkotuulta. Avaruussäähäiriöiden esiintymistiheys noudattaa 11 vuoden sykliä, ollen voimakkaimmillaan auringonpilkkujen maksimin aikaan. (Radioaallon eteneminen HF-alueella 2020, 12.)

Yksi dramaattisimmista avaruussään ilmiöistä on äkillisen auringonpurkauksen aiheuttama radiohäiriö (radio blackout). Purkauksesta lähtevä voimakas röntgensäteily saavuttaa Maan noin kahdeksassa minuutissa ja ionisoi erittäin voimakkaasti ionosfäärin alimman D-kerroksen. Normaalisti vain vaimentava D-kerros muuttuu tällöin lähes läpäisemättömäksi ja absorboi kaikki sitä kohti tulevat HF-aallot. Tämä estää signaalien pääsyn ylempiin heijastaviin kerroksiin, mikä johtaa HF-yhteyksien täydelliseen katkeamiseen koko maapallon päiväpuolella. (Ionosfääri 2015, 16–19.)

Tämän ilmiön vaikutus on havainnollistettu kuviossa 8, jossa nähdään, kuinka äkillinen auringonpurkaus voi ionisoida D-kerroksen niin voimakkaasti, että HF-aallot eivät enää pääse heijastumaan ylempiin kerroksiin.



Kuvio 8. Auringonpurkauksen aiheuttama D-kerroksen absorptio estää HF-aaltojen heijastumisen (Ionosfääri 2015, 18)

Kun voimistunut aurinkotuuli saavuttaa Maan magneettikentän, se voi aiheuttaa geomagneettisen myrskyn. Myrskyn aikana Maan magneettikenttä häiriintyy voimakkaasti, mikä voi muun muassa aiheuttaa revontulia ja merkittäviä häiriöitä ionosfäärin rakenteeseen. Nämä myrskyt voivat aiheuttaa laajoja ja nopeita muutoksia, jotka sirottavat ja vaimentavat tutkasignaalia. Tämä voi johtaa tutkan kantaman lyhenemiseen, tarkkuuden heikkenemiseen ja katvealueen koon ja sijainnin arvaamattomaan vaihteluun. (Goodman 2010, 130; Radioaallon eteneminen HF-alueella 2020, 12.)

Geomagneettisten myrskyjen yhteydessä voi esiintyä ionosfäärisiä häiriöaaltoja eli TIDs-ilmiöitä (Traveling Ionospheric Disturbances), jotka ovat suurikokoisia, aaltomaisia muutoksia ionosfäärin elektronitiheydessä. Nämä häiriöt voivat siirtää tai vääristää tutkasignaalin etenemisreittejä, mikä

näkyy maalin sijainnin vaihteluna tai tutkakuvan epävakautena. Pienempimittakaavaisia vaikutuksia aiheuttaa radiotaajuinen skintillaatio, jossa tutkasignaalin voimakkuus ja vaihe vaihtelevat nopeasti. Tällöin tutkassa havaittavat kohteet voivat ”välkkyä” tai kadota hetkellisesti, mikä vaikeuttaa seurantaa. (Goodman 2010, 130–133.)

3.2.2 Sporadinen E-kerros (Es) ja sen vaikutukset

Avaruussään aiheuttamien laajojen häiriöiden lisäksi tutkajärjestelmien toimintaa voivat sekoittaa paikallisemmat ja ennustamattomat ilmiöt, joista merkittävin on sporadinen E-kerros (Es). Se on E-kerroksen korkeudelle (90–130 km) satunnaisesti muodostuva ohut, mutta poikkeuksellisen tiheästi ionisoitunut sekä voimakkaasti heijastava kerros. Toisin kuin muut ionosfäärin osat, Es-kerros ei synny suoraan Auringon säteilyn vaikutuksesta, vaan sen muodostumisen taustalla ovat tuuli-leikkausten keskittämät metalliset ionit, jotka ovat peräisin meteoriittien hajoamisesta ilmakehässä. (Goodman 2010, 114.)

Kerroksen elektronitiheys voi olla niin suuri, että se heijastaa taajuuksia, jotka normaalisti läpäisisivät koko ionosfäärin, mukaan lukien osan VHF-taajuuksista (30–300 MHz). Merivalvonnassa tämä ilmiö voi aiheuttaa merkittäviä harhatulkintoja. Jos sporadinen E-kerros heijastaa tutkasignaalin normaalin kantaman ulkopuolella olevaan kohteeseen, tutka tulkitsee kaukaisen kohteen virheellisesti lähellä olevaksi maaliksi. Vaikka tämä harhamaaleja tuottava ilmiö on lyhytkestoinen, sen vaikutus tilannekuvan tarkkuuteen voi olla merkittävä ja koska sen tarkkoja muodostumismekanismeja ei täysin ymmärretä, se on merkittävä epävarmuustekijä kriittisissä valvontasovelluksissa. (Goodman 2010, 114–116.)

3.2.3 Vaikutukset tutkajärjestelmien suorituskykyyn

Auringon aktiivisuuden tasolla ja sen aiheuttamilla häiriöillä on suora vaikutus kaukovalvontatutkan suorituskykyyn. Auringonpilkkujen maksimin aikaan ionosfääri on voimakkaammin ionisoitunut, mikä heijastaa paremmin korkeita HF-taajuuksia ja mahdollistaa siten pidemmät ja vakaammat havaintoetäisyydet. Kääntöpuolena on, että myös kaukaa tulevien signaalien aiheuttamat häiriöt lisääntyvät ja voimakkaiden hiukkaspurkausten riski on suurimmillaan. Pilkkuminimin aikaan ionosfääri on heikko, mikä vaikeuttaa yhteyksien muodostumista ja pakottaa käyttämään matalampia taajuuksia. (Radioaallon eteneminen HF-alueella 2020, 8–11; Ionosfääri 2015, 16–19.)

Pienempimittakaavaisia vaikutuksia aiheuttaa skintillaatio, jossa tutkasignaalin voimakkuus ja vaihe vaihtelevat nopeasti ionosfäärin epätasaisuuksien vuoksi. Tällöin tutkassa havaittavat kohteet voivat “välkkyä” tai kadota hetkellisesti, mikä vaikeuttaa seurantaa ja voi heikentää luotettavuutta. (Goodman 2010, 132–133.) Lisäksi paikallisesti syntyvä sporadinen E-kerros (Es) voi hetkellisesti laajentaa tutkan havaintokenttää ennakoimattomasti, mikä voi tuottaa harhamaaleja ja aiheuttaa virheellisiä tulkintoja. (Goodman 2010, 114.)

Luonnolliset ja avaruussään aiheuttamat ionosfäärimuutokset muodostavat merkittävimmän yksittäisen rajoitteen kaukovalvontatutkien luotettavuudelle. Ilmiöiden hallinta edellyttää reaaliaikaista ionosfäärimittausta, adaptiivista taajuudenhallintaa sekä kehittyneitä signaalinkäsittelyalgoritmeja, jotka mahdollistavat tutkan toiminnan muuttuvissa olosuhteissa. Näiden ratkaisujen kehittäminen on myös keskeinen osa kyberturvallisuuden näkökulmasta, sillä luonnollinen ja tahallinen häiriö voivat vaikuttaa järjestelmään samanaikaisesi. Yhteenvetona voidaan todeta, että ionosfäärin ja geomagneettisten ilmiöiden yhteisvaikutus asettaa merkittäviä vaatimuksia tutkan taajuusvalinnalle, antennigeometrialle ja ECCM-menetelmien tehokkuudelle.

4 Suojausmenetelmät ja tekniset ratkaisut

Tutkajärjestelmät ovat yhä enemmän ohjelmisto-ohjattuja ja verkottuneita, minkä seurauksena niiden uhkakenttä ei rajoitu pelkästään sähkömagneettiseen taistelukenttään, vaan ulottuu myös tietoverkkoihin, signaalitasoon sekä järjestelmäintegraatioon. Perinteiset elektronisen sodankäynnin uhkat kuten kohinahäirintä ja harhauttava häirintä muodostavat edelleen ytimen, mutta niiden rinnalle ovat nousseet signaalin väärentäminen (spoofing) sekä ohjelmisto- ja verkkokerroksen hyökkäykset. (Adamy 2015, 50–90; Poisel 2013, 15–38; Skolnik 2008, 1180–1195.)

Nykyaikaisen tutkan toimintaympäristö on siten monikerroksinen sekä monitasoinen. Fyysinen, sähkömagneettinen ja digitaalinen toimintakenttä ovat kietoutuneet yhteen siten, että yhden kerroksen haavoittuvuus voi heijastua koko järjestelmän toimintaan. Tämä on muuttanut myös suojauksen painopistettä: pelkkä radiotaajuinen suojautuminen ei enää riitä vaan tarvitaan integroituja menetelmiä, jotka kattavat koko signaalin ja datan käsittelyketjun. (Adamy 2015, 85–110; Poisel 2013, 25–36.)

Tämän luvun tarkastelussa uhat jaetaan kahteen pääryhmään. Ensimmäisen ryhmän muodostavat radiotaajuiset (RF) uhkat, jotka kohdistuvat suoraan tutkasignaaliin ja sen vastaanottoon. Nämä voidaan edelleen jakaa havaitsemisen estämiseen tehtävään kohinahäirintään sekä tilannekuvan manipulointiin pyrkivään harhauttavaan häirintään ja väärentämiseen. Toisen ryhmän muodostavat järjestelmätason uhat, jotka eivät kohdistu suoraan tutkasignaaliin, vaan hyödyntävät järjestelmän muita haavoittuvuuksia, kuten sen riippuvuutta ulkoisista datalähteistä tai sen ohjelmisto- ja verkkoinfrastruktuuria. (Adamy 2015, 85–110; Poisel 2013, 25–36.)

Edellä kuvattu yhdistelmä tekee tutkajärjestelmistä moniulotteisen suojattavan kohteen. Perinteiset ECCM-menetelmät (taajuushyppy, teho-/suuntausadaptio, signaalin prosessointi) ovat välttämättömiä, mutta eivät yksinään riittäviä. Näiden lisäksi tarvitaan järjestelmätason puolustuskeinoja, kuten signaalin autentikointia, monilähdefuusiota sekä verkon turvallisuuskäytäntöjen vahvistamista. (Adamy 2015, 85–110; Poisel 2013, 25–36.)

4.1 Havaitsemisen estäminen: Kohinahäirintä

Häirintä eli jamming on yksi yleisimmistä elektronisen sodankäynnin (ELSO) vastatoimista. Sen perustavoite on heikentää tai estää tutkan kykyä vastaanottaa ja tulkita kohteista heijastuneita signaaleja. Kohinahäirintä (noise jamming) pyrkii tähän sokaisevaan vaikutukseen lähettämällä voimakasta kohinasignaalia tutkan käyttämälle taajuudelle, jolloin vastaanottimen signaali-kohinasuhde (J/S) heikkenee ja oikeat maalikaiut hukkuvat kohinan alle. (Skolnik 2008, 1180–1195.)

Kohinahäirinnästä on olemassa useita eri muotoja, kuten pistemäinen häirintä (spot jamming), jossa signaali kohdistetaan yhdelle tarkalle taajuudelle, pyyhkäisevä häirintä (sweep jamming), jossa häirintä ”pyyhkii” nopeasti tiettyä taajuuskaistaa sekä laaja-alainen häirintä (barrage jamming), joka kattaa samanaikaisesti suuren taajuusalueen (Adamy 2015, 89–90). Häirinnän tehokkuutta arvioidaan läpipalamisetäisyydellä (burn-through range), joka on etäisyys, jonka sisällä tutkan oma signaali on riittävän voimakas voittaakseen häirinnän (Skolnik 2008, 1185–1189).

Kohinahäirinnän vaikutukset voivat vaihdella suuresti riippuen käytetystä taajuudesta, antennigeometriasta ja ympäristöstä. Esimerkiksi monitie-eteneminen ja heijastukset voivat vahvistaa tai heikentää häirinnän tehoa paikallisesti. Häirinnän vastatoimina voidaan käyttää erilaisia ECCM-

tekniikoita (Electronic Counter-Countermeasures), kuten taajuushypyttämistä, pulssien koodauksia ja suunta-antenneja, joiden tarkoituksena on parantaa tutkan signaali–kohinasuhdetta häiritsevässä ympäristössä. (Poisel 2013, 28–35).

4.2 Tilannekuvan manipulointi: Harhauttaminen ja väärentäminen

Toisin kuin kohinahäirintä, harhauttava häirintä ja väärentäminen (deception jamming & spoofing) eivät pyri sokeuttamaan tutkaa, vaan syöttämään sille virheellistä tietoa uskottavassa muodossa. Tämä perustuu tutkan omien signaalien sieppaamiseen, muokkaamiseen ja uudelleenlähettämiseen siten, että tutkalle syntyy harhamaali tai mittausvirhe. Tavoitteena on manipuloida tilannekuvaa siten, että tutka tulkitsee todellisten kohteiden sijaintia, nopeutta tai liikerataa väärin. (Adamy 2015, 60–80; Skolnik 2008, 1190–1193.)

Tällaiset hyökkäykset haastavat tutkan tiedon luotettavuuden, eivät pelkästään sen herkkyyden. Ne voidaan kohdistaa joko suoraan tutkasignaaliin tai sen käyttämään dataan, kuten navigointiin ja tunnistusjärjestelmiin. Signaalitason hyökkäykset manipuloivat tutkan lähettämää ja vastaanottamaa radiosignaalia, kun taas järjestelmätason hyökkäykset väärentävät tukijärjestelmien, kuten GNSS- tai AIS-datan, sisältöä. (Adamy 2015, 60–80; Poisel 2013, 30–38; Psiaki & Humphreys 2016.)

4.2.1 Signaalitason hyökkäykset: Harhamaalien luonti DRFM-tekniikalla

Yksi kehittyneimmistä tavoista manipuloida tutkaa suoraan on keinotekoisten harhamaalien synnyttäminen. Nykyaikainen teknologia tähän on lähes poikkeuksetta DRFM (Digital Radio Frequency Memory), jonka avulla tutkan lähettämä signaali voidaan tallentaa, muokata digitaalisesti ja lähettää takaisin tutkalle halutuilla parametreilla. DRFM-järjestelmä mahdollistaa signaalin taajuuden, amplitudin, vaiheen ja viiveen tarkan hallinnan, millä voidaan luoda vaikutelma liikkuvista tai staattisista kohteista, joita ei todellisuudessa ole olemassa. (Adamy 2015, 253–256; Poisel 2013, 43–44.)

Kehittyneissä hyökkäyksissä DRFM-järjestelmä voi generoida useita samanaikaisia harhamaaleja, jotka noudattavat johdonmukaista, mutta epäluonnollista liikerataa, kuten ympyrää tai spiraalia. Tällainen hyökkäys ei välttämättä paljastu heti, sillä DRFM kykenee manipuloimaan paluusignaalin taajuutta luoden harhamaalille uskottavan Doppler-siirtymän, jolloin tutka analysoi sen todellisena

liikkuvana kohteena. Tavoitteena voi olla harhauttaa tutkaa lukitsemaan virheellisiä kohteita tai peittää oikea maali signaalien joukkoon. (Skolnik 2008, 1188–1192; Adamy 2015, 93–95.)

4.2.2 Järjestelmätason hyökkäykset: Tukijärjestelmien väärentäminen

Tilannekuvaa voidaan manipuloida myös hyökkäämällä tutkaan integroitujen tukijärjestelmien kimppuun. GNSS-spoofing-hyökkäys muuttaa satelliittipaikannusdatan virheelliseksi ilman, että tutkajärjestelmä välttämättä havaitsee väärää signaalia. Kun väärennetty paikkatieto yhdistetään tutkadataan, se voi siirtää tutkan omaa tai sen havaitsemien kohteiden sijaintia kartalla huomaamattomasti. (Psiaki & Humphreys 2016, 7–9.)

AIS-spoofing puolestaan kohdistuu meriliikenteen automaattiseen tunnistusjärjestelmään ja muokkaa aluksen tunnistetietoja, sijaintia tai nopeutta. Kun tämä manipuloitu data yhdistetään sensorifuusiossa tutkadataan, voi syntyä näennäisesti looginen mutta virheellinen tilannekuva, jossa todelliset ja keinotekoiset kohteet sekoittuvat. (Resiliency in PNT: GNSS Jamming and Spoofing 2025; Countering GNSS Jamming and Spoofing 2025.)

4.2.3 Vaikutukset tilannekuvan eheyteen ja luotettavuuteen

Nykyaikaisen tutkajärjestelmän tilannekuva on monimutkainen fuusio sen omista havainnoista ja ulkoisista datalähteistä. Edellä kuvattujen signaali- ja järjestelmätason hyökkäysten yhdistelmä on erityisen vaarallinen, koska se voi heikentää tilannekuvan eheyttä usealla tasolla samanaikaisesti. DRFM-tekniikalla luodut harhamaalit voivat sekoittua todellisiin kohteisiin niin, että seurantajärjestelmä lukittuu virheellisiin maaleihin, samalla kun väärennetty GNSS- ja AIS-data vahvistaa tätä virheellistä kuvaa. (Adamy 2015, 253–254; Skolnik 2008, 1189–1192.)

Näiden hyökkäysten yhteisvaikutus tekee uhkasta moniulotteisen. Keinotekoiset kohteet voivat houkutella puolustusjärjestelmän toimimaan väärin, jolloin todellinen uhka jää havaitsematta. Spoofingin tunnistaminen perustuu usein poikkeamien havaitsemiseen, kuten liikeratapohjaisiin ristiriitoihin tai epänormaaleihin signaalipiirteisiin. (Countering GNSS Jamming and Spoofing 2023.)

4.3 Järjestelmätason haavoittuvuudet

Tutkajärjestelmien turvallisuus ei rajoitu ainoastaan radiosignaalitasoon kohdistuviin uhkiin, kuten häirintään tai harhamaaleihin. Modernit tutkat ovat osa laajempia tilannekuva- ja johtamisjärjestelmiä, joissa tietoliikenneverkot, ohjelmistot, käyttöliittymät ja ulkoiset datalähteet muodostavat merkittäviä haavoittuvuusalueita. (Poisel 2013, 30–38.)

Nykyaikainen uhkamalli on siten sekä horisontaalinen että vertikaalinen: horisontaalisesti eri järjestelmien välillä ja vertikaalisesti järjestelmän sisällä fyysisestä tasosta ohjelmistoon. Verkkoinfrastruktuurin haavoittuvuudet ovat yksi keskeisimmistä riskeistä, sillä tutkat eivät enää ole eristettyjä saarekkeita. Mikäli liikennettä ei ole suojattu salauksella ja autentikoinnilla, hyökkääjä voi siepata tutkadataa tai syöttää manipuloitua tietoa (Man-in-the-Middle-hyökkäys). Lisäksi palvelunestohyökkäykset (DoS) voivat lamauttaa tutkan verkkoyhteydet ja estää tiedonsiirron johtamisjärjestelmälle. (Stouffer, Pease, Tang, Zimmerman, Pillitteri, Lightman, Hahn, Saravia, Sherule & Thompson 2023.)

Toinen merkittävä uhkavektori liittyy ohjelmistoihin ja laitteistoon. Monet nykyaikaiset tutkat perustuvat kaupallisiin COTS-komponentteihin (Commercial Off-the-Shelf) ja käyttöjärjestelmiin, joissa voi olla tunnettuja haavoittuvuuksia. Jos järjestelmän ohjelmistoja ei päivitetä säännöllisesti, hyökkääjä voi hyödyntää niitä esimerkiksi haittaohjelman asentamiseen. Erityisen riskialtis on toimitusketjuhyökkäys (supply chain attack), jossa takaovi lisätään laitteeseen jo valmistusvaiheessa. Myös suojaamattomat huoltoliitännät ja heikot salasanat voivat tarjota hyökkääjälle pääsyn järjestelmän hallintaan. (Poisel 2013, 34–36.)

Näiden uhkien vaikutus on operatiivisesti sama kuin perinteisen ELSO-hyökkäyksen: tutka voidaan lamauttaa tai sen tilannekuva vääristää — mutta ilman radiotaajuista toimintaa. Tämä tekee havaitsemisesta vaikeampaa ja korostaa kokonaisvaltaisen turvallisuusajattelun merkitystä, jossa suojataan yhtä aikaa sekä sähkömagneettinen että digitaalinen taso. (Stouffer ym. 2023.)

4.4 Tulevaisuuden ratkaisut: Kognitiivinen tutka

Tutkateknologian kehitys etenee kohti järjestelmiä, jotka eivät ainoastaan reagoi ympäristön muutoksiin, vaan myös oppivat sekä sopeutuvat niihin itsenäisesti. Tätä lähestymistapaa edustaa kognitiivinen tutka (Cognitive Radar), joka hyödyntää tekoälyä, koneoppimista sekä adaptiivista signaaliskäsittelyä toimintansa optimointiin. (Gurbuz, Griffiths, Charlish, Rangaswamy, Greco & Bell 2019, 1–3; Skolnik 2008, 1200–1205.)

Kognitiivisen tutkan toimintamalli perustuu havainto–toiminta–palautesilmukkaan (perception–action cycle), jossa tutka analysoi ympäristöään ja säätää parametrejaan reaaliaikaisesti. Näin se kykenee säilyttämään toimintakykynsä muuttuvissa ja häiriöalttiissa olosuhteissa, joissa perinteinen tutka menettäisi tehokkuutensa. (Adamy 2015, 230–232; Poisel 2013, 52–55.)

4.4.1 Adaptiivinen signaalinkäsittely ja tekoäly

Kognitiivisen tutkan ydin on tekoälyssä ja adaptiivisessa signaalinkäsittelyssä, joiden yhteistyö mahdollistaa ympäristön muutoksiin reagoivan toiminnan. Koneoppimiseen perustuvat mallit pystyvät tunnistamaan signaalin poikkeamia ja ennakoimaan häirinnän tai harhamaalien synnyttämät epäjohdonmukaisuudet jo ennen kuin ne heikentävät järjestelmien suorituskykyä. (Reddy & Sinha 2025, 48–52; Adamy 2015, 240–242.)

Tulevaisuudessa neuroverkkopohjaiset ratkaisut mahdollistavat myös kohteiden luotettavuuden arvioinnin automaattisesti, jolloin tutka voi valita optimaalisimman toimintatilan ilman ihmisen välitöntä puuttumista. Tämä parantaa reaktio- ja suorituskykyä, mutta edellyttää samalla läpinäkyvyyttä ja mallien selitettävyyttä, jotta tekoälyn päätöksiä voidaan auditoida ja valvoa myös autonomisissa tilanteissa. (Howard, Shebert, Martone & Buehrer 2023, 4–7; Stouffer ym. 2023, 45–47.)

4.4.2 Yhteistoiminnalliset ja verkottuneet tutkajärjestelmät

Seuraava askel on yhteistoiminnallisten tutkien (collaborative radar systems) laajentuminen, jossa useat sensorit jakavat tietoa ja optimoivat toimintaansa verkottuneessa ympäristössä. Näin voidaan parantaa havaitsemisvarmuutta sekä vähentää yksittäisen järjestelmän haavoittuvuutta (Reddy & Sinha 2025, 53–56).

Verkottunut rakenne kuitenkin lisää tietoturvahaasteita. Tulevaisuuden tutkaverkot vaativat teollisten ohjausjärjestelmien turvastandardeihin perustuvia kerrosrakenteisia ratkaisuja (defence-in-depth), jotka varmistavat toiminnan jatkuvuuden myös kyberhyökkäysten aikana. (Stouffer ym. 2023, 46–48; Gurbuz ym. 2019, 1–3.)

4.4.3 Tutkimuksen tulevaisuus ja sovellusten laajeneminen

Kognitiivisen tutkan kehitys etenee kohti järjestelmiä, jossa tekoäly ja signaalinkäsittely toimivat yhdessä monitasoisessa päätöksenteossa. Tulevaisuudessa nämä järjestelmät pystyvät oppimaan operatiivisista kokemuksista ja jakamaan opittua tietoa muun sensoriverkon kanssa, mikä muuttaa tutkan roolia pelkästä havaintolaitteesta aktiiviseksi päätöksenteon tukijärjestelmäksi. (Gurbuz ym. 2019, 10–12.)

Reddy ja Sinha (2025) korostavat, että jatkotutkimuksen keskeisiä teemoja ovat resilienssi, itseoppivien mallien turvallisuus sekä autonomisten järjestelmien valvonta. Samalla kognitiivisen tutkan sovelluskenttä laajenee siviili- ja avaruustekniikkaan, missä adaptiiviset havainnointimenetelmät mahdollistavat entistä tarkemman seurannan ja resurssien kohdentamisen. Kognitiivinen tutka edustaa näin sekä teknologista että strategista muutosta tutkajärjestelmien suunnittelussa ja toimintaperiaatteissa.

4.5 Yhteenveto

Tässä luvussa tarkasteltiin tutkajärjestelmien suojausmenetelmiä kolmella tasolla: signaalitasolla, järjestelmätasolla ja tulevaisuuden adaptiivisissa ratkaisuissa. Keskeinen havainto on, että tutkien suojaus ei enää perustu yksittäisiin teknisiin keinoihin, vaan moniulotteiseen puolustusrakenteeseen, jossa sähkömagneettinen, ohjelmistollinen ja tietoverkkotaso toimivat yhtenä kokonaisuutena.

Perinteiset ECCM-menetelmät, kuten taajuushyppy ja pulssikoodaus, tarjoavat edelleen tehokkaan ensilinjan suojaa, mutta ne eivät yksin riitä monimutkaisia harhautus- ja väärentämishyökkäyksiä vastaan. Näiden torjuminen edellyttää signaalien autentikointia, monilähteistä datan validointia ja jatkuvaa tilannetietoisuutta, jossa myös ulkoiset tukijärjestelmät, kuten GNSS ja AIS, ovat suojattuja väärentämiseltä.

Samalla on ilmeistä, että tutkien tulevaisuuden turvallisuus perustuu kognitiivisiin ja tekoälypohjaisiin järjestelmiin, jotka kykenevät havaitsemaan ja torjumaan häirinnän autonomisesti. Tämä ei ainoastaan lisää tutkien toimintavarmuutta, vaan myös siirtää niiden roolia passiivisesta havaitsemisesta aktiiviseen päätöksenteon tukemiseen.

Kokonaisuutena luvun johtopäätös on, että tutkien suojaus on siirtymässä reaktiivisesta puolustuksesta kohti ennakoivaa ja adaptiivista toimintamallia. Tämä kehityssuunta luo pohjan myös seuraavalle luvulle, jossa tarkastellaan kokeellisesti, miten eri häiriötyypit vaikuttavat tutkien suorituskykyyn ja mitä suojamekanismeja voidaan mitata ja vertailla käytännössä.

5 Tutkimuksen toteutus ja tulokset

Tässä luvussa esitellään tutkimuksen toteutuksen rakenne, käytetyt menetelmät, simulaatiomallit sekä saadut tulokset. Opinnäytetyö toteutettiin kokeellisena ja soveltavana tutkimuksena, jonka tavoitteena on tuottaa uutta tietoa merivalvontatutkien kyberturvallisuusuhista ja niihin liittyvistä suojausratkaisuista. Tutkimuksen perusidea on yhdistää signaalinkäsittelyn fysikaalinen mallinnus ja kyberturvallisuuden järjestelmätason analyysi yhdeksi kokonaisuudeksi.

Tämä lähestymistapa on valittu, koska tutkajärjestelmien turvallisuus on monikerroksinen ilmiö, jossa sähkömagneettisen spektrin hallinta, ohjelmistoturvallisuus ja dataintegraatio muodostavat toisiinsa kytkeytyvän kokonaisuuden. Perinteisesti tutkien toimintaa on tarkasteltu erillään kyberturvallisuuden näkökulmasta, mutta tämän tutkimuksen tavoitteena on osoittaa, että tekninen ja tietoturvallinen eheys ovat kriittisiä suorituskyvyn kannalta.

Tutkimusstrategia on kokeellinen simulaatiotutkimus, jossa rakennettiin kolme erillistä mallia (Koe A-C) eri uhkatyyppien arvioimiseksi. Jokainen koe havainnollistaa tiettyä hyökkäysmenetelmää, tutkan vasteita siihen sekä potentiaalisia suojausratkaisuja. Tulokset tukevat teoreettista viitekehystä ja auttavat ymmärtämään, miten havaintotietojen luotettavuus ja operatiivinen tilannekuva voidaan turvata myös häiriötilanteissa.

Simulaatioympäristö mahdollistaa todentuntuisen, mutta hallitun tutkimusasetelman. Käytännön kokeita ei ollut mahdollista toteuttaa todellisilla tutkajärjestelmillä operatiivisten turvallisuusrajoitteiden vuoksi, mutta mallinnuksen avulla saavutetaan vertailukelpoisia ja analysoitavia tuloksia. Tulokset ovat siten luotettavia ja toistettavia ominaisuuksia, joita edellytetään teknologiapainoitteisessa tutkimuksessa.

Tutkimuksen eettisyys ja tietoturvallisuus huomioitiin kaikissa vaiheissa. Kaikki käytetyt aineistot ovat julkisia tai avoimesti saatavilla olevia lähteitä. Koodit ja simulaatiomallit on rakennettu itse ja tulosten esityksessä on vältetty turvaluokiteltua tietoa. Lisäksi tutkimuksessa käytetyt viittaukset pohjautuvat luotettaviin tieteellisiin- sekä viranomaislähteisiin.

5.1 Menetelmien kuvaus

Tutkimuksen toteutuksessa hyödynnettiin ohjelmistopohjaista simulaatiomenetelmää, joka perustuu tieteelliseen laskentaan sekä signaalinkäsittelyn mallintamiseen Python-ohjelmointiympäristössä. Simulaatio on validi ja turvallinen tapa tutkia tutkajärjestelmien käyttäytymistä, koska se mahdollistaa häiriö- ja hyökkäystilanteiden tarkastelun ilman todellisia riskejä tai laitteistoja.

Simulaatio on valittu ensisijaiseksi menetelmäksi kolmesta syystä.
1. Toistettavuus ja kontrolli: Virtuaalisessa ympäristössä kaikkia parametrejä voidaan hallita ja muuttaa systemaattisesti, mikä tekee vertailusta luotettavaa.
2. Turvallisuus: Todellisten häirintä- ja harhautuskoeasetelmien suorittaminen olisi operatiivisesti riskialtista ja lainsäädännöllisesti rajoitettua.
3. Analyyttisyys: Ohjelmallinen mallinnus mahdollistaa ilmiöiden erottelin ja yksittäisten tekijöiden vaikutuksen mittaamisen ilman ympäristömelua tai sivuvaikutuksia.

Menetelmän rajoituksena on ympäristön satunnaisuuden puuttuminen ja radiotaajuusolosuhteiden idealisointi, mutta tämä kompensoidaan herkkyysanalyysillä, jossa arvioidaan parametrien vaikutusta tulosten luotettavuuteen (ks. luku 5.3).

Kokeet toteutettiin Python 3.10 -ympäristössä käyttäen seuraavia kirjastoja:

- NumPy (laskenta ja signaalin muodostus)
- SciPy (sovitussuodatus ja Fourier-analyysi)
- Matplotlib (visualisointi ja tulosten kuvaajat)
- Pandas (tulosten käsittely ja tallennus

Kaikki koodi kirjoitettiin modulaarisesti ja jokainen osio (A-C) toteutettiin omana skriptinään. Tämä rakenne mahdollistaa tulosten toistettavuuden ja validoinnin. Kuvien ja datan tallennus suoritettiin automaattisesti tiedostomuodoissa .csv ja .png, jolloin kaikki tutkimuksen vaiheet ovat dokumentoitavissa.

5.1.1 Tutkajärjestelmän mallinnusperiaate

Simulaatiossa mallinnettiin lineaarisesti taajuusmoduloitu (LFM) tutka, joka on tyypillinen merivalvontatutkien aaltomuoto (Richards ym. 2010). Tutkan signaali mallinnettiin kompleksimuotoisena baseband-signaalina, jossa aikatasossa esiintyy amplitudi-, vaihe- ja taajuusmuutoksia. Sovitussuodatus (matched filtering) toteutettiin vastaanottimessa signaalin kaikuja analysoimalla.

Tutkajärjestelmän parametrit asetettiin seuraavasti:

- Kantataajuus 9,5 GHz (X-kaista)
- Kaistanleveys 20 MHz
- Pulssin kesto 50 µs
- Näytteenottotaajuus 80 MHz
- Kohinan teho 0,01 W
- Säädettävä J/S-suhde (häirintäsuhde) 0–20 dB

Näillä parametreilla saatiin tarkka mutta realistinen kuva tutkasignaalin käyttäytymisestä.

5.1.2 Analyysimenetelmät ja luotettavuuden varmistus

Tulosten analyysi toteutettiin kahdella tasolla:

1. Signaalitason analyysi, jossa tarkasteltiin tutkasignaalin amplitudi-, vaihe- ja doppler-ominaisuuksia sekä häirinnän vaikutusta kohteen havaitsemiseen.
2. Järjestelmätason analyysi, jossa tutkittiin sensorifuusion (tutka, GNSS ja AIS) vaikutusta tilannekuvan eheyteen.

Luotettavuuden varmistamiseksi kokeet toistettiin useilla parametriarvoilla ja tulosten keskihajonta analysoitiin. Kunkin kokeen tulokset verrattiin kirjallisuudessa esitettyihin ja julkaistuihin tutkimuksiin. Tämä triangulointi parantaa tutkimuksen sisäistä valideettia ja varmistaa, että tulokset ovat vertailukelpoisia.

5.2 Tapaustutkimuksen / Simulaation tulokset

Tutkimuksen kokeellinen osuus koostui kolmesta erillisestä simulaatiosta (A-C), joiden avulla tarkasteltiin tutkajärjestelmien toimintaa erilaisissa kyber- ja elektronisen sodankäynnin uhkatilanteissa. Jokainen koe toteutettiin samoilla perusparametreilla (luku 5.1.1), mutta eri hyökkäysmallilla. Tulosten avulla pyrittiin arvioimaan tutkajärjestelmien suorituskykyä, havaintokykyä ja tietoturvallisuutta eri tilanteissa.

Simulaatiot eivät ainoastaan osoita tutkasignaalien herkkyyttä häiriöille vaan myös korostavat monikerroksisen puolustuksen merkitystä. Perinteiset ECCM-menetelmät, kuten taajuushypyt tai suunta-antenni eivät yksin riitä, vaan tarvitaan ohjelmistopohjaisia ja tekoälyä hyödyntäviä tunnistusmekanismeja.

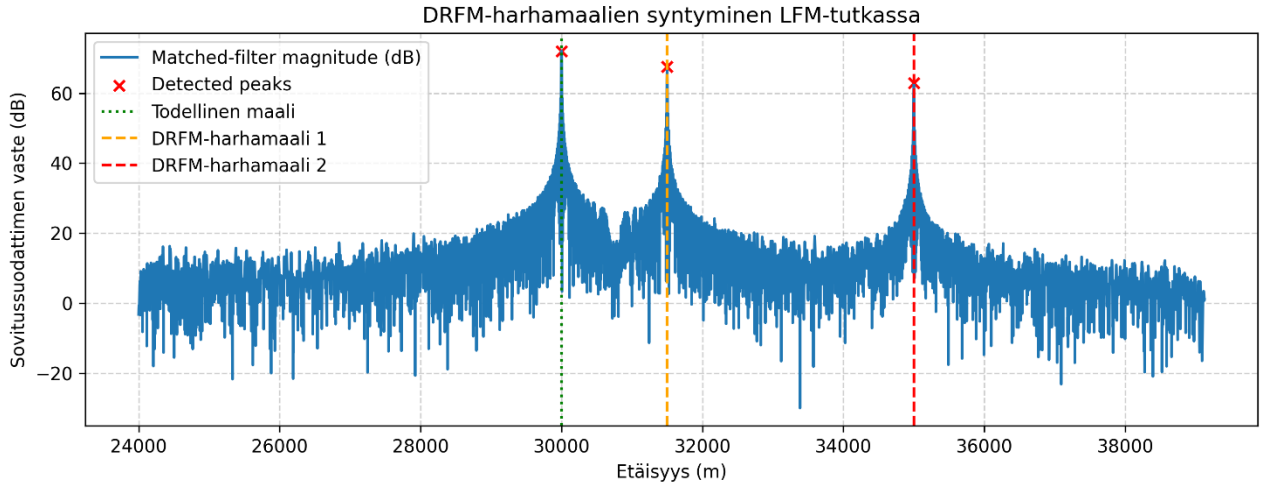
5.2.1 Koe A: DRFM-harhautus (Spoofing Attack)

Ensimmäisessä simulaatiossa mallinnettiin digitaaliseen radiomuistiin (Digital Radio Frequency Memory, DRFM) perustuva harhautus, joka edustaa signaalitason hyökkäystä. DRFM-järjestelmä sieppaa tutkan lähettämän signaalin, tallentaa sen ja lähettää sen takaisin tutkaan viivästettynä ja muokattuna, jolloin tutkalle syntyy keinotekoisia ”harhamaaleja”.

Simulaatiossa mallinnettiin yksi todellinen maali (etäisyys 30 km) ja kaksi keinotekoista harhamaalia, jotka toistettiin viiveillä 1,5 km ja 5 km. Harhamaalien amplitudit asetettiin vastaamaan todellista heijastusta -4,4 dB ja -9,1 dB heikompina, mikä tekee niistä realistisia, mutta havaittavissa olevia.

Sovitussuodattimen (matched filter) tuloksena syntynyt range-profiili osoitti kolme erillistä kaikua: Todellinen maali 30 000 m, ensimmäinen harhamaali 31 500 m, toinen harhamaali 35 000 m. Harhamaalien amplitudit olivat ohjelmallisesti säädetty realistisiksi, mutta selvästi tunnistettaviksi,

mikä vastaa käytännössä havaittuja DRFM-hyökkäysten signaaliprofiileja. Näiden harhamaalien syntyminen sekä suhteellinen amplitudi on esitetty kuviossa 9.



Kuvio 9. DRFM-harhamaalien syntyminen LFM-tutkassa. Todellinen maali (30 km) sekä kaksi harhamaalia (31,5 km ja 35 km), amplitudit -4,4 dB ja -9,1 dB

Tulokset osoittavat, että DRFM-hyökkäys voi tuottaa useita uskottavia maaleja, jotka sekoittuvat todellisiin kohteisiin. Tämä heikentää merkittävästi automaattisen seurantajärjestelmän luotettavuutta, erityisesti jos algoritmit perustuvat pelkkään signaalin voimakkuuteen ja doppler-analyyseihin.

DRFM-harhautus on erityisen vaarallinen siksi, että sen toteuttamiseen ei tarvita suurta lähetysteholoa vaan tarkkaa synkronointia sekä spektrin hallintaa. Tämän vuoksi sen havaitseminen pelkästään amplitudi- tai vaihe-erojen avulla on haastavaa. (Adamy 2015, 93–95; Poisel 2013, 43–44.)

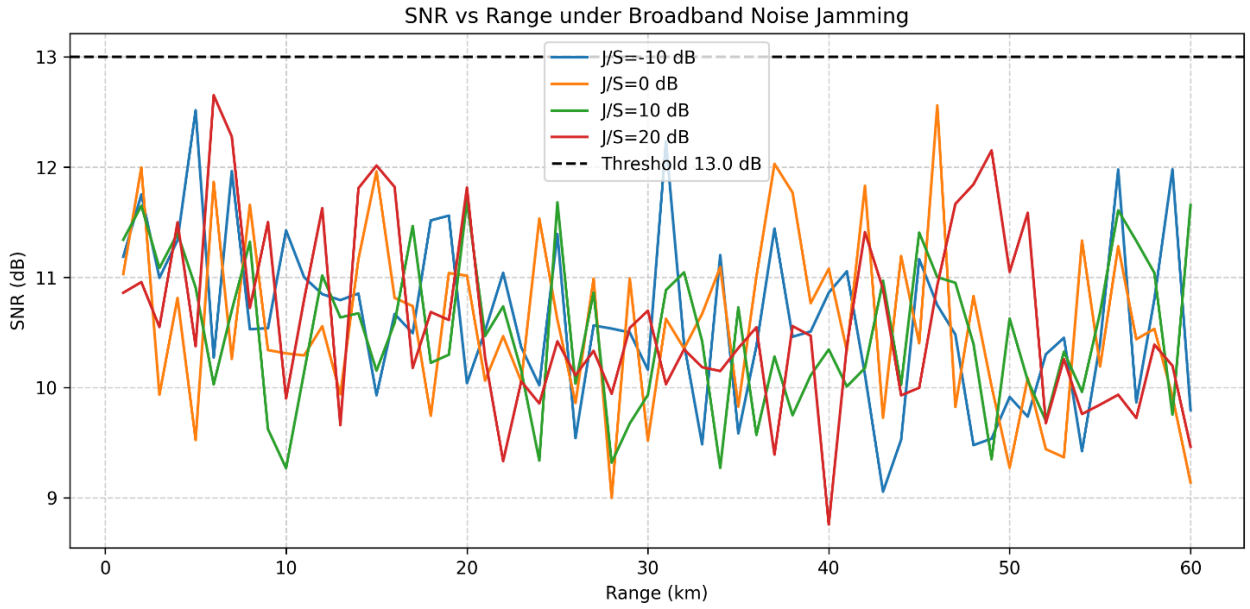
Tutkimuksen kannalta tulokset vahvistavat kirjallisuuden näkemyksen siitä, että signaalitasoinen kyberturvallisuus on tutkajärjestelmissä yhtä tärkeä kuin verkko- tai ohjelmistotason suojaus. Havaitsemisen luotettavuuden parantaminen edellyttää adaptiivisia ECCM-menetelmiä, monilähdefuusioita ja signaalin autentikointia.

5.2.2 Koe B: Kohinahäirintä (Broadband Noise Jamming)

Toisessa simulaatiossa tutkittiin laaja-alaisen kohinahäirinnän vaikutusta tutkajärjestelmän havaintokykyyn. Kohinahäirintä perustuu siihen, että häirintälähetin tuottaa tutkan toimintakaistalle laajakaistaista kohinaa, joka nostaa vastaanottimen kohinapohjaa ja heikentää tutkan signaali-kohinasuhdetta (SNR). Tällöin todellisten kohteiden heijastukset jäävät peittoon ja havaintokyky heikkenee merkittävästi.

Simulaatiossa käytettiin samoja tutkaparametrejä kuin kokeessa A (ks. luku 5.1.1), mutta DRFM-harhamaalien sijaan tutkan vastaanottosignaaliin lisättiin laajakaistainen kohinahäirintä eri voimakkuuksilla. Häirinnän tehoa muutettiin J/S-suhteen (Jammer-to-Signal ratio) mukaan arvoilla −10 dB, 0 dB, 10 dB ja 20 dB, jotka kuvaavat tyypillisiä taktisia tilanteita heikosta kohtalaisen voimakkaaseen häirintään.

Kuviossa 10 esitetään sovitussuodattimen vasteen perusteella laskettu signaali-kohinasuhde etäisyyden funktiona eri J/S-arvoilla. Musta katkoviiva osoittaa 13 dB:n havaitsemiskynnyksen, jota voidaan pitää luotettavan havaintotodennäköisyyden rajana (Skolnik 2008, s. 6–9). Kuvio havainnollistaa, kuinka kohinahäirinnän voimakkuuden kasvu lyhentää tutkan käytännön kantamaa sekä heikentää havaintotodennäköisyyttä.



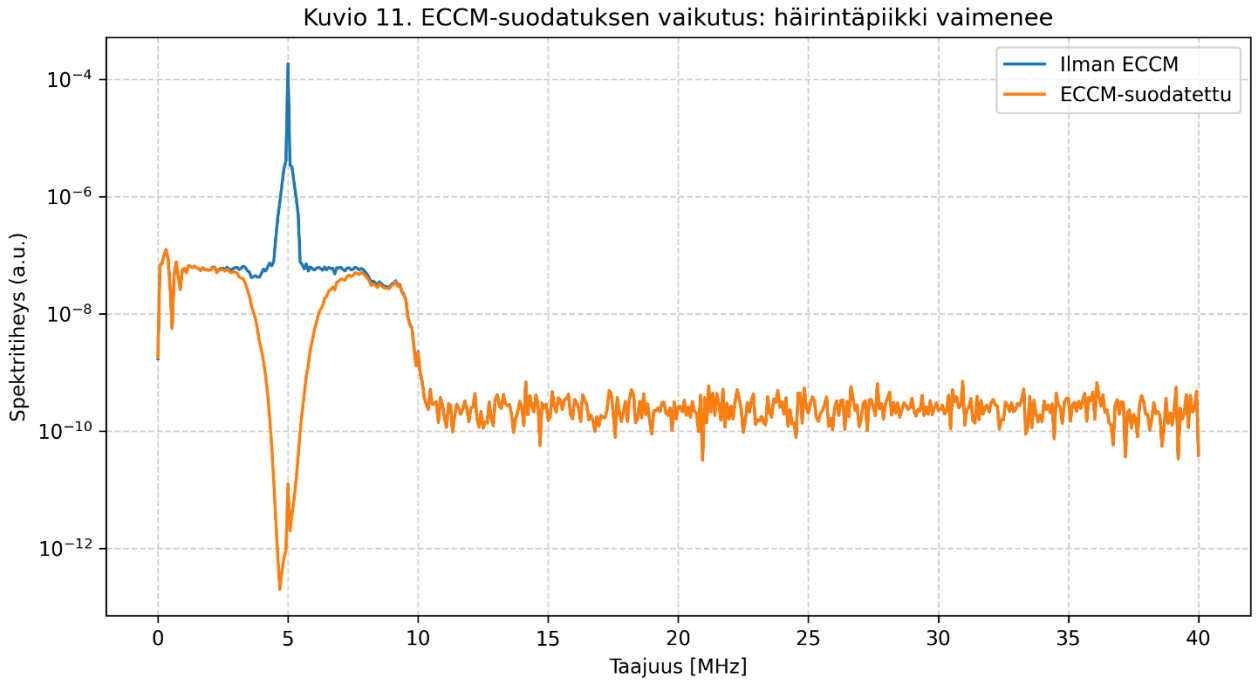
Kuvio 10. SNR etäisyyden funktiona eri J/S-suhteilla (−10, 0, 10 ja 20 dB)

Tulokset osoittavat, että kaikilla J/S-tasoilla SNR jäi selvästi havaintokynnyksen alapuolelle, tyypillisesti 9–12 dB:n tasolle. Tämä tarkoittaa, että tutka ei kykene erottamaan todellisia maaleja, kun koko kaista peittyy kohinahäirintään. Suuremmilla J/S-arvoilla (≥ 10 dB) kohinasignaali dominoi täysin ja burn-through-etäisyyttä ei saavutettu lainkaan.

Tulokset ovat linjassa kirjallisuudessa esitettyjen havaintojen kanssa (Adamy 2015, s. 88–90; Poisel 2013, s. 28–31; Skolnik 2008, s. 14–15), joiden mukaan laaja-alainen kohinahäirintä on yksi tehokkaimmista tutkan toimintaa heikentävistä menetelmistä. Häirinnän vaikutus ei rajoitu yksittäiseen taajuuskomponenttiin, vaan se heikentää koko vastaanottospektrin hyötysuhdetta.

Kokeen B tulokset havainnollistavat, että tutka ei kykene luotettavaan kohteiden havaitsemiseen, jos havaintoprosessi perustuu ainoastaan signaalin amplitudiin ja perinteiseen sovitussuodatukseen. Häirintäympäristössä tällainen menetelmä menettää tehokkuutensa ja tutka tarvitsee adaptiivisia ECCM-ratkaisuja selviytyäkseen. Käytännössä tämä tarkoittaa sitä, että tutkan on kyettävä mukauttamaan vastaanottotapaa ja signaalinkäsittelyä reaaliaikaisesti häirintätilanteen mukaan. Tehokkaita keinoja tähän ovat esimerkiksi kapeakaistainen vastaanotto, taajuushyppytekniikka sekä kohinasuodatus spektrianalyysin avulla. Näiden menetelmien avulla tutka voi suodattaa häirinnän vaikutuksia ja säilyttää havaintokykynsä myös tilanteissa, joissa kohinahäirintä olisi muuten lamauttava.

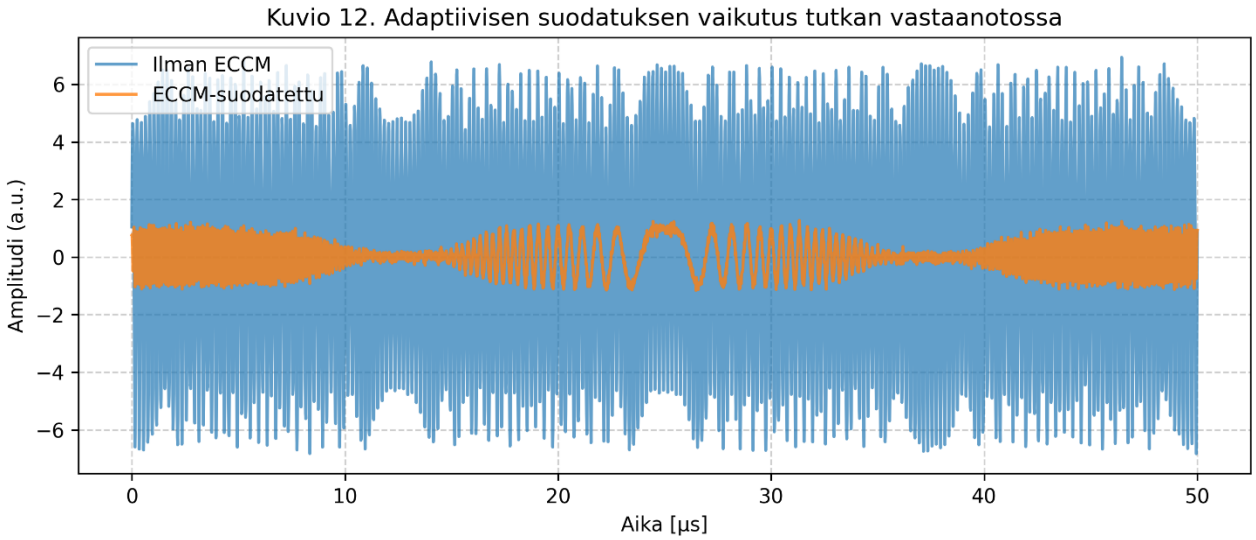
Simulaatiota laajennettiin havainnollistamaan, miten yksinkertainen spektripohjainen adaptiivinen ECCM-toimenpide voi palauttaa tutkan havaintokyvyn laaja-alaisen kohinahäirinnän alla. Käytännössä koodimuutokset olivat seuraavat: vastaanotetun LFM-pulssin käsittelyyn lisättiin simuloitu laaja-alainen kohinahäirintä (jammer) ja tämän jälkeen toteutettiin notch-tyyppinen kapeakaistainen band-stop-suodatin, jonka keskitaajuus säädettiin häirintäkomponentin kohdalle. Spektrianalyysilla (spectrogram) ja aika-alueen visualisoinnilla verrattiin tilannetta ennen ja jälkeen suodatuksen. Suodattimen pääparametrit (keskitaajuus ja Q-arvo) valittiin siten, että vaikutus on selektiivinen eikä leikkaa pois merkittävää osa-aluetta LFM-pulssin hyödyllistä spektriä. Näiden vaikutus näkyy kuviossa 11, jossa vertaillaan spektrin rakennetta ennen ja jälkeen ECCM-suodatuksen.



Kuvio 11. ECCM-suodatuksen vaikutus: häirintäpiikki vaimenee

Kuvio 11 esittää vastaanotetun signaalin keskimääräisen spektritiheyden ennen (sininen) ja jälkeen (oranssi) adaptiivisen notch-suodatuksen. Huomattava häirintäpiikki n.5 MHz:n kohdalla vaimenee suodatuksen jälkeen usealla desibelillä, samalla kun muun spektrin rakenne säilyy. Tämä osoittaa, että häirintäenergia voidaan poistaa selektiivisesti ilman, että tutkalle tärkeä signaalisisältö kärsii.

Jotta ilmiöstä saadaan kokonaiskuva, kuvio 12 havainnollistaa saman ECCM-suodatuksen vaikutuksen aika-alueella, missä pulssin rakenteen palautuminen on nähtävissä suoraan aaltomuodosta.



Kuvio 12. Adaptiivisen suodatuksen vaikutus aika-alueella

Kuvio 12 näyttää vastaanotetun LFM-pulssin aika-alueella ennen (sininen täyte) ja jälkeen (oranssi) suodatuksen. Ilman ECCM:ää häirintä peittää pulssin rakenteen ja kasvattaa kohinatasoa huomattavasti, kun taas suodatuksen jälkeen pulssin modulaatiorakenne ja amplitudielementit tulevat erotettaviksi. Tämä palauttaa sovitussuodatuksen ja muiden havaitsemisalgoritmien edellyttämän SNR-rakenteen. Käytännössä tutkalla on jälleen mahdollisuus saavuttaa luotettava havaitseminen.

Edellä esitetty yksinkertainen demonstraatio havainnollistaa käytännön periaatteen: reaaliaikainen, spektriin perustuva suodatus voi merkittävästi parantaa tutkan suorituskykyä häirintätilanteessa ilman lisälähetystehoa tai laiteprosessien muutoksia. Tulokset tukevat kirjallisuudessa esitettyä käsitystä adaptiivisen ECCM-menetelmän keskeisyydestä merivalvontatutkissa (Adamy 2015; Poisel 2013) ja osoittavat, että ohjelmistopohjaiset suojaukset tarjoavat kustannustehokkaan tavan lisätä järjestelmän resilienssiä. Kuvioiden numeerinen data (spektrianalyysi ja aika-alueen aaltomuoto) on tallennettu tutkimuksen tulostiedostoihin ja toimii suoraan todennettavuutena esitetylle väitteelle.

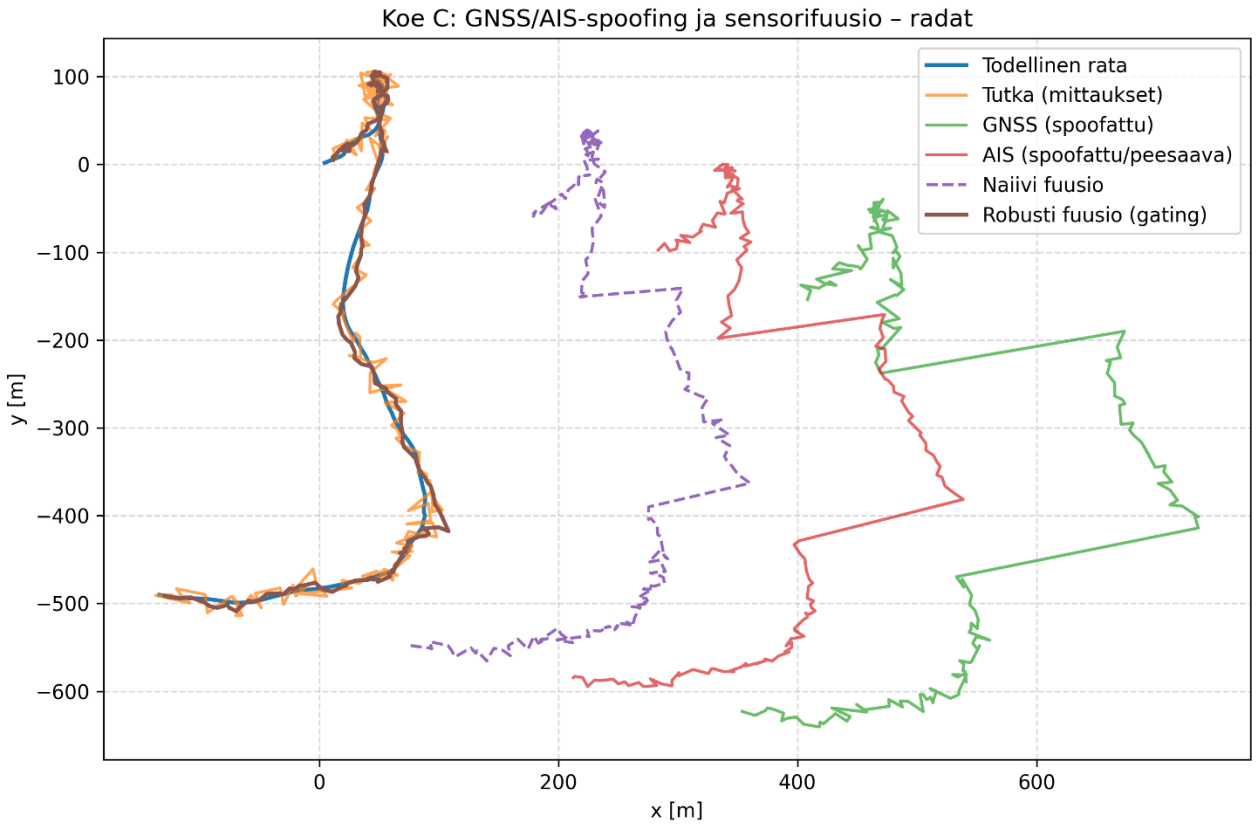
5.2.3 Koe C: GNSS/AIS-spoofing ja sensorifuusio

Koe C mallinsi järjestelmätason väärentämishyökkäyksen vaikutusta tilannekuvan muodostukseen. Simulaatiossa todellinen kohde seurasi jatkuvaa 2D-rataa; tutka tuotti ei-spoofattuja havaintoja, kun taas GNSS-kanava mallinnettiin sisältämään noin 400 metrin biasin, pienen lineaarisen driftin

sekä ajoittaisen hyppäyksen. AIS-mittaukset puolestaan peesasivat osittain GNSS-virhettä (aste ≈ 70 %), mikä teki niistä erityisen vaarallisia naiivissa fuusiomenetelmässä.

Fuusioiden vertailuun toteutettiin kaksi lähestymistapaa: painotettu keskiarvo sekä robusti Kalman-pohjainen fuusio, jossa kukin sensoripäivitys hyväksyttiin vain, jos per-sensorinen Mahalanobis-etäisyys jäi asetetun kynnystason alle (gate = 7.8).

Näiden menetelmien tuottamat radat ja mittausjoukot esitetään kuviossa 13, jonka avulla voidaan suoraan vertailla naiivin ja robustin fuusion käyttäytymistä spoofing-tilanteessa.

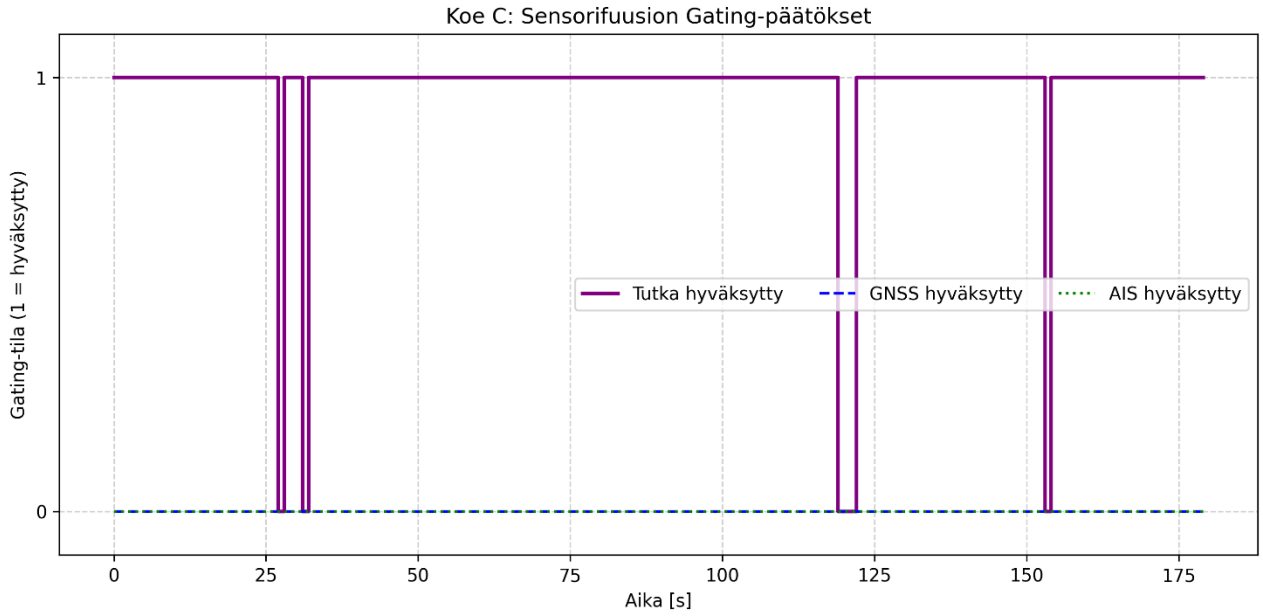


Kuvio 13. Keskeiset trajektoriat: todellinen rata, tutkan mittaukset, spoofattu GNSS, peesaava AIS, naiivi fuusio ja robusti fuusio

Kuviosta 13 havaitaan selvästi, että naiivi fuusio seuraa voimakkaasti GNSS/AIS-spoofattua dataa ja antaa siten virheellisen tilannekuvan. Robusti fuusio sen sijaan pysyy lähellä todellista rataa, koska epäjohdonmukaiset GNSS/AIS-havainnot hylätään ennen tila-arvion päivittämistä. Tämä ero näkyy

johdonmukaisesti koko simulaatiojakson ajan ja korostuu erityisesti spoofauksen aktivoituessa (drift ja hyppy).

Jotta sensorifuusion toimintaa voidaan arvioida tarkemmin, erityisesti yksittäisten mittausten hyväksymisen ja hylkäämisen osalta, kuviossa 14 esitetään robustin Kalman-suodattimen gating-päätökset koko simulaation ajalta. Kuva havainnollistaa, miten jokainen tutka-, GNSS- ja AIS-mittaus luokitellaan joko hyväksytyksi (tila 1) tai hylätyksi (tila 0) tilastollisen konsistenssitestin perusteella. Näin voidaan vertailla, miten fuusioalgoritmi reagoi spoofattuihin signaaleihin suhteessa luotettavaan tutkadataan.



Kuvio 14. Sensorifuusion Gating-päätökset. Robusti Kalman-suodatin hyväksyy tutkamittaukset ja hylkää spoofatut GNSS- ja AIS-havainnot

Spoofauksjakson aikana GNSS-mittaukset hylätään toistuvasti, ja myös AIS-mittauksista nähdään ajoittaisia hylkäyksiä, kun ne poikkeavat tutkan odotetusta referenssistä. Tutkamittaukset hyväksytään johdonmukaisesti, mikä korostaa tutkan roolia luotettavana lokaalisena referenssinä fuusiojärjestelmässä. Yhdessä kuvioiden 13 ja 14 antama data osoittaa, että järjestelmätason puolustusmekanismit, erityisesti mittauskonsistenssin testaaminen ennen fuusiota, ovat tehokas tapa rajoittaa GNSS/AIS-spoofingin vaikutusta tilannekuvaan.

Tulosten numeerinen tarkastelu vahvistaa visuaaliset havainnot. Laskettaessa keskimääräinen paikannusvirhe (Root Mean Square Error, RMSE) todellisen radan ja fuusioarvon välillä, naiivin fuusion virhe oli 405,2 metriä, kun robustin fuusion virhe jäi vain 37,8 metriin. Tämä lähes kymmenkertainen ero osoittaa, että gating-mekanismi onnistui tehokkaasti estämään väärien GNSS/AIS-havaintojen vaikutuksen järjestelmätason päätöksiin. Ero on erityisen merkittävä, koska käytetty robusti menetelmä ei perustu signaalitasoiseen tunnistukseen vaan puhtaasti tilastolliseen mittauksen konsistenssiin, mikä tekee siitä skaalautuvan ja siirrettävän eri sensorifuusiokehityksiin.

Kokeen C tulkinta on selkeä, mutta vaikutukseltaan merkittävä: pelkkään signaalien absoluuttiseen arvoon tai yksinkertaiseen painotettuun fuusioon perustuva järjestelmä voi olla altis vakaville operatiivisille virhetulkinnoille, kun taas robusti fuusio, joka hyödyntää riippumatonta sensoria (tutka) ja konsistenssitestausta, säilyttää tilannekuvan eheyden. Tämä tulos korostaa työn aiemmissa luvuissa esitettyä johtopäätöstä: suojauksen on oltava monikerroksista. Signaalitason suojausten (Koe A/B) lisäksi tarvitaan järjestelmätason mekanismeja, kuten mittauksen validointi ja robustit estimaattorit, jotta tilannekuva pysyy luotettavana myös kyberhyökkäyksen alla.

Tulokset tukevat Psiaki ja Humphreysin (2016) kaltaista kirjallisuutta, joiden mukaan GNSS-spoofingin vaikutukset voidaan osittain kompensoida järjestelmätason mekanismein, erityisesti silloin, kun käytössä on riippumaton sensorireferenssi (esimerkiksi tutka) ja mittausten luotettavuuden arviointi. Käytännön suosituksena voidaan todeta, että sensorifuusiomenetelmiin tulisi sisällyttää robustit konsistenssitestit ja mittausten painotusluokitukset sekä säilyttää tutka ensisijaisena referenssinä automaattisessa päätöksenteossa.

5.3 Tulosten koonti ja analyysi

Tutkimuksen kolmen kokeen (A-C) tulokset muodostavat kokonaisuuden, joka havainnollistaa tutkajärjestelmien toiminnallista haavoittuvuutta ja puolustusmekanismeja eri uhkatasoilla. Kokeet etenevät loogisesti signaalitasolta järjestelmätasolle: koe A keskittyi DRFM-harhautukseen, koe B kohinahäirintään ja koe C järjestelmätason spoofing-hyökkäykseen sensorifuusiota vastaan. Näiden rinnastaminen mahdollistaa kokonaisvaltaisen kuvan siitä, miten tutkajärjestelmien eheyteen sekä luotettavuuteen voidaan vaikuttaa eri tasoilla ja millä teknisillä ratkaisuilla niiden häi-

riönsietokykyä voidaan parantaa. Tulokset osoittavat, että monilähteinen fuusio parantaa häiriönsietoa merkittävästi, mutta edellyttää jatkuvaa kalibrointia, jotta väärät korrelaatiot eivät aiheuta harhamaaleja.

Koe A osoitti, että DRFM-hyökkäys voi tuottaa tutkan mittausprofiiliin täysin uskottavia harhamaaleja, jotka sekoittuvat todellisiin kohteisiin. Tämä vahvisti käsityksen siitä, että signaalitasoinen harhautus on edelleen yksi vaikeimmin tunnistettavista uhista. Vaikka amplitudi- ja vaihe-erot ovat teoreettisesti havaittavissa, käytännössä niiden analysointi reaaliajassa vaatii laskennallisesti raskasta signaalin autentikointia ja useiden rinnakkaisten havaintokanavien käyttöä. Tutkimuksen tulokset tukevat Adamyn (2015) ja Poiselin (2013) esittämiä havaintoja siitä, että DRFM-harhautuksen tehokkuus perustuu sen kykyyn jäljitellä tutkan omaa aaltomuotoa lähes täydellisesti. Käytännön johtopäätös on, että perinteiset ECCM-keinot, kuten taajuushyppy tai pulssikoodaus, eivät yksin riitä vaan tarvitaan spektrianalyysiin ja adaptiiviseen tunnistukseen perustuvia ratkaisuja.

Koe B laajensi tarkastelun jatkuvaan kohinahäirintään, joka eroaa harhautuksesta siten, että se ei vääristä mittausdataa vaan heikentää havaitsemisen perusedellytyksen eli signaali-kohinasuhteen (SNR). Tulokset osoittivat, että perinteinen sovitussuodatus menettää tehokkuutensa, kun J/S-suhde kasvaa yli 10 dB:n. Tällöin todelliset kohteet peittyvät lähes kokonaan kohinapeiton alle. Kuitenkin kun käyttöön otettiin adaptiivinen ECCM-suodatus (bandstop/notch filter) ja taajuushyppy, tutka kykeni osittain palauttamaan havaitsemiskykynsä. Tämä tulos on merkittävä, sillä se osoittaa käytännön tasolla, että häirinnän vaikutusta voidaan kompensoida ohjelmallisesti ilman lähetystehojen kasvattamista. Kokeen B perusteella voidaan todeta, että tutkajärjestelmien häirinnänsietokyky perustuu ennen kaikkea vastaanottimen älykkyyteen, ei pelkästään signaalin voimakkuuteen. Tulokset tukevat Reddyn ja Sinhan (2025) näkemyksiä siitä, että tulevaisuuden tutkajärjestelmät tulevat nojaamaan kognitiivisiin ECCM-algoritmeihin, jotka pystyvät mukauttamaan signaalinkäsittelystrategiaansa reaaliaikaisesti havaittujen uhkien mukaan.

Koe C siirsi tarkastelun järjestelmätasolle ja osoitti, että uhkia ei tule tarkastella ainoastaan sähkömagneettisen spektrin näkökulmasta. GNSS- ja AIS-järjestelmiin kohdistuva spoofing osoittautui yhtä vaaralliseksi kuin radiotaajuiset hyökkäykset, sillä se pystyi vääristämään tilannekuvaa ilman,

että yksikään tutkasignaaliin kohdistuva häiriö havaittiin. Naiivissa sensorifuusiossa väärä paikkadata ohjasi koko järjestelmän harhaan, kun taas robusti Kalman-fuusiomenetelmä säilytti todellisen kohteen sijainnin. Kuten tarkempi numeerinen analyysi osoitti, robustin fuusion keskimääräinen paikannusvirhe (RMSE) jäi 37,8 metriin, kun taas naiivin fuusion virhe oli yli 400 metriä. Tämä koe osoitti selvästi monilähteisen dataintegraation riskit, mutta samalla sen potentiaalin: jos fuusiomekanismi on suunniteltu oikein, se toimii myös tehokkaana suojamekanismina datan väärentämistä vastaan. Tulokset ovat linjassa Gurbuzin ja muiden (2019) esittämän kognitiivisen tutkan käsitteen kanssa, jonka mukaan järjestelmä oppii ja sopeutuu uhkien perusteella parantaen luotettavuuttaan jatkuvasti.

Yhdessä tarkasteltuna kokeiden tulokset osoittavat, että tutkajärjestelmien kyberturvallisuus on monikerroksinen kokonaisuus, jossa yksittäinen suojausmenetelmä ei riitä. Signaalitason suojaus (kuten ECCM) on tehokas vain, jos järjestelmätason eheys on varmistettu, ja päinvastoin. Lisäksi tulokset vahvistavat teoreettista oletusta, jonka mukaan häiriönsietokyky ei ole pelkkä tekninen ominaisuus vaan järjestelmätason suunnitteluvalinta. Käytännössä tämä tarkoittaa, että tutkajärjestelmän suorituskyky ei enää riipu yksittäisen komponentin tehosta vaan sen kyvystä havaita, päätellä ja mukautua dynaamiseen uhkaympäristöön.

Tutkimuksen kontribuutio on kaksitasoinen. Ensinnäkin se tuottaa kokeellista näyttöä siitä, miten eri häirintätyypit vaikuttavat tutkajärjestelmien havaintokykyyn ja miten nämä vaikutukset voidaan osittain kompensoida ohjelmallisesti. Toiseksi se yhdistää signaalitason ja kyberturvallisuuden näkökulmat yhteiseen analyysikehykseen, jota voidaan hyödyntää jatkossa tutkajärjestelmien suunnittelussa, testauksessa ja puolustuksellisessa arvioinnissa. Tulokset tukevat käsitystä, että tulevaisuuden merivalvontatutkat ovat entistä enemmän ohjelmistopohjaisia ja kognitiivisia järjestelmiä, jotka pystyvät tunnistamaan poikkeamia ja oppimaan häiriöympäristön piirteitä automaattisesti.

Näiden havaintojen perusteella voidaan lopuksi todeta, että tutkajärjestelmän luotettavuus on yhtä vahva kuin sen heikoin integraatiokerros. Häiriöiden torjunta ja kyberuhkien hallinta eivät ole erillisiä tehtäviä vaan osa yhtä ja samaa turvallisuusarkkitehtuuria. Tämä tutkimus osoittaa, että monitasoinen, adaptiivinen ja tietopohjainen lähestymistapa on välttämätön, jotta merivalvontatutkat voivat säilyttää toimintakykynsä myös muuttuvassa ja vihamielisessä toimintaympäristössä.

6 Pohdinta ja johtopäätökset

Kokonaisuutena tutkimus osoitti, että tutkajärjestelmien toimintaympäristö on yhä moniulotteisempi, eikä järjestelmän luotettavuus määräydy enää pelkästään radioteknisten parametrien perusteella. Fyysisten olosuhteiden (ionosfäärin tila, sateet, kanavoituminen) ja tietoturvaperäisten uhkien (kuten spoofing, DRFM, jamming, ohjelmistohyökkäykset) välinen vuorovaikutus muodostaa dynaamisen kokonaisuuden, mikä tekee perinteisistä ECCM-ratkaisuista vain osittain riittäviä. (Adamy 2015, 85–110; Skolnik 2008, 1180–1195; Poisel 2013, 25–36.)

Työn simulaatiokokeet (A-C) vahvistivat tämän havainnon käytännössä. Järjestelmän suorituskyky romahti, kun se altistettiin useille häiriötyypeille ja se tukeutui yksittäiseen havaintokanavaan. Vasta kun järjestelmään lisättiin adaptiivinen signaalinkäsittely, tekoälypohjainen analyysi ja monilähdefuusio, havaintotarkkuus palautui. Tämä osoittaa, että tulevaisuuden tutkajärjestelmien on perustuttava reaaliaikaiseen päätöksentekoon, jossa tutka analysoi ympäristöään sekä valitsee optimaaliset toimintaparametrit automaattisesti. (Gurbuz ym. 2019, 4–7; Reddy & Sinha 2025, 48–52.)

Tulosten perusteella voidaan todeta, että häiriönsietokyky ei ole yksittäinen tekninen ominaisuus, vaan kokonaisarkkitehtuurin laatuun ja tiedonhallintaan liittyvä ominaisuus. Tutkajärjestelmän resilienssi syntyy fyysisen, digitaalisen ja kognitiivisen tason yhteistoiminnasta, mikä merkitsee tutkateknologian kehityksessä perustavanlaatuista muutosta perinteisestä havainnoinnista kohti adaptiivista ja oppivaa järjestelmää. (Gurbuz ym. 2019, 1–3; Stouffer ym. 2023, 45–47.) Seuraavissa alaluvuissa nämä johtopäätökset puretaan yksityiskohtaisemmin vastaamalla asetettuihin tutkimuskysymyksiin, arvioimalla työn luotettavuutta ja esittämällä suosituksia jatkotutkimukselle.

On kuitenkin tunnistettava, että simulaatiot eivät täysin vastaa operatiivisia olosuhteita. Todellisessa ympäristössä signaalin sironta sekä ionosfäärin vaihtelu voivat tuottaa ennakoimattomia virheitä. Tämä korostaa, että simulaatiot soveltuvat ennen kaikkea ilmiöiden periaatteellisen vaikutuksen arviointiin, ei absoluuttisten suoritusarvojen määrittämiseen.

6.1 Johtopäätökset ja vastaus tutkimuskysymyksiin

Tutkimuskysymys 1: Miten keskeisimmät radioaaltojen etenemiseen vaikuttavat fysikaaliset ilmiöt heikentävät tutkan suorituskykyä merivalvonnassa?

Tulosten perusteella voidaan todeta, että radioaaltojen etenemiseen vaikuttavat fysikaaliset ilmiöt, kuten sateen aiheuttama vaimennus, troposfäärinen kanavoituminen ja ionosfäärin vaihtelut, muodostavat tutkajärjestelmälle jatkuvan ja moniulotteisen haasteen. LOS-tutkien (Line-of-Sight) kohdalla merkittävimmät häiriölähteet liittyvät ilmakehän alempiin kerroksiin, jossa kosteuden lämpötilan ja paineen muutokset voivat aiheuttaa vaimennusta, monitie-etenemistä sekä anomaalista kanavoitumista. (Skolnik 2008, 995–999; Richards ym. 2010, 171–172.)

Kaukovalvontatutkissa (OTHR) kriittinen tekijä on ionosfäärin tila, joka säteilee HF-aaltojen heijastumista ja kantamaa. Auringon aktiivisuuden vaihtelut, geomagneettiset myrskyt ja sporadiset E-kerrokset voivat muuttaa heijastusominaisuuksia nopeasti, mikä johtaa kantaman heilahteluihin, katvealueiden siirtymiseen ja harhamaalien syntymiseen (Goodman 2010, 103–116; Hunsucker & Hargreaves 2003, 68–72). Tulokset osoittavat, että nämä fysikaaliset tekijät eivät toimi toisistaan riippumatta, vaan voivat muodostaa kerrannaisvaikutuksia, joissa esimerkiksi sadevaimennus ja troposfäärinen kanavoituminen yhdessä vääristävät kohteen etäisyyttä ja amplitudia.

Tutkimuskysymys 2: Millä tavoin nykyaikaisiin tutkajärjestelmiin kohdistuvat kyberturvallisuusuhat vaarantavat järjestelmien luotettavuuden ja tuottaman tilannekuvan eheyden?

Tutkimuksessa havaittiin, että tutkajärjestelmien digitalisoituminen ja verkostoituminen ovat laajentaneet uhkaympäristöä perinteisestä sähkömagneettisesta spektristä kohti ohjelmisto- ja tietoverkkotason uhkia. Kohinahäirintä ja harhauttava häirintä (DRFM-jamming) heikentävät signaalin havaittavuutta ja voivat tuottaa keinotekoisia maaleja, jotka hämärtävät tutkan todellista tilannekuvaa (Adamy 2015, 60–90; Poisel 2013, 43–44). Samanaikaisesti järjestelmätason hyökkäykset, kuten GNSS- ja AIS-spoofing, voivat manipuloida tutkadatan rinnalla hyödynnettyjen ulkoisten datalähteiden tietoja ja siten vääristää sensorifuusion lopputulosta (Psiaki & Humphreys 2016, 7–9).

Työ osoittaa, että kyberuhkien ja fysikaalisten häiriöiden välinen rajapinta on käytännössä hämärtynyt, esimerkiksi DRFM-häirintä voi naamioitua luonnolliseksi kohinaksi, mikä tekee havaintojen validoinnista haastavaa.

Työn kokeellinen osa (erityisesti koe C) osoitti, että sensorifuusion ja GNSS/AIS-tiedon väärentäminen voi aiheuttaa tilanteen, jossa järjestelmä pitää harhamaaleja todellisina ja todellisia maaleja harhana. Tämä korostaa, että tutkajärjestelmien luotettavuus ei enää määräydy vain fyysisen havaintokyvyn perusteella, vaan sen on sisällettävä myös kyky arvioida vastaanottamansa datan eheyttä sekä uskottavuutta. (Resiliency in PNT: GNSS Jamming and Spoofing 2025; Countering GNSS Jamming and Spoofing 2025.)

Tutkimuskysymys 3: Millä teknisillä ja operatiivisilla menetelmillä sekä luonnollisten että tahallisten häiriöiden vaikutuksia voidaan torjua tai lieventää?

Tutkimuksessa esitetyt simulaatiot ja analyysit (Koe B ja C) osoittivat, että tehokkain suojaus ei perustu yhteen menetelmään, vaan adaptiiviseen ja hierarkkiseen kokonaisuuteen, joka yhdistää ECCM-tekniikat, monilähdefuusion sekä järjestelmätason tietoturvan. Häirinnän torjunnassa keskeisiä menetelmiä ovat taajuushyppytekniikat, kapeakaistainen vastaanotto sekä spektripohjainen kohinasuodatus, jotka parantavat signaali-kohinasuhdetta kohinahäirinnän aikana. (Skolnik 2008, 1185–1190.)

Järjestelmätasolla tärkeimpiä keinoja ovat signaalin autentikointi, GNSS/AIS-datan ristiinvalidointi sekä adaptiivinen sensorifuusio, joka tunnistaa epäloogiset liikeradat ja poikkeavat mittausarvot. Nämä tulokset tukevat kokonaisvaltaista mallia, jossa tutkajärjestelmän häiriönsieto rakentuu kolmen tason varaan: havainto-, datafuusio- ja päätöksentekotasolle. (Adamy 2015, 230–232; Stouffer ym. 2023, 45–47.)

Erityisen merkittävänä havaintona on, että kognitiivinen tutka edustaa tutkateknologian kehityksessä perustavanlaatuista muutosta, jossa siirrytään perinteisestä havainnoinnista kohti adaptiivista ja oppivaa järjestelmää (Gurbuz ym. 2019, 1–12). Se kykenee paitsi havaitsemaan häiriöitä myös oppimaan niiden piirteet ja ennakoimaan niiden vaikutusta reaaliajassa. Tämä kehityssuunta muuttaa koko tutkajärjestelmien suojausajattelua reaktiivisesta puolustuksesta kohti ennakoivaa

ja itseoppivaa toimintaa. Tämä lähestymistapa yhdistää tekoälyn, datatieteen ja sähkömagneettisen fysiikan näkökulmat yhdeksi operatiiviseksi kokonaisuudeksi ja se on työn keskeisin tieteellinen kontribuutio.

Tutkimus vahvisti tutkajärjestelmien toimintaympäristön olevan entistä moniulotteisempi yhdistelmä luonnonilmiöitä ja kyberuhkia. Häiriönsieto ei ole enää yksittäinen tekninen ominaisuus, vaan järjestelmätason kyvykkyys, joka rakentuu reaaliaikaisen päätöksenteon, tekoälyn ja datan eheyden varaan. Tulevaisuuden merivalvontatutka ei ole vain sensori, vaan oppiva ja adaptiivinen järjestelmä, joka kykenee tunnistamaan, erottamaan ja hallitsemaan samanaikaisia fysikaalisia ja tietoturvallisia häiriöitä ja siten säilyttämään toimintakykynsä myös haastavimmissa olosuhteissa.

6.2 Työn luotettavuuden ja eettisyyden arviointi

Tutkimus yhdisti teoreettisen analyysin, kirjallisuuskatsauksen ja simulaatiot, jotka toteutettiin todenmukaisilla parametreilla sekä validoitiin lähdeaineiston avulla. Tulokset tukivat kirjallisuutta sekä laadullisesti että määrällisesti. Luotettavuutta rajoittaa kuitenkin simulaatioiden idealisointi: todellisissa olosuhteissa signaaliin vaikuttavat satunnaiset tekijät, kuten dynaamiset säämuutokset, antennin reaalimaailman keilat ja järjestelmäviiveet. Tästä huolimatta työn tulokset antavat realistisen kuvan eri häiriötyyppien suhteellisista vaikutuksista sekä auttavat hahmottamaan, millaisia kehitystoimia tulevaisuuden tutkajärjestelmät vaativat.

Tutkimuksessa ei käytetty luokiteltua aineistoa, eikä sen menetelmillä aiheutettu todellisia häiriöitä siviilitaajuuksille. Koeasetelmat toteutettiin simulaatioympäristössä, mikä tekee tutkimuksesta eettisesti kestävän ja turvallisen. Eettisesti merkittävää on myös läpinäkyvyys: kaikki lähteet on merkitty asianmukaisesti ja tutkimuksessa on vältetty liiallista tulosten yleistämistä. Jatkossa, mikäli menetelmiä sovelletaan kenttäolosuhteissa, on varmistettava viranomaislupa ja häiriöttömyys muille järjestelmille. Kognitiivisten järjestelmien päätöksenteossa eettinen valvonta ja mallien läpinäkyvyys ovat välttämättömiä, jotta automaattinen toiminta ei johda virheellisiin uhka-arvioihin. Lisäksi työn läpinäkyvyys, lähdeviitteiden tarkkuus ja menetelmien toistettavuus tukevat sen tieteellistä luotettavuutta.

6.3 Jatkotutkimusaiheet

Tämän työn perusteella jatkotutkimuksen kannalta keskeisintä on yhdistää luonnolliset ympäristöilmiöt ja tahallinen analyysihäirintä samaan analyysikehykseen. Erityisen kiinnostavaa olisi tutkia, miten esimerkiksi geomagneettinen myrsky tai voimakas sadevaimennus vaikuttavat tutkasignaalin käyttäytymiseen tilanteessa, jossa järjestelmää häiritään samanaikaisesti tarkoituksellisesti.

Tällaiset yhdistelmätilanteet voivat aiheuttaa monimutkaisia virhelähteitä, joissa tutka havaitsee yhtä aikaa sekä fysikaalisesti vääristyneen että tietoturvallisesti manipuloidun signaalin. Tämä on kriittinen tutkimussuunta, sillä nykyiset ECCM-menetelmät on kehitetty pääosin yksittäisiä häiriöitä vastaan.

Mallintamalla nämä tilanteet yhdessä olisi mahdollista arvioida tutkajärjestelmien todellista häiriönsietokykyä ja kehittää adaptiivisia ECCM-algoritmeja, jotka erottavat luonnollisen kohinan ja vihamielisen toiminnan vaikutukset tosistaan. Tämä edellyttää fysikaalisten propagaatioilmiöiden (ionosfäärimallit, sadevaimennus) ja signaalinkäsittelyn yhdistämistä samaan laskennalliseen simulaatioon, mikä tarjoaisi poikkeuksellisen realistisen kuvan tutkien operatiivisesta toimintaympäristöstä.

Lisäksi jatkokehityksen kannalta merkittäviä teemoja ovat:

- Selitettävä tekoäly ja autonominen päätöksenteko: miten kognitiivinen tutka voidaan auditoida ja valvoa luotettavasti?
- Inhimillinen ja tekninen yhteistoiminta: miten ihmisen päätöksenteko ja autonomiset järjestelmät integroidaan siten, ettei vastuu ja valvonta katoa?
- Operatiivinen validointi: kenttäkokeet, joissa tutkitaan signaalin ja verkon suojausmenetelmien käytännön tehokkuutta hallituissa olosuhteissa.

Tämä tutkimus vahvistaa, että tutkajärjestelmien luotettavuus ei ole vain tekninen kysymys, vaan systeeminen ja monitieteinen haaste. Tutkan on samanaikaisesti ymmärrettävä ympäristöään, tunnistettava uhkia ja mukautettava toimintaansa. Tulevaisuuden ratkaisut, kuten kognitiivinen tutka, adaptiivinen ECCM ja monilähdefuusio, eivät pelkästään lisää järjestelmien tehokkuutta, vaan myös niiden resilienssiä ja päätöksenteon luotettavuutta.

Työ tarjoaa näin sekä teoreettisen perustan että käytännön suuntaviivat tutkateknologian seuraavaan kehitysvaiheen ymmärtämiseen ja tukee turvallisen, luotettavan ja autonomisesti sopeutuvan merivalvonnan rakentamista. Laajemmin tarkasteltuna tämä tutkimus avaa pohjan monitieteiselle jatkotyölle, jossa yhdistyvät fysiikka, tietotekniikka, tekoäly ja turvallisuustutkimus. Tällainen kokonaisvaltainen lähestymistapa on välttämätön, jotta tulevaisuuden merivalvontajärjestelmät voivat toimia luotettavasti yhä kompleksisemmassa uhkaympäristössä.

Lähteet

Adamy, D. L. 2015. EW 104: Electronic Warfare Against a New Generation of Threats. Boston: Artech House.

Avaruussää. 2024. Artikkeli Ilmatieteen laitoksen verkkosivuilla. Viitattu 5.9.2025. http://ilmatieteenlaitos.fi/avaruussaa

Countering GNSS Jamming and Spoofing for Aerospace and Defense Applications. Artikkeli Taoglas-verkkosivustolla. Viitattu 30.9.2025. https://www.taoglas.com/blogs/countering-gnss-jamming-and-spoofing-for-aerospace-and-defense-applications/

Creswell, J. W. 2014. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. 4th ed. Thousand Oaks: Sage Publications.

Davies, K. 1990. Ionospheric Radio. Lontoo: Peter Peregrinus Ltd.

Electronic Warfare and Radar Systems Engineering Handbook: RF Atmospheric Absorption / Ducting. 2025. Artikkeli RF Cafe -verkkosivustolla. Viitattu 5.9.2025. https://www.rfcafe.com/references/electrical/ew-radar-handbook/rf-atmospheric-absorption-ducting.html

Goodman, J. M. 2010. Space Weather & Telecommunications. New York: Springer Science + Business Media Inc.

Gurbuz, Z. S., Griffiths, H. D., Charlish, A., Rangaswamy, M., Greco, M. S. & Bell, K. 2019. An Overview of Cognitive Radar: Past, Present and Future. Sensors 19(23), artikkeli 5122, 1–13. Viitattu 2.11.2025. https://www.metsci.com/wp-content/uploads/2021/05/Overview-Cognitive-Radar-Past-Present-Future-Gurbuz-et-al-2019.pdf

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2015. Tutki ja kirjoita. 20. p. Helsinki: Tammi.

Howard, W. W., Shebert, S. R., Martone, A. F. & Buehrer, R. M. 2023. Mode Selection in Cognitive Radar Networks. Viitattu 30.10.2025. https://arxiv.org/pdf/2312.09428

Hunsucker, R. D. & Hargreaves, J. K. 2003. The High-Latitude Ionosphere and its Effects on Radio Propagation. Cambridge: Cambridge University Press.

Impacts: Radio Communications. 2024. Artikkeli Space Weather Prediction Center (NOAA) -verkkosivuilla. Viitattu 4.9.2025. https://www.swpc.noaa.gov/impacts/radio-communications

Ionosfääri-koulutus. 2015. Puolustusvoimat. Julkaisematon PowerPoint-esitys.

Ionosphere and magnetosphere. 2024. Artikkeli Encyclopaedia Britannica -verkkosivustolla. Viitattu 5.9.2025. https://www.britannica.com/science/ionosphere-and-magnetosphere

Kingsley, S. & Quegan, S. 1999. Understanding Radar Systems. Raleigh: SciTech Publishing.

National Institute of Standards and Technology. (2023). NIST Special Publication 800-82 Revision 3: Guide to Operational Technology (OT) Security. Gaithersburg, MD: NIST. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

Pitkänen, M. 2012. Alailmakehän heijastukset tutkataajuuksilla. Ylöjärvi: Puolustusvoimien Teknillinen Tutkimuslaitos.

Poisel, R. A. 2013. Electronic Protection (EP) within the EW System. Boston: Artech House.

Psiaki, M. L. & Humphreys, T. E. 2016. GNSS Spoofing and Detection. Proceedings of the IEEE 104(6), 1258–1270.

Radioaallon eteneminen HF-alueella. 2020. Rajavartiolaitos. Julkaisematon PowerPoint-esitys.

Reddy, A. & Sinha, R. 2025. State-of-the-Art Review: Electronic Warfare Against Radar Systems. IEEE Access. Viitattu 30.10.2025. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10943203

Reinisch, B. W. & Galkin, I. A. 2011. Global Ionospheric Radio Observatory (GIRO). Earth, Planets and Space, 63, 377–381.

Resiliency in PNT: GNSS Jamming and Spoofing. Artikkeli Safran Navigation & Timing -verkkosivustolla. Viitattu 30.9.2025. https://safran-navigation-timing.com/resiliency-in-pnt-gps-gnss-jamming-and-spoofing/

Richards, M. A., Scheer, J. A. & Holm, W. A. (toim.). 2010. Principles of Modern Radar: Basic Principles. Raleigh: SciTech Publishing.

Schleher, C. D. 1999. Electronic Warfare in the Information Age. Boston: Artech House.

Skolnik, M. I. (toim.). 2008. Radar Handbook. 3. painos. New York: McGraw-Hill.

Sodankylän geofysiikan observatorio (SGO). 2024. Data. Viitattu 22.7.2025. http://www.sgo.fi/Data/Ionosonde/latestIonosonde.php.

Solar Cycle Progression. 2025. Artikkeli Space Weather Prediction Center (NOAA) -verkkosivuilla. Viitattu 4.9.2025. https://www.swpc.noaa.gov/products/solar-cycle-progression

Space Weather. 2024. Artikkeli IPS Radio and Space Services -verkkosivustolla. Viitattu 22.7.2025. http://www.ips.gov.au/Space_Weather

Tropospheric Propagation of VHF and UHF radio signals. 2024. Artikkeli VK3FS-verkkosivustolla. Viitattu 5.9.2025. https://3fs.net.au/tropospheric-propagation/

Liitteet

Liite 1. Simulaatiokoodit (Python)

Tässä liitteessä esitetään tiivis kuvaus käytetystä simulaatioympäristöstä ja keskeisistä Python-koodiosuuksista, joita hyödynnettiin kokeissa A–C tutkajärjestelmien suorituskyvyn ja häiriönsietokyvyn analysoimiseksi. Simulaatiot toteutettiin Python 3.10 -ympäristössä käyttäen kirjastoja NumPy, SciPy, Matplotlib ja Pandas, jotka mahdollistivat erilaisten häiriötyyppien (kohinahäirintä, DRFM-harhautus, GNSS/AIS-spoofing) mallintamisen signaalitasolla.

Kokonaisarkkitehtuuri mallinsi tutkajärjestelmän periaatemallia, jossa lähetys-, vastaanotto- ja häirintäprosessit voitiin määrittää ja parametrisoida erikseen. Koodit on jäsennelty kokeiden A–C mukaisesti niiden tutkimustarkoituksen ja keskeisen toiminnallisuuden perusteella.

Ensimmäisessä simulaatiossa (Koe A) tutkittiin DRFM-harhamaalien vaikutusta tutkajärjestelmään tilanteessa, jossa ECCM-toimintoja ei ollut käytössä. Koodissa mallinnettiin signaalin muodostus, kohteen ja harhamaalien lisääminen sekä sovitussuodatus, jotta voitiin arvioida järjestelmän herkkyyttä taajuus- ja aikadomainin häiriöille.

Toinen simulaatio (Koe B) mallinsi adaptiivisia ECCM-menetelmiä, kuten taajuushyppyä, spektripohjaista suodatusta ja signaalin rekonstruointia. Näiden avulla tutkittiin, kuinka tehokkaasti järjestelmä pystyi palauttamaan havaintotarkkuuden kohinahäiriön aikana sekä kuinka adaptiivinen signaalinkäsittely paransi kohteen havaitsemista.

Kolmannessa simulaatiossa (Koe C) keskityttiin GNSS- ja AIS-signaalien manipulaation vaikutuksiin sensorifuusiossa. Tässä mallinnettiin datan väärentämistä, fuusioalgoritmia ja poikkeamien tunnistusta, joiden avulla arvioitiin järjestelmän kykyä havaita ja käsitellä manipuloitua tietoa reaaliaikaisesti.

Käyttöympäristö:

- Ohjelmointikieli: Python 3.10
- Kirjastot: NumPy, SciPy, Matplotlib, Pandas

- Suoritusympäristö: PyCharm IDE
- Ajoaika: keskimäärin 5–15 sekuntia per simulaatio
- Lähtödata: synteettinen signaalidata (ei luokiteltua tietoa)

Kokeiden kuvaus ja koodikatkelmat

A. Häiriösimulaatio ilman ECCM (Koe A)

Kokeessa A tutkittiin, miten Digital RF Memory (DRFM) -tekniikalla toteutettu harhautus vaikutti tutkajärjestelmän havaintokykyyn, kun järjestelmässä ei ole käytössä ECCM-toimintoja. Tavoitteena oli mallintaa ja analysoida, miten DRFM voi tuottaa keinotekoisia kohteita (false targets) todellisen maalin ympärille ja siten vaikeuttaa havaitsemista ja seurantaa.

Simulaatiossa luotiin LFM-pulssi (Linear Frequency Modulated) ja mallinnettiin sen vastaanotto tilanteessa, jossa todellisen kohteen lisäksi ilmestyi kaksi DRFM-harhamaalia eri etäisyyksillä ja vaimennustasoilla. Tutkasignaali suodatettiin sovitussuodattimella, jonka avulla muodostettiin etäisyysprofiili ja tunnistettiin havaintohuiput.

Tulosten perusteella havaittiin, että DRFM-hyökkäys voi luoda useita uskottavia heijastuksia, joiden voimakkuus ja sijainti vaihtelevat ohjelmallisesti. Tämä vaikeuttaa todellisen maalin erottamista ja heikentää järjestelmän päätöksenteon luotettavuutta. Kokeen tulokset osoittivat, että ilman ECCM-toimintoja tutkajärjestelmä reagoi DRFM-signaaliin kuin se olisi useita todellisia kohteita.

Kokeen analyysi ja tulokset on esitetty opinnäytetyön luvussa 5.

```
# --- DRFM Simulation: parameters ---
c = 3e8
fc = 9.5e9
B = 20e6
Tp = 50e-6
fs = 80e6
R_true = 30e3
drfm_delays_m = [1500.0, 5000.0]
drfm_scales = [0.6, 0.35]

# --- Generate LFM pulse and add DRFM echoes ---
k = B / Tp
t = np.arange(0, Tp, 1/fs)
s = np.exp(1j * np.pi * k * t**2)

rx = np.zeros(int(len(t) * 8), dtype=complex)
rx = add_echo(rx, R_true, 1.0)
for dR, sc in zip(drfm_delays_m, drfm_scales):
    rx = add_echo(rx, R_true + dR, sc)

# --- Matched filter and result plot ---
mf = np.convolve(rx, np.conj(s[::-1]), mode='same')
rng_axis = (np.arange(len(mf)) - len(s)//2) * (c / (2 * fs))
plt.plot(rng_axis, 20*np.log10(np.abs(mf)))
plt.title("DRFM deception: true target and false targets")
plt.xlabel("Range (m)")
plt.ylabel("Magnitude (dB)")
plt.grid(True)
plt.show()
```

Yllä oleva koodikatkelma havainnollistaa kokeen keskeisen vaiheen, jossa DRFM-harhamaalit lisättiin tutkasignaaliin ja analysoitiin sovitussuodattimen avulla.

Tulosten perusteella todettiin, että DRFM voi aiheuttaa monihuippuisen vasteen, jossa todellisen ja keinotekoisten kohteiden erottaminen vaatii adaptiivisia ECCM-menetelmiä.

B. Adaptiivinen ECCM ja kohinahäirinnän torjunta (Koe B)

Kokeessa B mallinnettiin tutkajärjestelmän toimintaa laajakaistaisen kohinahäirinnän (broadband jamming) aikana sekä arvioitiin, kuinka tehokkaasti adaptiiviset ECCM-menetelmät pystyivät palauttamaan järjestelmän havaintokyvyn.

Simulaatiossa tutkittiin kahta osa-aluetta:
1. SNR:n käyttäytymistä eri J/S-tasoilla (jammer-to-signal) ja tutkan “burn-through rangea”
2. Adaptiivisen suodatuksen vaikutusta häirintäpiikkien poistamisessa taajuus- ja aikatasossa

Ensimmäisessä osassa (B1) mallinnettiin kohteen ja häirinnän välistä etäisyysriippuvuutta. Tuloksena havaittiin, että kun J/S-suhde kasvoi, tutkan signaalipeitto lyheni ja havaintotodennäköisyys heikkeni, kunnes adaptiivinen ECCM palautti SNR-arvon kynnystasolle. Toisessa osassa (B2) käytettiin notch-suodatukseen perustuvaa adaptiivista ECCM-ratkaisua, jolla häirintäpiikki poistettiin signaalista reaaliaikaisesti ilman merkittävää signaalin vaimennusta.

Koodissa määritettiin tutkaparametrit, lisättiin kohinahäirintä ja toteutettiin adaptiivinen suodatus, joka havainnollisti, kuinka ECCM paransi tutkan suorituskykyä häiriön aikana. Kokeen tulokset on esitetty ja analysoitu opinnäytetyön luvussa 5.

```
# --- Adaptive ECCM (Notch Filter) ---
def notch_filter(x, fs, f0, Q=30):
    low = (f0 - (fs/(2*Q))) / (fs/2)
    high = (f0 + (fs/(2*Q))) / (fs/2)
    b, a = butter(2, [low, high], btype='bandstop')
    return filtfilt(b, a, x)

rx_ECCM = notch_filter(rx_noECCM, fs, jam_freq)


# --- Spectrum (Before vs After) ---
plt.figure(figsize=(9, 5))
plt.semilogy(f_noECCM/1e6, np.mean(Sxx_noECCM, axis=1), label="Ilman ECCM")
plt.semilogy(f_ECCM/1e6, np.mean(Sxx_ECCM, axis=1), label="ECCM-suodatettu")
plt.xlabel("Taajuus [MHz]")
plt.ylabel("Spektritiheys (a.u.)")
plt.title("ECCM-suodatuksen vaikutus: häirintäpiikki vaimenee")
plt.legend()
plt.grid(True, linestyle="--", alpha=0.6)
plt.tight_layout()
plt.savefig(FIG / "adaptive_eccm_spectrum.png", dpi=300)
```

Yllä oleva koodikatkelma havainnollistaa adaptiivisen notch-suodattimen toimintaa, jolla poistettiin kapeakaistainen kohinahäirintä tutkan vastaanotetusta signaalista. Simulaatiossa suodatuksen jälkeen spektrissä näkyvä häirintäpiikki vaimeni merkittävästi ja vastaanotetun signaalin dynamiikka palautui lähes alkuperäiselle tasolle.

Menetelmä osoitti, että adaptiivinen ECCM parantaa signaali–kohinasuhdetta (SNR) erityisesti tilanteissa, joissa häirintä kohdistuu kapeaan taajuuskaistaan.

C. Sensorifuusio ja GNSS/AIS-spoofingin vaikutus (Koe C)

Kokeessa C tutkittiin tutkajärjestelmän sensorifuusion luotettavuutta tilanteessa, jossa GNSS- ja AIS-dataa manipuloitiin tahallisesti (spoofing). Tavoitteena oli arvioida, miten järjestelmä pystyi havaitsemaan ja hylkäämään poikkeavia havaintoja sekä säilyttämään tilannekuvan eheyden.

Simulaatiossa mallinnettiin kolmen sensorin (tutka, GNSS ja AIS) tuottamat paikkahavainnot synteettisessä merivalvontaskenaariossa. GNSS-signaaliin lisättiin ajallisesti kasvava paikka- ja nopeusvirhe, ja AIS-data tehtiin seuraamaan osittain spoofattua GNSS-virhettä. Näin luotiin realistinen tilanne, jossa osa sensoreista välittää virheellistä tai väärennettyä tietoa.

Tuloksia analysoitiin vertaamalla naiivia fuusiomenetelmää (painotettu keskiarvo) ja robustia Kalman-suodatukseen perustuvaa menetelmää, joka käytti mahalanobis-etäisyyteen perustuvaa gating-päätöstä mittausten hyväksymiseksi tai hylkäämiseksi. Havaittiin, että spoofing-vaiheessa naiivi fuusio seurasi väärää kohdetta, kun taas robusti algoritmi hylkäsi poikkeavat mittaukset ja säilytti seurannan todellisessa kohteessa.

Koodissa toteutettiin sekä mittausdatan generointi että fuusioalgoritmin hyväksyntälogiikka, ja tulokset visualisoitiin kahdessa kuvassa: kohteiden rataero ja hyväksyttyjen mittausten aikajakauma.

Kokeen analyysi ja tulokset on esitetty luvussa 5.

```python
# --- Robust Fusion: Kalman Filter + Gating ---
def kf_predict(x,P):
    x_ = F @ x
    P_ = F @ P @ F.T + Q
    return x_, P_

def kf_update(x,P,z,R):
    S = H @ P @ H.T + R
    K = P @ H.T @ np.linalg.inv(S)
    y = z - H @ x
    x_new = x + K @ y
    P_new = (np.eye(4) - K @ H) @ P
    return x_new, P_new, y, S

def maha(y,S):
    return float(y.T @ np.linalg.inv(S) @ y)

gate = 7.8  # chi2(2) ~ 5.99; tighter gating threshold

for k in range(N):
    x_est, P_est = kf_predict(x_est, P_est)

    for src, Z, R in [("radar", Z_radar, R_radar),
                      ("gnss", Z_gnss, R_gnss),
                      ("ais", Z_ais, R_ais)]:
        z = Z[k,:]
        S = H @ P_est @ H.T + R
        y = z - (H @ x_est)
        d2 = maha(y,S)

        if d2 <= gate:
            x_est, P_est, _, _ = kf_update(x_est, P_est, z, R)
            accepted[src].append(k)
        else:
            rejected[src].append(k)
    track_robust[k,:] = x_est
```

Yllä oleva koodikatkelma havainnollistaa robustin sensorifuusion päätöksentekoa, jossa jokainen mittaus validoitiin tilastollisen portin (gating) avulla.

Mikäli mittaus poikkesi odotusarvosta liikaa, se hylättiin eikä vaikuttanut tilannekuvaan. Menetelmä osoitti, että Kalman-suodatukseen perustuva gating mahdollistaa järjestelmän toiminnan jatkumisen luotettavasti myös spoofing-hyökkäysten aikana, kun taas naiivi fuusio johti virheelliseen kohteen sijaintiin.