**Tuomas Aaltonen**

# Satelliittipaikannusjärjestelmien haavoittuvuudet

Tietotekniikan kandidaatintutkielma

30. huhtikuuta 2023

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

**Tekijä:** Tuomas Aaltonen

**Yhteystiedot:** thaaltos@student.jyu.fi

**Ohjaaja:** Timo Tiihonen

**Työn nimi:** Satelliittipaikannusjärjestelmien haavoittuvuudet

**Title in English:** Vulnerabilities in satellite navigation systems

**Työ:** Kandidaatintutkielma

**Opintosuunta:** Tietotekniikka

**Sivumäärä:** 21+0

**Tiivistelmä:** Maailmanlaajuiset satelliittipaikannusjärjestelmät, eli GNSS-järjestelmät ovat nyky-yhteiskunnassa tärkeässä asemassa. Tutkielman keskeisenä tavoitteena on perehtyä näissä järjestelmissä tunnistettuihin haavoittuvuuksiin, niihin liittyviin riskeihin ja uhkiin eri yhteiskunnan sektoreiden näkökulmasta sekä koota yhteen keskeisiä esitettyjä suojautumismenetelmiä. Tutkimuksessa esiin nousseiden tulosten perusteella signaalihäirintää voi pitää vakavana uhkana GNSS-järjestelmien toimintaan nojaaville toiminnoille, ja häiriötilanteisiin varautumiseen sekä varajärjestelmien integrointiin tulisikin kiinnittää huomiota.

**Avainsanat:** Satelliittipaikannusjärjestelmät, signaalihäirintä, väärennys, tukkiminen

**Abstract:** Global Navigation Satellite Systems (GNSS) are an important part of today's society. The main objective of this thesis is to examine identified vulnerabilities that these systems have, the risks and threats associated with these vulnerabilities from the viewpoint of different societal sectors, and to compile the main proposed defensive mechanisms against the identified threats. Based on the results of this study, signal interference can be seen as a serious threat to functions that rely on GNSS, and attention should be paid to preparing for disruptions and integrating backup systems.

**Keywords:** GNSS, signal interference, spoofing, jamming

# Kuviot

Kuvio 1. GPS-järjestelmän ohjaussegmentin osat ja niiden tehtävät. (Muokattu Kaplan ja Hegarty (2017, s. 118) pohjalta) ..... 3
Kuvio 2. GNSS-vastaanottimen toiminta. (Muokattu Kaplan ja Hegarty (2017, s. 139) pohjalta) ..... 4
Kuvio 3. AoA-suojaus. (Muokattu Schmidt ym. (2016) pohjalta) ..... 12

# Sisällys

1 JOHDANTO ..... 1

2 SATELLIITTIPAIKANNUSJÄRJESTELMÄT ..... 2
2.1 Maasegmentti ..... 2
2.2 Avaruussegmentti ..... 3
2.3 Vastaanotin ..... 4

3 RISKIT JA UHAT ..... 6
3.1 Vaikutukset kriittiseen infrastruktuuriin ..... 6
3.2 Taloudelliset vaikutukset ..... 7
3.3 Turvallisuus ja kansallinen puolustus ..... 8

4 SATELLIITTIPAIKANNUSJÄRJESTELMIEN HAAVOITTUVUUDET ..... 9
4.1 Haavoittuvuuden määrittely ..... 9
4.2 Signaalihäirintä ..... 10
4.2.1 Väärentäminen ..... 10
4.2.2 Tukkiminen ..... 11
4.3 Mitigointi ..... 11

5 YHTEENVETO ..... 14

LÄHTEET ..... 15

# 1 Johdanto

Maailmanlaajuiset satelliittipaikannusjärjestelmät (engl. *Global Navigation Satellite Systems*), eli GNSS-järjestelmät ovat keskeisessä asemassa monilla yhteiskunnan sektoreilla. GNSS-järjestelmien toiminta perustuu satelliittien lähettämiin radiosignaaleihin, joita vastaanottimet maanpinnalla käyttävät paikan ja ajan tarkkaan määrittämiseen. GNSS-järjestelmät ovat mahdollistaneet monenlaisten teknologisten toteutusten ja sovellusten kehittämisen, kuten navigaattorit, logistiikan tukitoiminnot ja erilaiset energiaverkkojen monitorointitoimet. GNSS-järjestelmät ovat kuitenkin haavoittuvia monille häiriöille, jonka takia niihin liittyy myös laaja kirjo riskejä ja uhkia, jotka voivat vaikuttaa merkittävästi yhteiskuntamme toimintaan. Nämä riskit voivat vaihdella kriittisen infrastruktuurin häiriöistä taloudellisiin vaikutuksiin ja jopa kansallisen turvallisuuden uhkiin.

Tutkielma on toteutettu kirjallisuuskatsauksena ja sen tarkoituksena on tutkia satelliittipaikannusjärjestelmiin liittyviä haavoittuvuuksia, niiden mahdollisia vaikutuksia yhteiskuntaamme ja tarkastella esitettyjä ratkaisuja näiden haavoittuvuuksien minimoimiseksi lähdekirjallisuuteen pohjautuen. Tutkielman luvussa 2 käsitellään satelliittipaikannusjärjestelmien yleisiä piirteitä ja toimintaperiaatteita, syventyen myös järjestelmien tekniseen toteutukseen. Tämä antaa lukijalle tarvittavan taustatiedon järjestelmiin, joita tutkielmassa käsitellään. Luvussa 3 käsitellään satelliittipaikannusjärjestelmiin liittyviä riskejä ja uhkia. Luvussa keskitytään tarkastelemaan uhkia erityisesti kriittisen infrastruktuurin, talouden sekä kansallisen turvallisuuden näkökulmista ja sen tavoitteena on antaa lukijalle ymmärrys satelliittipaikannusjärjestelmien merkittävyydestä ja häiriöiden potentiaalisista vaikutuksista yhteiskuntaamme. Luvussa 4 paneudutaan satelliittipaikannusjärjestelmien haavoittuvuuksiin. Ensin määritellään haavoittuvuudet, jonka jälkeen tarkastellaan kahden yleisimmän signaalihäirinnän muodon, väärentämisen sekä tukkimisen teknisiä piirteitä, jonka jälkeen tarkastellaan ehdotettuja mitigointikeinoja. Lopuksi esitetään yhteenveto luvussa 5, jossa käydään läpi tutkimuksessa esiin nousseita pääkohtia.

# 2 Satelliittipaikannusjärjestelmät

GNSS-järjestelmillä tarkoitetaan satelliittipaikannusjärjestelmiä, joita voidaan käyttää maailmanlaajuisesti ajan ja paikan mittaamiseen sekä navigointiin (Hegarty 2012). GNSS-järjestelmiä on tällä hetkellä kiertoradalla neljä: Yhdysvaltojen Global Positioning System (GPS), venäläinen Glonass, eurooppalainen Galileo ja kiinalainen BeiDou. Globaalien satelliittipaikannusjärjestelmien lisäksi on olemassa paikallisesti toimivia paikannusjärjestelmiä, kuten intialainen NavIC ja japanilainen QZSS. (Montenbruck, Steigenberger ja Hauschild 2020).

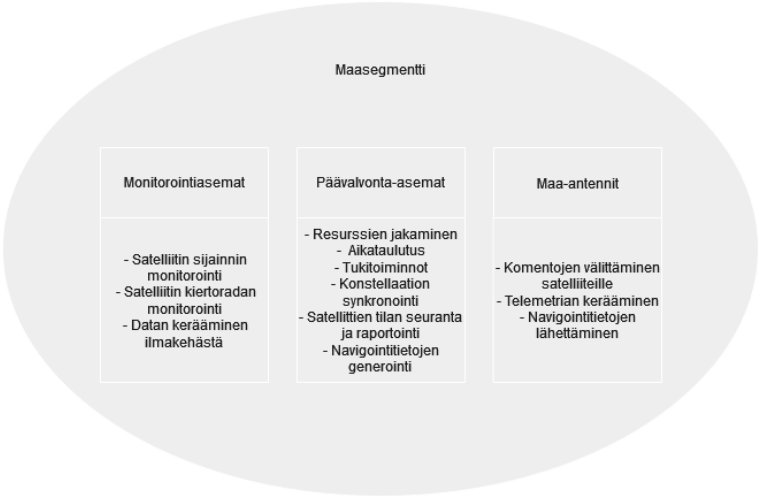
Eri satelliittipaikannusjärjestelmät eivät ole toiminnaltaan täysin identtisiä, mutta luvussa on käytetty niissä esiintyviä toimintaperiaatteiden samankaltaisuuksia kuvaamaan järjestelmiä yleisellä tasolla. Järjestelmien toiminta perustuu tyypillisesti MEO-radalla (engl. *medium Earth orbit*) kiertävään, koko maapallon kattavaan satelliittikonstellaatioon, jonka lähettämät radiosignaalit GNSS-vastaanotin, joka voi sijaita esimerkiksi puhelimessa, vastaanottaa ja tulkkaa käyttäjälle hyödylliseen muotoon. (Kaplan ja Hegarty 2017, s. 2). Satelliittipaikannusjärjestelmien voidaan yleisesti kuvata koostuvan kolmesta osasta: maasegmentistä, avaruussegmentistä ja vastaanottimesta. Seuraavissa alaluvuissa esitetään tarkemmin näiden järjestelmän osien teknisiä piirteitä sekä toimintaperiaatteita.

## 2.1 Maasegmentti

GNSS-järjestelmien maasegmentit tai ohjaussegmentit (engl. *control segment*) koostuvat maa-asemista, joita käytetään mm. satelliittien monitorointiin, seurantaan sekä komentojen tai datan lähettämiseen konstellaatiolle. Maa-asemat voivat olla esimerkiksi ohjausasemia, maa-antenneita tai monitorointiasemia. (Kaplan ja Hegarty 2017, s. 118). GPS-järjestelmän ohjaussegmenttiin kuuluvia maa-asemia ja niiden tehtäviä on visualisoitu alla (Kuvio 1). Kuviosta näemme, että GPS-järjestelmän monitorointiasemien tehtäviin kuuluu itse satelliitin sijainnin ja kiertoradan monitoroinnin lisäksi myös mm. datan kerääminen ilmakehästä. Maa-antennien tehtävät sen sijaan jakautuvat esimerkiksi komentojen välittämiseen satelliitille, telemetrian keräämiseen sekä navigointitietojen lähettämiseen. Näin ollen monitorointiasemat toimivat pelkästään datan vastaanottajina, kun taas maa-antennit voivat sekä

vastaanottaa että lähettää dataa satelliiteille.

Maa-asemien kokonaisuuteen kuuluu yleisesti myös yksi tai useampi päävalvonta-asema (engl. *Master Control Station*), joita sijaitsee mm. GPS-järjestelmällä Coloradossa Schrieverin ilmavoimien tukikohdassa ja Glonassilla Venäjän Krasnoznamenskissa. Päävalvonta-asemien toimenkuvaan kuuluvat resurssien jakamisen ja aikataulutuksen lisäksi myös erilaiset tukitoiminnot, konstellaation synkronointi, satelliittien tilan seuranta ja raportointi sekä navigointitietojen generointi. (Kaplan ja Hegarty 2017, s. 118).




Kuvio 1. GPS-järjestelmän ohjaussegmentin osat ja niiden tehtävät. (Muokattu Kaplan ja Hegarty (2017, s. 118) pohjalta)

## 2.2 Avaruussegmentti

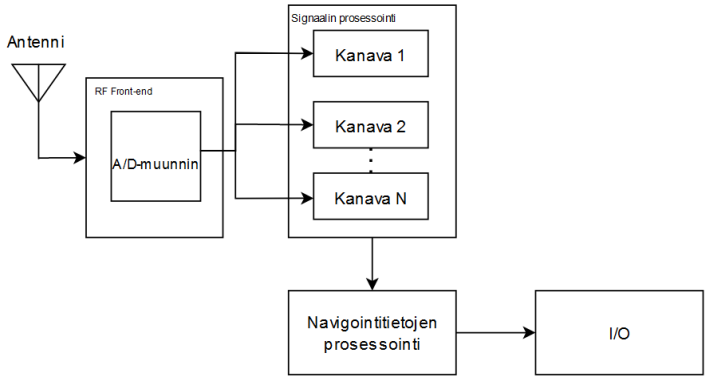
Avaruussegmentillä tarkoitetaan satelliittipaikannusjärjestelmän avaruudessa sijaitsevaa osaa, tässä tapauksessa satelliittikonstellaatiota tai yksittäistä satelliittia. GPS-järjestelmän konstellaatio koostuu 31 satelliitista, jotka kiertävät maapalloa kuudella eri kiertoratatasolla (National Coordination Office for Space-Based Positioning, Navigation, and Timing 2022). Eurooppalainen Galileo ja venäläinen GLONASS -järjestelmä koostuvat molemmat sen sijaan 24 aktiivisesta satelliitista (Kaplan ja Hegarty 2017, s. 191, 221). Avaruussegmentin tehtävä GNSS-järjestelmän kokonaisuudessa on lähettää radiosignaaleja maan pinnalle. Kaikki neljä suurinta GNSS-järjestelmää (Galileo, GPS, Glonass, BeiDou) käyttävät IEEE:n määrittelyn mukaista 1-2Ghz L-kaistan (engl. *L-band*) radiotaajuusaluetta radiosignaalien lähet-

tämiseen (Montenbruck, Steigenberger ja Hauschild 2020).

Radiosignaalit lähetetään GNSS-satelliiteista maan pinnalle käyttäen erilaisia signaalityyppejä ja -protokollia. GPS-järjestelmä käyttää kolmea erilaista signaalityyppiä, joita kutsutaan L1-, L2- ja L5-signaaleiksi. L1-signaali lähetetään 1575,42 MHz, L2-signaali 1227,60 MHz ja L5-signaali 1176,45Mhz taajuudella. (National Coordination Office for Space-Based Positioning, Navigation and Timing 2020). Satelliittipaikannusjärjestelmien avaruussegmentit sisältävät myös satelliitteihin asennetut atomikellot, joita käytetään ajan tarkkaan mittaamiseen. Avaruussegmentti vastaanottaa tämän lisäksi maa-asemilta tulevia ohjauskomentoja.

## 2.3 Vastaanotin

Komponenttien pienikokoistumisen, tuotannon tehostumisen ja kustannusten laskemisen myötä GNSS-vastaanottimia on sulautettu moniin päivittäisiin esineisiin. Näitä esineitä ovat esimerkiksi autot, puhelimet ja kamerat. Tänä päivänä valtaosa GNSS-vastaanottimista on yksittäisiä mikrosiruja integroituna miljardeihin käytössä oleviin matkapuhelimiin. (Kaplan ja Hegarty 2017, s. 137). Kirjassaan Kaplan ja Hegarty (2017) kuvaavat GNSS-vastaanottimien koostuvan viidestä pääasiallisesta komponentista: antennista, RFFE:stä (*RF Front end*), prosessorista, I/O laitteesta ja virtalähteestä. Vastaanottimen toimintaa on yksinkertaistetusti havainnollistettu lohkokaaviossa (Kuvio 2).




Kuvio 2. GNSS-vastaanottimen toiminta. (Muokattu Kaplan ja Hegarty (2017, s. 139) pohjalta)

Kuten kuviosta näemme, useimmissa vastaanottimissa on useampi kanava eri satelliittien lähettämien signaalien vastaanottamiselle. Antennin tarkoitus on vastaanottaa GNSS-signaali ja muuntaa se jännitteeksi, jonka jälkeen RFFE muuttaa antennin vastaanottamat signaalit digitalisoitavaan ja pidemmälle prosessoitavaan muotoon. Navigointitietojen prosessoinnissa vastaanotin suorittaa käyttäjän sijainnin laskemisen. (Kaplan ja Hegarty 2017, s. 341-343). Laskeakseen käyttäjän tarkan sijainnin, täytyy GNSS-vastaanottimen vastaanottaa neljä signaalia: kolme signaalia sijainnin määrittämiseen ja yksi kellovirheen (engl. *clock error*) laskemiseen. Näennäisetäisyys, josta käyttäjän sijainti on mahdollista johtaa trilateraatiomenetelmällä (engl. *trilateration*) voidaan laskea seuraavasti

$$\rho = c \cdot (t - t_0), \tag{2.1}$$

missä $\rho$ on tuntematon näennäisetäisyys, $c$ on valonnopeus, $t$ vastaanottoaika ja $t_0$ signaalin lähetysaika. (Ziedan 2006, s. 3-4).

# 3 Riskit ja uhat

Satelliittipaikannusjärjestelmät ovat nykypäivän yhteiskunnassa korvaamattomia monilla eri sektoreilla, kuten kriittisessä infrastruktuurissa, taloudessa ja kansallisessa puolustuksessa. Näillä sektoreilla hyödynnetään tarkkaa paikannustietoa ja ajan mittausta esimerkiksi logistiikassa, kuljetuksissa, sähköverkoissa, lentoliikenteessä ja pankkitoiminnassa. GNSS-järjestelmien haavoittuvuuksiin liittyy kuitenkin monia riskejä ja uhkia. Esimerkiksi kriittisessä infrastruktuurissa GNSS-järjestelmän häiriö voi aiheuttaa vakavia ongelmia sähköverkoille ja muille kriittisille toiminnoille. (Yao ym. 2017). Taloudessa GNSS-järjestelmän häiriö voi vaikuttaa negatiivisesti esimerkiksi kaupankäyntiin ja logistiikkaan, joka voi johtaa merkittäviin taloudellisiin menetyksiin. Kansallisen puolustuksen näkökulmasta GNSS-järjestelmän häiriö voi vaikuttaa vakavasti esimerkiksi valvontaan, asejärjestelmiin, johtojärjestelmiin ja viestintäverkkoihin (Westbrook 2019). Tässä luvussa tarkastelemme tarkemmin GNSS-järjestelmien riskejä ja uhkia kriittisen infrastruktuurin, talouden ja kansallisen puolustuksen näkökulmista.

## 3.1 Vaikutukset kriittiseen infrastruktuuriin

Kriittiseen infrastruktuuriin kuuluu useita toimintoja, jotka nojaavat GNSS-järjestelmiin. Näitä toimintoja ovat esimerkiksi energian siirto- ja jakelujärjestelmät sekä liikenne ja logistiikka. Esimerkiksi vuonna 2018 lentäjät raportoivat Eurocontrolille 4364 tapahtumaa, joihin liittyi GNSS-signaalin häiriöitä (Eurocontrol 2021). Tapauksien suuri lukumäärä alleviivaa siviilikäyttöisten GNSS-vastaanottimien haavoittuvuutta ja sitä, kuinka yleisestä ilmiöstä on kyse. Jokainen tapahtuma, jossa lentokone menettää GNSS-signaalin on vakava turvallisuusuhka sekä itse lentokoneelle ja sen matkustajille että muille ilmatilan käyttäjille. Esimerkkinä signaalin menetyksen vakavuudesta lentoliikenteelle on vuonna 2019 julkaistussa raportissa esitetty tilanne, jossa GPS-signaalin menetys huonossa säässä oli aiheuttaa matkustajakoneen törmäyksen korkeaan maastoon (NASA 2019).

Myös voimalaitokset ja energianjakelujärjestelmät ovat haavoittuvia GNSS-signaalien häiriöistä johtuville ongelmille. Sähkövoimajärjestelmien monitoroinnissa käytetyt SMD-laitteet

(*Synchronized Measurement Device*) hyödyntävät GNSS-signaaleita synkronoidakseen monitorointia eri mittauspisteiden välillä. Jos GNSS-signaali menetetään, SMD-laitteet voivat menettää synkronoinnin ja tämä voi vaikuttaa mittausten tarkkuuteen ja luotettavuuteen. Tämä voi johtaa virheellisiin päätöksiin, vikojen havaitsematta jäämiseen tai turvallisuusriskien syntymiseen. (Yao ym. 2017). On siis tärkeää, että sähkövoimajärjestelmien monitorointijärjestelmät on suunniteltu ottaen huomioon mahdolliset GNSS-signaalien menetykset.

## 3.2 Taloudelliset vaikutukset

Satelliittipaikannusjärjestelmät ovat merkittävässä asemassa yksityisellä sektorilla. Yhdysvaltain kauppaministeriön vuonna 2019 tilaaman tutkimuksen mukaan GPS-järjestelmä on tuottanut käyttöönotostaan lähtien noin 1.4 biljoonan Yhdysvaltain dollarin taloudellisen hyödyn yksityiselle sektorille. Raportissa käsitellään myös mahdollista GPS-järjestelmän katkosta ja sen taloudellisia vaikutuksia. GPS-järjestelmän 30 päivän mittaisen katkon vaikutukset olisivat raportin mukaan laajalti epävarmoja, mutta arviot taloudellisista menetyksistä esimerkiksi tietoliikenneyrityksille sijoittuvat 5-14 miljardin dollarin välille. (O'Connor ym. 2019). Arviot alleviivaavat yksityisen sektorin toimijoiden riippuvuutta GNSS-järjestelmien toiminnoista ja pitkäkestoinen katko voidaan nähdä selkeänä uhkana yritysten toimintaedellytyksille.

Satelliittipaikannusjärjestelmien häiriöiden vaikutusta lentoliikenteeseen on myös tutkittu laajasti. Artikkelissaan Xue, Yang ja Liu (2022) estimoivat, että Hongkongin kansainväliseen lentokenttään vaikuttavan voimakkaan geomagneettisen myrskyn johdosta taloudelliset kustannukset lentoyhtiöille voisivat olla noin 2 miljoonaa euroa lentojen peruuntumisten, lentojen uudelleenreititysten ja myöhästymisten johdosta. Matkustajiin liittyvät kustannukset voisivat nousta jopa 3 miljoonaan euroon. (Xue, Yang ja Liu 2022).

GNSS-järjestelmien toiminta on myös oleellinen osa finanssisektoria. GNSS-järjestelmien tarkkaa ajanmittausta käytetään rahoitustapahtumien käsittelyssä transaktioiden suoritusjärjestysten tarkkaan määrittämiseen. Sääntelyn näkökulmasta on myös tärkeää, että aikaleimat ovat riittävän tarkkoja. GPS-järjestelmän vaikutusta eri finanssisektorin toimijoihin tutkineet O'Connor ym. (2019) eivät kuitenkaan tutkimuksessaan nähneet merkittävien taloudellis-

ten tappioiden olevan todennäköisiä GPS-järjestelmän häiriötilanteessa, koska finanssisektorin toiminnot sisältävät varajärjestelmiä, jotka GPS-järjestelmän häiriötilanteessa pystyvät tuottamaan tarkkoja aikaleimoja vain n. 1 mikrosekunnin poikkeamalla usean päivän jälkeen. (O'Connor ym. 2019).

Huomionarvoista yllä esitellyissä havainnoissa on eri sektoreiden valmiudet kohdata GNSS-järjestelmien häiriöitä. Esimerkiksi tietoliikenneyritysten voidaan nähdä olevan hyvin taloudellisesti haavoittuvassa asemassa GNSS-järjestelmien häiriötilanteissa, kun taas muilla sektoreilla, kuten finanssisektorilla kyseisiin tapahtumiin on varauduttu implementoimalla varajärjestelmiä.

## 3.3 Turvallisuus ja kansallinen puolustus

GNSS-järjestelmät ovat tärkeitä myös monille sotilaallisille järjestelmille, kuten ilma-aluksille, ohjuksille ja ajoneuvoille. Nämä järjestelmät voivat kuitenkin olla siviilikäytössä olevien järjestelmien tapaan alttiita signaalihäirinnälle, mikä voi häiritä niiden toimintaa tai jopa estää niitä toimimasta kokonaan. Yhdysvaltain asevoimien ja sen liittolaisten käyttöön tarkoitetut GPS-signaalit, nk. M-koodin (engl. *M-code*) signaalit, jotka otettiin ensimmäisen kerran käyttöön GPS:n Block III satelliiteissa vuonna 2018 on kehitetty vastaamaan GPS-häirinnän uhkaan sotilaallisille järjestelmille hyödyntäen signaalin salausta sekä voimakkaampaa signaalin tehoa. (Rui ym. 2022).

Vaikka sotilaskäytössä olevat GNSS-järjestelmät ovatkin suojattuja, GNSS-signaalien häiriöillä voi silti olla kielteisiä vaikutuksia moniin kriittisiin sotilasjärjestelmiin. Sotilaskäyttöisten GPS-signaalien häirintää tutkinut Westbrook (2019) esittää useita tapauksia lähihistoriasta, joissa ennen M-koodin kehitystä GPS-signaalien häirintää on käytetty sotilaallisia järjestelmiä vastaan. Esimerkiksi vuonna 2011 Iranin asevoimat onnistuivat kaappaamaan yhdysvaltalaisen RQ170-Sentinel miehittämättömän ilma-aluksen väärentämällä sen vastaanottaman GPS-signaalin, mikä sai ilma-aluksen laskeutumaan Iranin rajojen sisälle. Westbrook (2019) tuleekin artikkelissaan johtopäätökseen, että sotilasjärjestelmien GNSS-signaalien häirintä voi vaikuttaa operaatioiden tehokkuuteen, suorituskykyyn sekä joukkojen moraaliin.

# 4 Satelliittipaikannusjärjestelmien haavoittuvuudet

Tieteen ja teknologian alalla on tärkeää ymmärtää ja määritellä käsitteitä oikein, jotta voidaan kehittää luotettavia ja turvallisia järjestelmiä ja ratkaisuja. Informaatioteknologian alalla käsite haavoittuvuus (engl. *vulnerability*) on yleisesti käytetty, mutta sen määrittelyssä voi esiintyä eroja riippuen siitä, missä asiayhteydessä sitä käytetään. Tässä luvussa määrittellään haavoittuvuudet kirjallisuuden pohjalta, jonka jälkeen tarkastellaan tarkemmin satelliittipaikannusjärjestelmissä ilmeneviä haavoittuvuuksia ja niihin mahdollisesti esitettyjä ratkaisuja.

## 4.1 Haavoittuvuuden määrittely

Yhdysvaltain standardisointi- ja teknologiainstituutti määrittelee haavoittuvuuden heikkoutena laitteiston tai ohjelmiston koodissa. Määritelmän mukaan haavoittuvuuden hyödyntäminen voi vaikuttaa järjestelmän luottamuksellisuuteen, eheyteen tai saatavuuteen negatiivisesti. Tämänkaltaiset haavoittuvuudet pyritään usein torjumaan koodimuutoksilla, mutta myös muiden toimenpiteiden, kuten toimintojen poistamisen avulla. (National Institute of Standards and Technology 2023). Myös Dowd, McDonald ja Schuh (2006) lähestyvät määritelmää sovellustason näkökulmasta. Kirjassaan he määrittelevät haavoittuvuudet sovelluksessa esiintyvänä heikkoutena, jonka avulla hyökkääjä voi päästä käsiksi, häiritä, tuhota tai muuttaa järjestelmää tai sen sisältämää arkaluontoista tietoa. He korostavat kuitenkin, että vaikka sovellus toimisi suunnitellusti, siinä voi silti olla haavoittuvuuksia. Tämä johtuu osittain inhimillisistä tekijöistä, jotka voivat vaikuttaa haavoittuvuuksien ilmenemiseen. (Dowd, McDonald ja Schuh 2006).

Edellisistä määritelmistä poiketen Shirey (2007) mukaan haavoittuvuus voidaan määritellä virheenä tai heikkoutena järjestelmän suunnittelussa, toteutuksessa tai ylläpidossa, joka mahdollistaa järjestelmän turvallisuuden vaarantumisen. Tämä laajempi lähestyminen määritelmään sopii monenlaisiin konteksteihin, olipa kyse sitten ohjelmistossa ilmenevistä tai ihmisten toiminnasta johtuvista haavoittuvuuksista. Tämän tutkielman käsitellessä haavoittuvuuksia useasta eri näkökulmasta ottaen myös mm. fyysisen ulottuvuuden tarkasteluun, on Shirey (2007) määritelmä mielekkäämpi ja tutkielman tarkoitukseen sopivampi.

## 4.2 Signaalihäirintä

Maan pinnalle päästyään GNSS-järjestelmien lähettämät signaalit ovat heikentyneitä, minkä vuoksi vastaanottimet ovat hyvin alttiita häirinnälle (Sharifi-Tehrani, Sabahi ja Raees Danaee 2022). Signaalihäirintä voi olla sekä tahatonta, esimerkiksi langattomien viestintälaitteiden suuren määrän vuoksi, mutta myös tarkoituksellista. On tärkeää tiedostaa, että signaalihäirintä voi tapahtua monella eri tavalla. Yleisimpiä häirintätapoja ovat väärentäminen (engl. *spoofing*) ja tukkiminen (engl. *jamming*). Väärentämisessä vastaanotin hyväksyy väärennetyn signaalin oikeaksi GNSS-signaaliksi. Tukkimisessa taas vastaanotettava signaali peitetään häiriösignaalilla, jolloin vastaanotin ei pysty vastaanottamaan aitoa GNSS-signaalia. (Ioannides, Pany ja Gibbons 2016).

GNSS-järjestelmien lähettämät signaalit voivat myös häiriintyä luonnonilmiöiden vuoksi. Kun GNSS-signaali etenee ilmakehässä, elektronien määrä ionosfäärissä vaikuttaa signaalien etenemisaikaan. Tätä ilmiötä kutsutaan skintillaatioksi. Skintillaatiota voidaan pitää siis luonnollisena häiriönä, mikä joissakin tapauksissa voi vaikuttaa GNSS-vastaanottimien toimintaan. Voimakkaiden ionosfääri-ilmiöiden aikana tämä häiriö voi aiheuttaa jopa signaalilukituksen katoamisen. (Dovis 2015, s. 19-20). Seuraavaksi tutustumme tarkemmin edellä mainittuihin erilaisiin signaalihäirinnän muotoihin sekä niiden mitigointiin esitettyihin ratkaisuihin.

### 4.2.1 Väärentäminen

Kuten edellä mainittu, signaalin väärentäminen on yksi signaalihäirinnän muoto. Koska GNSS-järjestelmien käyttämien signaalien taajuus on yleisesti tiedossa (1575.42Mhz, 1227.60Mhz ja 1176Mhz), on signaalin väärentäminen suhteellisen helppoa. Artikkelissaan Ranyal ja Jain (2020) esittävät kaksi väärentämisen muotoa: salainen (engl. *covert*) ja avoin (engl. *overt*). Avoin signaalin väärentäminen perustuu *Jam-then-spoof* strategialle, jossa signaalin tukkimisella aiheutetaan ensin vastaanottimen yhteyden menettäminen alkuperäiseen GPS-signaaliin, jonka jälkeen yhteyden uudelleen muodostuksessa GPS-vastaanotin tarttuu väärennettyyn, voimakkaampaan signaaliin. Salainen signaalin väärennys perustuu avoimesta väärennyksestä poiketen strategiaan, jossa väärennetty GPS-signaali ensin kohdistetaan li-

mittäin autenttisen signaalin kanssa ja väärennettyä signaalia voimistamalla tavoitellaan vastaanottimen lukittautumista väärennettyyn signaaliin. (Ranyal ja Jain 2020).

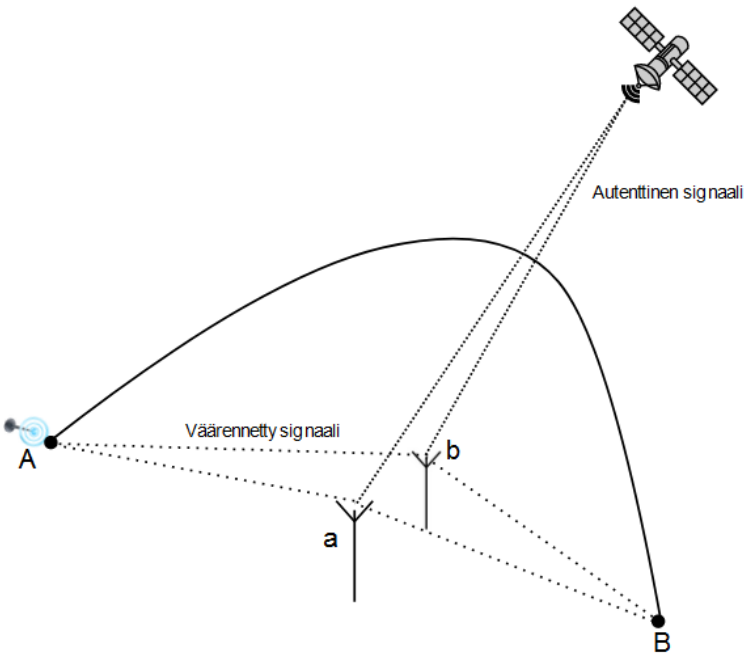
### 4.2.2 Tukkiminen

Tukkimisessa GNSS-signaali peitetään samalla taajuudella lähetetyllä häiriösignaalilla, jolloin vastaanotin ei pysty vastaanottamaan aitoa GNSS-signaalia. Mittava osa GNSS-signaalien tukkimisista suoritetaan niin kutsutuilla PPD-laitteilla (*Personal Privacy Device*). (Ioannides, Pany ja Gibbons 2016). Artikkelissaan Mitch ym. (2012) esittävät 18 erilaista siviilikäyttöistä, kaupallista PPD-laitetta. Laitteita vertailevassa testissä ilmeni, että heikoin PPD-laitteista vaikutti signaalillaan kaupallisen GNSS-vastaanottimen toimintaan 300 metrin päästä, kun taas voimakkain laitteista jopa 6 kilometrin päähän. Vuoden 2012 hinnoilla laitteiden hinnat vaihtelivat muutamasta kymmenestä Yhdysvaltain dollarista muutamaan sataan dollariin. (Mitch ym. 2012). Artikkelin tulokset alleviivaavat sitä, kuinka vähäisillä kustannuksilla on mahdollista GNSS-signaalien heikkouksia hyödyntäen tuottaa merkittävää haittaa signaalien käyttäjille. Vähäiset kustannukset luovat myös yksittäisille toimijoille mahdollisuuden aiheuttaa signaalihäirintää.

## 4.3 Mitigointi

Erilaiset signaalihäirinnän muodot ovat laajalti tutkittu aihealue, ja näin ollen signaalihäiriöitä vastaan on esitetty monenlaisia suojautumistekniikoita. GNSS-järjestelmien haavoittuvuuksia tutkineet Schmidt ym. (2016) jakavat signaalihäirinnältä suojautumisen menetelmät neljään kategoriaan: antennipohjaisiin, salauspohjaisiin, signaalin prosessointiin liittyviin sekä korreloiviin menetelmiin. Seuraavaksi luvussa esitellään yleisesti jokaiseen kategoriaan kuuluvia suojausmenetelmiä, sekä niiden mahdollisia heikkouksia.

Eräs antennipohjainen suojautumismenetelmä, *Angle of Arrival discrimination* (AoA) perustuu kahteen tai useampaan, lähelle toisiaan sijoitettuun antenniin, jotka määrittelevät vastaanottamiensa signaalien saapumiskulmien perusteella signaalin lähteen näennäisetäisyyden sekä lähteen osoitussuunnan. Suojauksen toimintaa on visualisoitu kuviossa 3. Näennäisetäisyyksien avulla voidaan johtaa signaalin lähde johonkin kuviossa esitetyn kaaren A-B




Kuvio 3. AoA-suojaus. (Muokattu Schmidt ym. (2016) pohjalta)

alueelle. Jos signaalin lähde on maan pinnalla, sijaitsee se joko pisteessä A tai B. Lähteen etäisyyden perusteella on mahdollista päätellä onko vastaanotetun signaalin alkuperä toivottu vai mahdollisesti väärennyslaitteen tuottamaa. Väärennyslaitteista vastaanotetut signaalit usein myös saapuvat antenneille samasta saapumiskulmasta, joka eroaa satelliitteista, joiden lähettämien signaalien saapumiskulmat kiertoradan vuoksi vaihtelevat. Tämä tekee väärennettyjen signaalien havaitsemisesta suhteellisen helppoa. (Schmidt ym. 2016). AoA-suojaus on kuitenkin mahdollista ohittaa asettamalla yksittäisiä synkronoituja kannettavia väärentämislaitteita antennien läheisyyteen. Tämä suojauksen ohitustekniikka on kuitenkin hyvin monimutkainen ja kallis, mikä tekee siitä epätodennäköisen, mutta samalla hyvin vaikean havaita. (Humphreys ym. 2008).

Signaalinhäirinnän mitigoimiseksi on esitetty useita salaukseen pohjautuvia suojautumismenetelmiä. Yhtenä suojauksen tyyppinä on esitetty niin kutsuttua symmetristä salausta, jossa lähettävä satelliitti ja vastaanotin käyttävät molemmat salattua avainta. Tätä menetelmää on kuitenkin haastava käyttää, koska avainten jakamiseen vastaanottajille tarvittaisiin jokin turvallinen tapa. Ratkaisuksi tähän on esitetty salausta, jossa hyödynnetään siviililähetyskoodin

ja salatun sotilaskoodin tunnettua suhdetta. Tällä menetelmällä vastaanotin ei tarvitsisi salausavainta. Kaksi vastaanotinta, joista toinen on varmasti väärennetyltä signaalilta suojassa, vertaavat signaaleita toisiinsa, jotta voidaan etsiä korrelaatiopiikkiä, joka osoittaa signaalien aitouden. Tämä järjestelmä voi toimia jälkikäteen tai lähes reaaliajassa, jos korkean kaistanleveyden viestintäyhteys on saatavilla vastaanottimien välillä. (Psiaki ja Humphreys 2016).

Kuten luvussa 2 selvisi, signaalin prosessointi vastaanottimessa koostuu monesta vaiheesta. Signaalin prosessointiin liittyvät suojausmenetelmät eroavat Schmidt ym. (2016) mukaan sekä salaamiseen pohjautuvista että fyysisistä suojautumismenetelmistä siinä, että ne eivät vaadi muutoksia nykyisiin laitteistoihin tai protokolliin. Signaalin prosessointiin liittyviä suojausmenetelmiä on esitetty useita, joista yhtenä käytetyimmistä on RAIM-menetelmä (*Receiver Autonomous Integrity Monitoring*). RAIM-suojaus perustuu käytettävissä olevien GNSS-signaalien spatiaalisen yhdenmukaisuuden varmistamiseen, joka sulkee pois poikkeavat signaalit. RAIM-suojauksen heikkoutena on esitetty suojausmenetelmän oletus siitä, että poikkeavia signaaleja on vain yksi tai kaksi. (Schmidt ym. 2016).

Toinen signaalin prosessointiin pohjautuva suojausmenetelmä on niin kutsuttu *Absolute Power*. Tämä menetelmä yksinkertaisuudessaan vertaa vastaanotetun signaalin voimakkuutta oletettuun autenttisen signaalin voimakkuuteen. Menetelmää on kuvailtu helposti toteutettavaksi suojaustoimeksi, mutta sen on arvioitu myös olevan herkkä tuottamaan vääriä positiivisia, sillä esimerkiksi olosuhteet ionisfäärissä voivat vaikuttaa signaalin voimakkuuteen. (Schmidt ym. 2016).

Korreloivat menetelmät sen sijaan tarkoittavat suojausmenetelmiä, jotka perustuvat paikka- ja aikatiedon vertaamiseen toisen lähteen, esimerkiksi IMU:n (*Inertial measurement unit*) kanssa. Korreloivien suojausmenetelmien on esitetty olevan teoriassa mahdollisia, jos toinen lähde on tarpeeksi tarkka. Ongelmaksi kuitenkin nousee saatavuus; Jos toisena paikka- ja aikatiedon lähteenä käytetään esimerkiksi Cesium-pohjaista atomikelloa, olisi tämä menetelmä liian kallis yleiseen käyttöön. Tätä halvemmat ratkaisut sen sijaan eivät olisi tarpeeksi tarkkoja, ja menettäisivät nopeasti synkronisoinnin GNSS-ajan kanssa. (Schmidt ym. 2016)

# 5 Yhteenveto

Tässä tutkielmassa käytiin läpi satelliittipaikannusjärjestelmien haavoittuvuuksia, haavoittuvuuksien synnyttämiä riskejä ja uhkia yhteiskunnan eri sektoreille sekä näihin esitettyjä suojautumiskeinoja. Satelliittipaikannusjärjestelmien yleisin haavoittuvuus koskee signaalihärintää, joka voidaan toteutustavan ja tarkoituksen mukaan jakaa kahteen osa-alueeseen: väärentämiseen sekä tukkimiseen. Huomionarvoista oli myös esille noussut luonnonilmiö, skintillaatio, joka voi aiheuttaa häiriöitä GNSS-signaaliin.

Tutkielmassa tarkasteltiin myös tarkemmin signaalihäirinnän eri muotoja. Näistä yleisimmät, väärentäminen ja tukkiminen ovat vakava uhka varsinkin siviilikäyttöisille, salaamattomia signaaleja käyttäville vastaanottimille. Tutkielmassa nousi esiin väärentämistä sekä tukkimista vastaan esitettyjä erilaisia suojautumiskeinoja, jotka jakautuivat neljään kategoriaan: salauspohjaisiin, korreloiviin, antennipohjaisiin sekä signaalin prosessointiin perustuviin suojautumiskeinoihin.

Esiin nousseista suojautumismenetelmistä selvisi, että vain salauspohjaiset menetelmät ovat suojaus, joka on lähes mahdoton kiertää. Salauspohjaisten suojausten implementoiminen jo valmiisiin protokolliin ja satelliitteihin ei tosin ole mahdollista, joten niin kutsut legacy-signaalit eivät todennäköisesti ikinä tule olemaan täysin turvassa signaalihäirinnältä. Siviilisektorin olisikin tärkeää siirtyä tulevaisuudessa käyttämään uudempia, suojattuja signaaleita.

Tutkielmassa nousi lisäksi esille yhteiskunnan eri sektoreiden valmiuksia kohdata GNSS-järjestelmien häiriötilanteita. Finanssisektoriin integroidut varajärjestelmät, sekä Yhdysvaltain ja sen liittolaisten asevoimien käyttämät M-koodin signaalit ovat keinoja vastata signaalihäirinnän uhkaan ja esimerkiksi finanssisektorilla häiriötilanteiden vaikutusten onkin arvioitu jäävän pieneksi. Näistä poiketen sekä lentoliikenteen sekä tietoliikenneyritysten voidaan nähdä olevan taloudellisesti haavoittuvassa asemassa häiriötilanteissa. Näillä sektoreilla olisikin tärkeää kehittää resilienssiä ja palautumista häiriötilanteista esimerkiksi integroimalla varajärjestelmiä.

# Lähteet


Dowd, Mark, John McDonald ja Justin Schuh. 2006. *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities (Volume 1 of 2).* 1. painos. 19–20. Addison Wesley Professional.

Dovis, Fabio. 2015. *GNSS Interference Threats and Countermeasures.* Artech House GNSS Technology and Applications Series. Boston: Artech House. https://web.p.ebscohost.com/ehost/ebookviewer/ebook/ZTAwMHh3d19fMTE1NTIwM19fQU41?sid=13b6360e-53a7-4fc5-8dfc-05b4b9525857@redis&vid=0&format=EB&rid=1.

Eurocontrol. 2021. *Does Radio Frequency Interference to Satellite Navigation pose an increasing threat to Network efficiency, cost-effectiveness and ultimately safety?,* maaliskuu. https://www.eurocontrol.int/sites/default/files/2021-03/eurocontrol-think-paper-9-radio-frequency-intereference-satellite-navigation.pdf.

Hegarty, Christopher J. 2012. "GNSS signals — An overview". Teoksessa *2012 IEEE International Frequency Control Symposium Proceedings,* 1–7. https://doi.org/10.1109/FCS.2012.6243707.

Humphreys, Todd E., Brent M. Ledvina, Mark L. Psiaki, Brady W. O'Hanlon ja Paul M. Kintner. 2008. *Assessing the spoofing threat: Development of a portable GPS civilian spoofer,* tammikuu. https://repositories.lib.utexas.edu/handle/2152/63316.

Ioannides, Rigas Themistoklis, Thomas Pany ja Glen Gibbons. 2016. "Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques". *Proceedings of the IEEE* 104 (6): 1174–1194. https://doi.org/10.1109/JPROC.2016.2535898.

Kaplan, Elliott D., ja C. Hegarty. 2017. *Understanding GPS/GNSS : Principles and Applications.* Nide Third edition. GNSS Technology and Applications Series. Artech House. ISBN: 9781630810580. https://web.p.ebscohost.com/ehost/detail/detail?vid=2&sid=7bc05150-51e3-4c94-942a-bc97b427c4c0%40redis&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#AN=1825930&db=nlebk.

Mitch, Ryan H., Mark L. Psiaki Ryan C. Dougherty, Steven P. Powell, Brady W. O'Hanlon, Jahshan A. Bhatti ja Todd E. Humphreys. 2012. "Know your enemy: Signal characteristics of civil GPS jammers". *GPS World* 23 (tammikuu): 64–71. http://digital.gpsworld.com/January2012.

Montenbruck, Oliver, Peter Steigenberger ja André Hauschild. 2020. "Comparing the 'Big 4' - A User's View on GNSS Performance". Teoksessa *2020 IEEE/ION Position, Location and Navigation Symposium (PLANS),* 407–418. https://doi.org/10.1109/PLANS46316.2020.9110208.

NASA. 2019. *Controlled flight toward terrain (CFTT).* https://asrs.arc.nasa.gov/docs/cb/cb_473.pdf.

National Coordination Office for Space-Based Positioning, Navigation and Timing. 2020. "New Civil Signals". Viitattu 3. huhtikuuta 2023. https://www.gps.gov/systems/gps/modernization/civilsignals/.

National Coordination Office for Space-Based Positioning, Navigation, and Timing. 2022. "Space Segment". Viitattu 3. huhtikuuta 2023. https://www.gps.gov/systems/gps/space/.

National Institute of Standards and Technology. 2023. *National Vulnerability Database.* https://nvd.nist.gov/vuln. Accessed: March 11, 2023.

O'Connor, A. C., M. P. Gallaher, K. B. Clark-Sutton, D. Lapidus, Z. Oliver, T. J. Scott ja D. Wood. 2019. *Economic benefits of the Global Positioning System (GPS).* https://www.rti.org/publication/economic-benefits-global-positioning-system-gps.

Psiaki, Mark L., ja Todd E. Humphreys. 2016. "GNSS Spoofing and Detection". *Proceedings of the IEEE* 104 (6): 1258–1270. https://doi.org/10.1109/JPROC.2016.2526658.

Ranyal, Eshta, ja Kamal Jain. 2020. "Unmanned Aerial Vehicle's Vulnerability to GPS Spoofing a Review". *Journal of the Indian Society of Remote Sensing* 49 (3): 585–591. ISSN: 0255-660X. https://doi.org/10.1007/s12524-020-01225-1. https://browzine.com/articles/422387493.

Rui, Zixuan, Xiaofeng Ouyang, Fangling Zeng ja Xu Xu. 2022. “Blind Estimation of GPS M-Code Signals under Noncooperative Conditions”. *Wireless Communications  Mobile Computing (Online)* 2022. https://www.proquest.com/scholarly-journals/blind-estimation-gps-m-code-signals-under/docview/2727492798/se-2.

Schmidt, Desmond, Kenneth Radke, Seyit Camtepe, Ernest Foo ja Michał Ren. 2016. “A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures”. *ACM Computing Surveys* 48 (toukokuu): 1–31. https://doi.org/10.1145/2897166.

Sharifi-Tehrani, Omid, Mohamad Farzan Sabahi ja Meysam Raees Danaee. 2022. “Efficient GNSS Jamming Mitigation Using the Marcenko Pastur Law and Karhunen–Loeve Decomposition”. *IEEE Transactions on Aerospace and Electronic Systems* 58 (3): 2291–2303. https://doi.org/10.1109/TAES.2021.3131400.

Shirey, R. 2007. *Internet Security Glossary, Version 2.* https://www.rfc-editor.org/rfc/rfc4949#section-5.

Westbrook, Tegg. 2019. “The Global Positioning System and Military Jamming: geographies of electronic warfare”. *Journal of Strategic Security* 12 (2): 1–16. ISSN: 19440464, 19440472, viitattu 3. huhtikuuta 2023. https://www.jstor.org/stable/26696257.

Xue, Dabin, Jian Yang ja Zhizhao Liu. 2022. “Potential Impact of GNSS Positioning Errors on the Satellite-Navigation-Based Air Traffic Management”. E2022SW003144 2022SW003144, *Space Weather* 20 (7): e2022SW003144. https://doi.org/https://doi.org/10.1029/2022SW003144. eprint: https://agupubs.onlinelibrary.wiley.com/doi/pdf/10.1029/2022SW003144. https://agupubs.onlinelibrary.wiley.com/doi/abs/10.1029/2022SW003144.

Yao, Wenxuan, Yong Liu, Dao Zhou, Zhuohong Pan, Micah Till, Jiecheng Zhao, Lin Zhu, Lingwei Zhan, Qiu Tang ja Yilu Liu. 2017. “Impact of GPS signal loss and its mitigation in power system synchronized measurement devices”. Teoksessa *2017 IEEE Power  Energy Society General Meeting,* 1–1. https://doi.org/10.1109/PESGM.2017.8274578.

Ziedan, Nesreen I. 2006. *GNSS Receivers for Weak Signals.* GNSS Techology And Application Series. Artech House. ISBN: 9781596930520. https://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=225165&site=ehost-live.