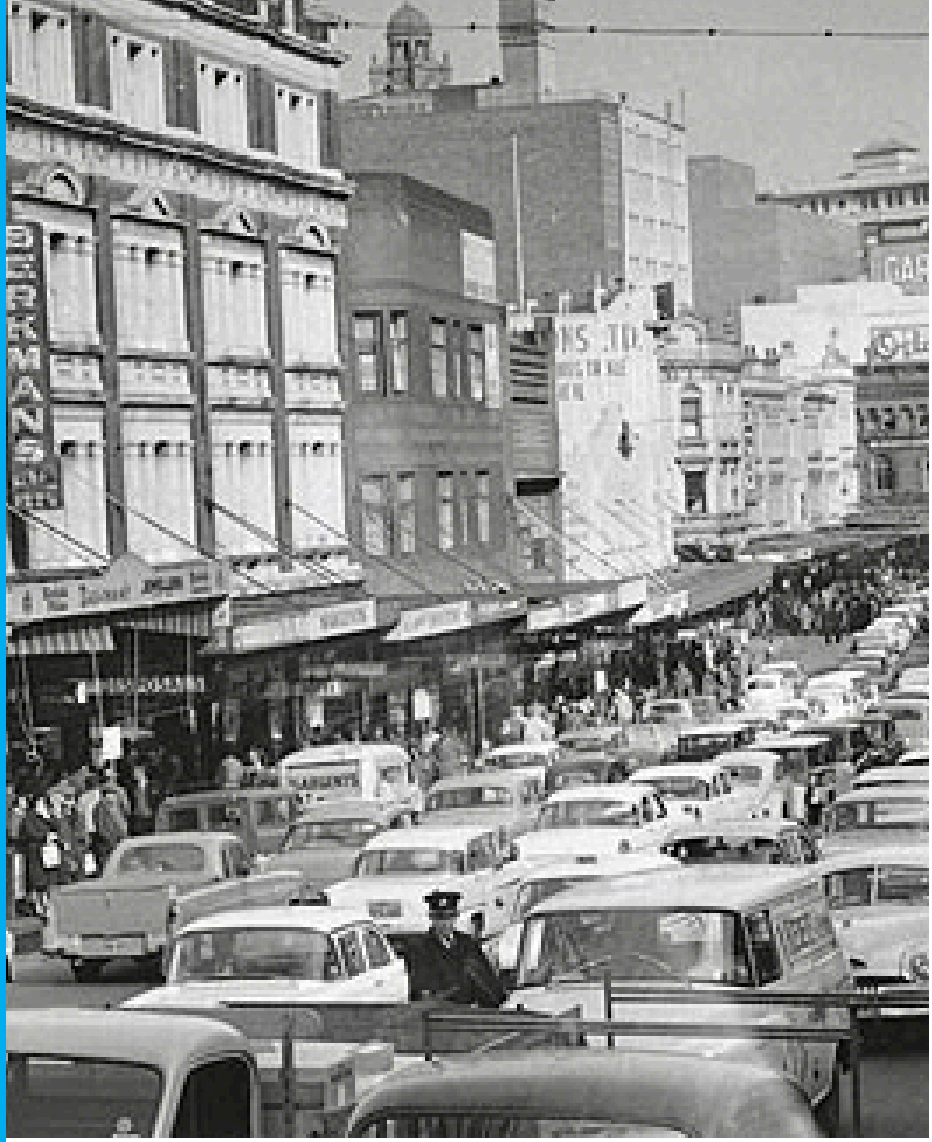


TECHNOLOGY • RESEARCH HIGHLIGHTS • VISIONS • SCIENCE

253

Liikenteen sähköisten palveluiden tietoturva – niihin kohdistuvat tietoturvariskit ja häirintämenetelmät sekä näiden vaikutukset ja ennaltaehkäisy

Sami Lehtonen | Ari Virtanen | Hanna Askola

VTT

VTT TECHNOLOGY 253

Liikenteen sähköisten palveluiden tietoturva – niihin kohdistuvat tietoturvariskit ja häirintämenetelmät sekä näiden vaikutukset ja ennaltaehkäisy

Sami Lehtonen, Ari Virtanen & Hanna Askola

ISBN 978-951-38-8406-2 (URL: http://www.vtt.fi/julkaisut)

VTT Technology 253

ISSN-L 2242-1211
ISSN 2242-122X (Verkkojulkaisu)
http://urn.fi/URN:ISBN:978-951-38-8406-2

JULKAISIJA – UTGIVARE – PUBLISHER

Teknologian tutkimuskeskus VTT Oy
PL 1000 (Tekniikantie 4 A, Espoo)
02044 VTT
Puh. 020 722 111, faksi 020 722 7001

Teknologiska forskningscentralen VTT Ab
PB 1000 (Teknikvägen 4 A, Esbo)
FI-02044 VTT
Tfn +358 20 722 111, telefax +358 20 722 7001

VTT Technical Research Centre of Finland Ltd
P.O. Box 1000 (Tekniikantie 4 A, Espoo)
FI-02044 VTT, Finland
Tel. +358 20 722 111, fax +358 20 722 7001

Alkusanat

Teknologian tutkimuskeskus VTT Oy on tehnyt tutkimuksen, joka käsittelee liikenteen sähköisten palveluiden tietoturvaa sekä tarkastelee kilometriveron välttelyn menetelmiä ja niihin varautumista. Lisäksi tarkasteltiin paikannuksen aktiivisen häirinnän vaikutuksia muihin kuin kilometriverojärjestelmään itseensä. Työ tehtiin osana Liikenteen sähköiset palvelut -tutkimusta. Tutkimuksesta vastasivat Sami Lehtonen, Ari Virtanen ja Hanna Askola.

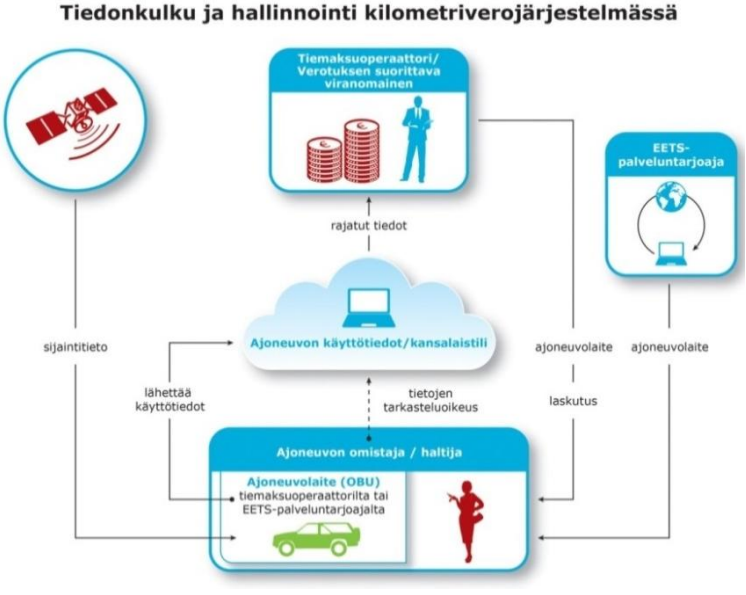
Tutkimuksen rahoittivat Tekes, Liikennevirasto, Trafi ja liikenne- ja viestintäministeriö (LVM). Hankkeen ohjausryhmän jäseniä olivat Juuso Kummala Liikennevirastosta, Anders Granfelt Trafista, Leif Beilinson ja Seppo Öörni LVM:stä, Sami Sahala ja Mikko Lehtonen Helsingin kaupungilta, Sampo Hietanen ITS Finlandista ja Karri Rantasila VTT:ltä.

Sisällysluettelo

1. Johdanto

Liikenneministeri Merja Kyllönen asetti 3.2.2012 työryhmän selvittämään, miten Suomessa voitaisiin edetä kohti oikeudenmukaisempaa ja älykkäämpää liikennejärjestelmää ja miten tulisi edetä tiemaksujärjestelmien käyttöönotossa pitkällä aikavälillä. Hallitusohjelmaan oli kirjattu, että hallitus selvittää satelliittipaikannukseen perustuvien tienkäyttömaksujen käyttöönottoa Suomessa. Asetetun työryhmän puheenjohtajana toimi Jorma Ollila, ja työryhmä julkaisi raporttinsa 16.12.2013 (LVM 2013).

Suunnitelmat siirtymisestä ajoneuvoverotuksessa käyttöön perustuvaan ns. kilometriveroon nostavat esiin myös veron välttelyn menetelmät. Vero kerättäisiin ajoneuvoon asennettavalla päätelaitteella, joka mittaa ajoneuvolla ajetun matkan eri tariffialueilla. Kuva 1 esittää kaavaillun järjestelmän periaatetta.



Kuva 1. Kilometriveron keruujärjestelmä (LVM 2013).

Kaiken internet tai esineiden internet, englanniksi Internet of Things (IoT), jossa yhä useammat laitteet kommunikoivat tilastaan, on merkittävä kehitystrendi. Käyttäjille IoT lupaa palveluita, jotka toimivat aiempaa tarkemmin ja tehokkaammin sekä ovat laajemmin saatavilla. Palveluiden toteuttamisessa hyödynnetään mm. pilvipalveluita ja laitteista kerättävää massadataa (big data). Myös nyt näköpiirissä olevat tulevaisuuden liikenteen sähköiset palvelut, jotka hyödyntävät paikannustietoa ja muuta liikenteestä kertyvää tietoa, ovat eräänlaisia IoT-sovelluksia.

Tässä raportissa käsitellään erityisesti satelliittipaikannukseen tukeutuvan suoriteperusteisen verotusjärjestelmän tietoturvariskejä. Verotuksen lisäksi laite saattaisi mahdollistaa myös lisäpalveluja. Raportissa käsitellään tähän kokonaisuuteen liittyviä tietoturvariskejä niin viranomaisten, palveluntuottajien kuin kuluttajienkin näkökulmista. Lisäksi tarkastellaan lyhyesti erilaisia teknisiä keinoja manipuloida ajoneuvolaitetta (OBU) ja keinoja estää manipulointiyritykset.

Yksi välttelykeinoista on käyttää satelliittipaikannuksen häirintälaitetta. Satelliittipaikannusta käytetään hyvin monilla eri alueilla yhteiskunnassa. Jos häirinnästä tulee laajamittaista, sillä voi olla vaikutusta muuallakin kuin liikenteessä. Jälkimmäisessä osiossa tarkastellaan satelliittipaikannuksen sovellusalueita ja häirinnän mahdollista vaikutusta niiden toimintaan.

Luvussa 2 tarkastellaan tietoturvan määritelmiä yleisellä tasolla, taustoitetaan tutkimuksen menetelmiä ja tarkastellaan suorituspohjaista verotusta palveluna. Luvussa 3 käsitellään suoriteperusteisen ajoneuvoverotuksen ja sen ohessa mahdollisesti tarjottavien lisäpalveluiden tietoturvariskejä eri osapuolten näkökulmista.

Luvussa 4 tarkastellaan lyhyesti GPS-signaalien häirinnän ja väärentämisen tekniikkaa sekä aikasynkronointia. Satelliittipaikannusta voidaan paikanmäärityksen lisäksi käyttää myös tarkan ajan lähteenä, sillä järjestelmä perustuu erittäin tarkkoihin keskenään synkronoituihin atomikelloihin.

Luvussa 5 käydään lävitse erilaiset ajoneuvolaitteen manipuloinnin mahdollisuudet sekä tarkastellaan manipuloinnin havaitsemista ja sen estämistä. Luvussa tarkastellaan myös ajoneuvolaitteen sertifiointia.

Viimeinen luku 6 käsittelee satelliittipaikannukseen perustuvien järjestelmien käyttöä yhteiskunnassa eri aloilla ja häirinnän vaikutuksia. Lopuksi esitetään loppuyhteenveto ja päätelmät.

2. Mitä on tietoturva?

Klassinen jako sisältää kolme eri tietoturvan osa-aluetta: luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability). Nämä kaikki olisi saavutettava, jotta voidaan puhua tietoturvallisesta järjestelmästä. Neljäntenä osa-alueena on pidetty kiistämättömyyttä (non-repudiability). Sitä ei yleensä nosteta em. kolmen muun osa-alueen rinnalle, koska tapauskohtaisesti kiistettävyys voi olla myös tavoiteltavaa, esimerkiksi anonymiteetin takaamiseksi.

Tavanomaisesti tietoturva pyritään huomioimaan mm. sellaisilla suunnitteluperiaatteilla kuin *pienimmän oikeuden periaate* (least privilege principle eli yksikään taho tai käyttäjä ei voi käyttää järjestelmässä muita toimintoja kuin itselleen tarpeellisia) ja *tarpeen tietää -periaate* (need to know principle eli mikään taho ei saa käsiinsä muuta kuin oman toimintansa kannalta välttämätöntä tai tarpeellista tietoa). Jos järjestelmän vaatimukset on määritelty väärin, on lopputuloksena joko toimimaton tai tietoturvaton palvelu.

Tietoturva on tasapainoilua luottamuksen ja eheyden ja toisaalta saatavuuden välillä, minkä havainnollistaa hyvin taulukko kuluttajille suunnatussa tietoturvaoppaassa (ks. taulukko 1).

Taulukko 1. Suojauskeinot ja niiden avulla saavutettava suoja luottamuksellisuuden, eheyden ja saatavuuden kannalta (FiCoRa 2016).

Toimenpide	Luottamuksellisuus	Eheys	Saatavuus
Sähköpostin salaus	Parantaa	Ei vaikutusta	Heikentää
Sähköinen allekirjoitus	Ei vaikutusta	Parantaa	Ei vaikutusta
Hyvän salasanan käyttö / PIN-koodit	Parantaa	Ei vaikutusta	Heikentää
Ohjelmistojen ajantasaiset päivitykset	Parantaa	Parantaa	Parantaa
WLAN-verkon avoimuus	Heikentää	Heikentää	Parantaa
Tiedon tai kovalevyn/muistitikun salaaminen	Parantaa	Ei vaikutusta	Heikentää
Yleisimpien pilvipalveluiden käyttö	Heikentää	Ei vaikutusta	Parantaa
WLAN-verkon WPA 2 -salaus	Parantaa	Ei vaikutusta	Ei vaikutusta

2.1 Taustaa

Aiemmin tehdyn kyselyn perusteella 42 % haastatelluista oli huolissaan suoriteperusteisen kilometriveron keruuta varten toteutettavan järjestelmän tietoturvasta (Innamaa ym. 2015). Kuluttajien suhtautuminen yksityisyyden suojaan vaihtelee hieman maittain. Tutkimuksissa on todettu kuluttajien jakautuvan kolmeen pääryhmään: 10 % on hyvin luottavaisia, eli heitä ei huoleta tietojen käyttö mitenkään, 25 % omaa hyvin tiukan asenteen yksityisyyden suojan heikkenemiseen, ja loput 65 % on kyllä huolissaan, mutta valmiita luopumaan yksityisyyden suojasta etenkin, jos he katsovat saavansa jotain hyödyllistä vastineeksi (Heino 2016). Käyttäjät ovat huomattavasti halukkaampia uhraamaan oman yksityisyytensä tai sen suojan vapaaehtoisesti kuin pakotettuna menettämään sen suhteessa viranomaiseen.

Liikenteestä kerättyä dataa käytetään maailmalla jo monin tavoin liikenteen valvontaan ja ohjaukseen. Aina se ei ole onnistunut kovin tietoturvallisesti, kuten Las Vegasissa 2014 järjestetyssä DEF CON 22 -tapahtumassa esiteltiin. Varsin helposti onnistuttiin syöttämään väärää tietoa liikennetietoa keräävään sensoriverkkoon, joka voitiin saada jumiutumaan, tai sille uskoteltiin, että liikennettä ei ole laisinkaan. (DEFCON22 2014.)

Haasteita tietoturvakuvaan tuovat eri toimijoiden varsin erilaiset lähtökohdat. Viranomaistahon toimintaa säätelee ensisijaisesti julkisuuslaki, kun taas palveluntarjoajia ohjaavat ennen kaikkea vapaa kilpailu ja liikesalaisuudet. Toisaalta palveluntarjoajista operaattoreita säätelee myös tietoyhteiskuntakaari[1], joka asettaa ne muista poikkeavaan asemaan. Kaikkia toimijoita kuitenkin säätelee tässäkin yhteydessä osaltaan henkilötietolaki, joka on EU:n tietosuojadirektiivin pohjalta laadittu kansallinen laki.

Kansalliset tietosuojalainsäädännöt ovat korvautumassa EU:n pitkään neuvotellulla yhteisellä tietosuoja-asetuksella, joka on suoraan jäsenmaita velvoittavaa lainsäädäntöä. Asetusta ryhdytään soveltamaan aikaisintaan vuonna 2018.

2.2 Riskianalyysin menetelmät

Riskianalyysi tai muu tarkempi tieturva-analyysi edellyttää aina palvelukohtaista tarkastelua palvelun tarvitsemien tietojen ja resurssien sekä toisaalta sen tarjoaman rajapinnan kautta. Analyysissä tarkastellaan myös eri osapuolten luottamusta tietoturvan näkökulmasta.

Sähköisen palvelun riskianalyysissä tunnistetaan ensin palvelun eri osapuolet. Tämän jälkeen määritellään eri osapuolten tarpeet järjestelmälle ja sen tuottamalle tiedolle, osapuolten intressit sekä näihin liittyvät haavoittuvuudet. Haavoittuvuuksiin kohdistuvien uhkien ohella arvioidaan myös niiden todennäköisyyttä. Tarkas-

[1] Laki, jonka tavoitteena on edistää sähköisen viestinnän palvelujen tarjontaa ja käyttöä sekä varmistaa, että viestintäverkkoja ja viestintäpalveluja on kohtuullisin ehdoin jokaisen saatavilla koko maassa.

telu on tässä selvityksessä tehty suoriteperusteisen kilometriveron keräämiseen tarvittavan järjestelmän eri vaihtoehtojen näkökulmasta.

Koska varsinaista suoriteperusteista kilometriverojärjestelmää ei ole määritelty eikä määrittelytyö ole myöskään käynnissä, liikenteeseen ja paikkatietoon liittyviä tietoturvauhkia käsitellään raportissa yleisellä tasolla eikä todennäköisyystarkastelua ole voitu tehdä tarkasti. LSP-hankkeessa tuotettu Yksityisyys ja luottamus -raportti kattaa osaltaan myös tietoturvan tarkastelua (Heino 2016).

Tietoturvauhkien tunnistamisessa on hyödynnetty useita julkaisuja eri palveluista ja palvelujen kehittämisestä (mm. LVM 2006, Khoo 2011) sekä mm. IoT:hen (Babar 2010, Ning 2011, Zhao 2013, Riahi 2013) ja sensoriverkkoihin kohdistuvista hyökkäyksistä (Karlof 2003, Hu 2003, Pulkkinen 2005).

2.3 Suoriteperusteinen kilometrivero palveluna

Paikannustietoja verojen tai tienkäyttömaksujen kantamiseksi voidaan kerätä eri tavoin. Yhtenä ratkaisuvaihtoehtona on selvitetty satelliittipaikannukseen perustuvaa järjestelmää. Satelliittipaikannus mahdollistaisi erilaisen verotuksen alue- ja jopa tiekohtaisesti. Muun muassa Helsingin seudun ruuhkamaksun jatkoselvityksessä (LVM 2011) on esitetty tällaista ratkaisuvaihtoehtoa. Lähes vastaavanlaiseen toiminnallisuuteen (tosin ilman kuljetun matkan mittaamista) päästään myös ajoneuvossa säilytettävän etäluettavan RFID-tunnisteen käytöllä, jos sen lukemiseen tarvittavia järjestelmiä rakennetaan eri tariffialueiden rajoille.

Vaikka satelliittipaikannukseen pohjautuva suoriteperusteinen kilonmetrivero ei saanut kannatusta julkisuudessa, ovat erilaiset ruuhkamaksu- ja tietullijärjestelmät edelleen mukana pääkaupunkiseudun liikennejärjestelmäsuunnittelussa, ainakin tulevina selvityksinä (HSL 2015).

Satelliittipaikannukseen perustuva järjestelmä tarjoaisi etäluettavaan RFID-tunnisteeseen verrattuna ylivoimaisen veroluokkien ja tiekohtaisten tariffien granulariteetin. Vastaava erottelutaso RFID-tunnisteilla toteutettuna edellyttäisi huomattavasti suurempia investointeja etäluentapisteisiin. Satelliittipaikannukseen perustuva järjestelmä tarjoaa myös mahdollisuuden kerätä liikenteestä tietoa, jota voitaisiin hyödyntää muissa palveluissa ja viranomaistoiminnassa, ml. liikennesuunnittelu ja liikenteen tilannekuva.

Tiedon hyödyntämistä varten sen tulee kuitenkin olla riittävän tuoretta, mikä asettaa vaatimuksia kerätyn tiedon muodolle ja lukemiselle. Pelkän veronkannon näkökulmasta saattaisi riittää, että tiedot ajetusta matkasta eri tariffialueilla luettaisiin esimerkiksi kerran vuodessa katsastuksen yhteydessä. Tällöin paikannustietoja ei voisi kuitenkaan hyödyntää muissa palveluissa. Tietojen keruu vain harvakseltaan hidastaisi myös ajoneuvolaitteen vikatilanteiden havaitsemista ja vaikuttaisi negatiivisesti käyttäjän oikeusturvaan vian aiheuttajaa selvitettäessä. Ajoneuvolaitteen toimivuuden varmistamiseksi sen tietoja tulisi käsitellä säännöllisesti.

Verotuksen edellyttämä tiedonkeruujärjestelmä vastaa toiminnallisuudeltaan IoT:n sensoriverkkoa. Yksittäisten sensoriverkon solmujen (eli autojen) resurssit voivat selvästi ylittää tavanomaiset sensorit, mutta verkon rakenteen ja toimintata-

van näkökulmasta vertaus on perusteltu. Monilta osin IoT:ssä onkin kyse sensoriverkosta yhdistettynä pilvipalveluiden ja massatiedon (big data) tuomiin mahdollisuuksiin.

IoT-terminologiaa käyttäen satelliittipaikantimella varustettu ajoneuvolaite on sensori, joka kerää paikannustietoa. Laite on luettavissa joko fyysisen liitännän kautta (esimerkiksi katsastuksen yhteydessä) tai langattomasti. Aggregaattorit puolestaan koostavat sensorien keräämää tietoa.

Sensoriverkolle on tyypillistä, että yksittäisten laitteiden tietoturvaominaisuudet ja -resurssit ovat varsin rajallisia. Moottoriliikenteessä on luonnollisesti käytettävissä ajoneuvon tuottama sähkövirta, mutta vaikka tällä hetkellä autoihin asennettaisiin resursseiltaan ja tietoturvaominaisuuksiltaan ajanmukaiset laitteet, seuraa ajoneuvojen pitkästä käyttöiästä se, että vanhemmassa kalustossa on käytössä muihin verrattuna rajalliset resurssit. Pitkällä aikavälillä ongelma kertautuu, koska käyttöön otettavaa järjestelmää ei haluttane uusia ja uudistaa täydellisesti parinkymmenen vuoden välein. Yhteensopivuus taaksepäin on kuitenkin tarpeen säilyttää.

Ajoneuvossa sijaitsevan mittalaitteen sijaan vaihtoehtoinen toteutustapa on tunniste (tag), jota luetaan tietyissä liikennepisteissä (tietullit). Myös tämän toteutustavan tietoturvariskejä tarkastellaan raportissa soveltuvin osin. RFID-teknologian tarjoamia mahdollisuuksia ja tietoturvariskejä on käsitelty mm. julkaisussa Khoo 2011.

3. Tietoturvariskit eri osapuolten näkökulmasta

Tässä luvussa käsitellään suoriteperusteisen kilometriverotuksen ja sen ohessa mahdollisesti tarjottavien lisäpalveluiden tietoturvariskejä eri osapuolten näkökulmista. Verotuksen ja palveluiden kokonaisuutta kutsutaan seuraavassa yleisemmin ”palveluksi”.

3.1 Viranomaisnäkökulma

Viranomaisnäkökulmasta tärkein palvelun tuottama tulos on ajosuoritteisten verojen keräämiseksi kerätty tieto. Tässä korostuu tiedon oikeellisuus. Viranomaisen kannalta tietojen vuotaminen muille tahoille ei ole merkittävää muuten kuin vastuukysymysten osalta.

Viranomaistoimintaan kuuluvat myös liikennesuunnittelu, -valvonta ja liikenteen ohjaus. Tässä toiminnassa viranomainen voi myös hyödyntää liikenteestä kerättävää tietoa, liikennemäärien, keskinopeuksien ja myös kuljettujen reittien osalta. Liikennesuunnittelussa korostuu pitkän aikavälin tietojen kerääminen, mutta liikenteen valvonnan tai ohjauksen kannalta tiedon pitää olla tuoretta – jopa reaaliaikaista.

3.1.1 Viranomaisen tietoturvariskit

Riski V1. Väärän tiedon syöttäminen järjestelmään

Hyökkääjä voi syöttää joko aidolla tai väärennetyllä paikanninlaitteella virheellisiä liikennetietoja keruupisteeseen. Tämän seurauksena järjestelmä tuottaa virheellistä informaatiota a) verotukseen, b) liikenteen valvontaan ja ohjaukseen. Verotuksen osalta pyrkimys on todennäköisesti välttää verotusta. Väärä liikenneinformaatio hankaloittaisi liikenteen ohjaamista.

Todennäköisyys: kohtalainen

Riski V2. Tiedon puuttuminen laitteesta

Käyttäjällä, mutta myös mahdollisella ulkopuolisella hyökkääjällä, voi olla pääsy laitteeseen joko fyysisesti tai radiorajapinnan kautta.
Käyttäjä tai muu taho voi muokata laitteeseen tallennettua tietoa pyrkimyksenään vähentää käytöstä seuraavia veroja tuhoamalla tietoja.
Laite voi olla myös mahdollista nollata fyysisen rajapinnan kautta.

Todennäköisyys: suuri

Riski V3. Tiedon manipulointi laitteessa

Käyttäjällä, mutta myös mahdollisella ulkopuolisella hyökkääjällä, voi olla pääsy laitteeseen joko fyysisesti tai radiorajapinnan kautta.
Käyttäjä tai muu taho voi muokata laitteeseen tallennettua tietoa pyrkimyksenään vähentää käytöstä seuraavia veroja joko ajosuoritteita poistamalla tai muuttamalla maksuluokkaa.

Todennäköisyys: suuri

Riski V4. Muusta syystä virheellinen tieto

Järjestelmävirheen tai muun seurauksena paikkatietoa ja siten ajosuoritetta ei saada tallennettua. Myös paikantimen antama sijaintitieto voi olla virheellinen.

Todennäköisyys: kohtalainen

Riski V5. Vanhentunut tieto

Pelkän veronkannon näkökulmasta tiedon iällä ei ole merkitystä – riittää, että verokauden ajalta tiedot saadaan kauden lopussa verotuspäätöksen tekemistä varten. Myös useamman vuoden aikajänteellä tehtävälle liikennesuunnittelulle riittää varsin harvoin tehtävä tiedonkeruu. Muun viranomaistoiminnan kannalta tiedon tuoreus on kuitenkin tärkeää.
Saatu tieto on vanhaa, eikä siitä ole enää viranomaiskäytössä hyötyä.

Todennäköisyys: riippuu teknisestä toteutustavasta

3.2 Palveluntuottajan näkökulma

Palveluntuottaja voi hyödyntää kerättyjä liikennetietoja omassa muussa palvelutuotannossaan. Lisäpalvelut voivat perustua paikannustietoihin tai niistä johdettuihin liikennetietoihin, tai näitä tietoja voidaan käyttää muiden palveluiden markkinoinnissa.

3.2.1 Palveluntuottajan tietoturvariskit

Riski P1. Väärä identiteetti

Palvelutuottaja voi erehtyä luulemaan sille esitetyn tiedon perusteella ajoneuvoa ja siten palvelun käyttäjää joksikin toiseksi. Väärän identiteetin turvin hyökkääjä voi saavuttaa etuja tai palveluita, jotka eivät olisi hänelle kuuluneet. Tämä riski koskee myös käyttäjää, esim. verotuksen kohdentuminen väärälle käyttäjälle.

Todennäköisyys: kohtalainen palveluissa, joihin kirjaudutaan sisään lyhytaikaisesti. Verotuksen osalta vähäinen, koska käyttäjien ajohistoria voidaan analysoida.

Riski P2. Väärä tieto käyttäjästä

Jonkin toisen tietoturvariskin realisoitumisen seurauksena palveluntuottaja saa järjestelmän kautta virheellistä tietoa yksittäisen käyttäjän sijainnista. Väärän sijainnin perusteella palveluntarjoajalle voi syntyä vahinkoa.

Todennäköisyys: vähäinen, mikäli palvelu perustuu liikennevirtojen analyysiin eli useiden laitteiden tietoihin

Riski P3. Palvelunesto

Järjestelmä, joka kerää tietoja sadoista tuhansista käyttäjistä, tarjoaisi suurta kapasiteettia, ja se myös suojattaisiin ns. palvelunestohyökkäyksiltä. Siitä huolimatta ei ole mahdotonta, että palvelu saataisiin sitä häiritsemällä hetkellisesti pois käytöstä. Vaikka verotietojen keruu todennäköisesti onnistuisi hyökkäyksen päätyttyä (riippuen toteutustavasta), kerättyihin tietoihin perustuvat ajantasaiset lisäpalvelut olisivat väliaikaisesti pois käytöstä.

Todennäköisyys: verotietojen osalta pieni, riippuen tosin toteutustavasta

Riski P4. Tietojen puuttuminen tai poistaminen

Taustajärjestelmään tulee tallentaa merkittävä määrä tietoa verotuksen määräämiseksi sekä tietojen oikeellisuuden varmistamiseksi. Kerättyjä tietoja analysoidaan myös väärinkäyttäjien havaitsemiseksi.
Väärinkäyttäjiä saatetaan havainnoida lisäksi erillisillä tienvarsiyksiköillä, jotka keräävät esim. tietoa rekisterikilvistä. Mikäli näihin tietovarantoihin päästäisiin käsiksi, väärinkäyttäjien havaitseminen vaikeutuisi.

Todennäköisyys: kokonaisuutena pieni, mikäli järjestelmän haavoittuvuudet kartoitetaan tarkasti

Riski P5. Tietovuoto

Mikäli palveluntarjoajan järjestelmiin tallentuu samankaltaista tietoa käyttäjien identiteetistä kuin verotuskäyttöön tarvitaan tai palveluntarjoaja ylläpitää viranomaisjärjestelmää suoraan verottajan puolesta, syntyy vastuukysymyksiä mahdollisten tietovuotojen osalta.

Todennäköisyys: kohtalainen

3.3 Käyttäjän/kuluttajan näkökulma

Käyttäjän näkökulmasta tärkeimmät tietoturvatavoitteet ovat yksityisyyden suojaaminen, jota tarkastellaan laajemmin toisessa raportissa (Heino 2016), ja ajosuoritteista tallennettavan tiedon oikeellisuus.

Käyttäjä voi hyötyä kerätystä tiedosta myös lisäpalveluiden kautta, esim. palvelun, joka opastaa taloudelliseen ajotapaan.

Käyttäjän tietoturvariskit:

Riski K1. Paikkatietojen salakuuntelu

Jos kerättyjä paikannustietoja luetaan langattomasti, jokin taho voi salakuunnella tiedonsiirtoa ja saada siten haltuunsa tietoja ajoneuvon (ja sen kuljettajan) sijainnista eri aikoina ja sillä suoritetuista matkoista.

Todennäköisyys: vähäinen, mikäli tiedonsiirto toteutetaan salattuna

Riski K2. Paikkatietojen oikeudeton lataaminen

Tietoja luetaan laitteesta käynnistämällä tiedonsiirto ilman käyttäjän tunnistusta tai väärentäen tunnistus. Näin saataisiin haltuun tietoa ajoneuvon (ja sen kuljettajan) sijainnista eri aikoina ja sillä suoritetuista matkoista.

Todennäköisyys: kohtalainen

Riski K3. Tiedon puuttuminen

Satelliittivastaanottimen toimintahäiriöstä, tietoisesta häirinnästä tai muusta laiteteknisestä syystä tieto ei tallennu ajoneuvolaitteeseen. Riippuen viranomaisten riskienhallinnasta tästä voi seurata käyttäjälle rangaistuksenomaisia veroseuraamuksia tai ajoneuvolaitteen tarkistustoimenpiteitä.

Todennäköisyys: kohtalainen

Riski K4. Palvelunesto

Hyökkääjä voi pyrkiä vaikuttamaan – tai käyttäjä tietämättömyyttään vaikuttaa – laitteen toimintaan siten, että laite ei toimi oikein, kaatuu tai tiedonsiirto epäonnistuu. Tämä voi johtaa ongelmiin veron määräytymisessä. Jos käyttäjä hyödyntää laitetta esimerkiksi myös navigointiin, palvelun käyttö estyy.

Todennäköisyys: kohtalainen

Riski K5. Identiteetin paljastuminen

Hyökkääjä voi saada selville käyttäjän identiteetin ilman, että käyttäjä on sallinut sitä. Toisaalta paikkatiedon keräävän laitteen identiteetti on verrattavissa moottoriajoneuvon rekisterikilpeen, jonka perusteella ajoneuvon omistaja/haltija on selvitettävissä.

Langattoman yhteyden käyttäminen laitteiden automaattiseen etsintään ja identiteettien luvattomaan selvittämiseen liikkuvista ohi ajavista ajoneuvoista saattaa olla jopa helpompaa kuin vastaava tunnistus rekisterikilpien perusteella. Kommunikaatio voidaan kuitenkin salata.

Laitteella on jokin staattinen identiteetti lähes tekniikasta riippumatta. Tällainen identiteetti on esimerkiksi radiorajapinnan MAC-osoite tai vastaava tunniste. Mikäli laite kommunikoi tätä staattista identiteettiä käyttäen, se tarjoaa mahdollisuuksia seurata käyttäjiä. Käyttäjän henkilöllisyys ei välttämättä ole tunnistettavissa suoraan, mutta hyökkääjä saattaa saada tietoja pysähtymisistä tiettyihin osoitteisiin.

Tulevissa liikenteen yhteistoiminnallisissa palveluissa (cooperative services, C-ITS) on kaavailtu käytettävän tilapäisiä identiteettejä ja mekanismeja niiden vaihtumiseksi. Staattinen identiteetti piilotettaisiin muilta ajoneuvoilta, joiden kanssa kommunikoidaan. Todellinen identiteetti olisi tiedossa vain tietyissä taustajärjestelmissä. Tällainen menettely vaikeuttaa käyttäjien seuraamista mutta asettaa toisaalta lisävaatimuksia taustajärjestelmille.

Todennäköisyys: suuri

Riski K6. Reittien ym. asioinnin paljastuminen

Käyttäjän reittivalinta, matka-ajankohta ja suunta paljastuvat ulkopuolisille. Ulkopuolinen voi tässä tapauksessa olla aktiivisen hyökkääjän ohella myös viranomainen, joka ei tarvitse kaikkea tätä tietoa. Tämän tiedon kertyminen mahdollistaa matkojen tarkoituksen tunnistamisen, työmatkat arkisin eri suuntiin, mökkimatkat kesäviikonloppuisin ym.

Todennäköisyys: kohtalainen

Riski K7. Haittaohjelmat

Vaikka varsinaisia, laitteelle räätälöityjä haittaohjelmia ei välttämättä ilmaantuisikaan, voi jokin alun perin muuhun samankaltaisella laitealustalla toimivaan ympäristöön tarkoitettu haittaohjelma löytää tiensä myös paikkatietoa tallentavaan yksikköön.

Todennäköisyys: pieni

Riski K8. Virheellinen tai haitallinen varusohjelmiston päivitys

Mikäli ajoneuvolaitteen ohjelmisto on mahdollista päivittää, siihen saatetaan ladata ohjelmisto, joka esimerkiksi kerää ja lähettää tietoja eri tavalla kuin on alun perin tarkoitettu. Kokonaan uusi ohjelmisto mahdollistaisi sekä käyttäjän laittoman seuraamisen että käyttäjälle aiheutuvaa kiusaa siitä, että verotukseen käytettävä järjestelmä ei toimi asianmukaisesti. Haitallisen päivityksen tehnyttä tahoa voi olla vaikea näyttää toteen.

Todennäköisyys: pieni

4. Suositukset ja toimenpiteet tietoturvan kannalta

4.1 Palvelun tietoturvan suositukset

Tietosuojalainsäädännön uudistus (EU:n tietosuoja-asetus) tuo mukanaan nykyistä selkeämpiä sääntöjä henkilötietojen käsittelystä. Loppukäyttäjän asema ja valta itseään koskeviin tietoihin lisääntyy, mutta uudistuksen voi nähdä myös kasvavana vastuuna omien tietojen käytön valvonnasta. Toisaalta palveluntarjoajan asema selkiytyy.

Raportissa tarkasteltujen tietoturvariskien perusteella voidaan tehdä joitakin suosituksia yleensä ja eri näkökulmista. Yksityisyyden suoja on otettava huomioon jo järjestelmää suunniteltaessa (Privacy by Design) ekosysteemin eri toimijoiden näkökulmista. Seuraavien suositusten perään on merkittynä riski tai riskit (ks. luku 3), joiden hallintaan suositus erityisesti liittyy.

Liikennetietojen tuoreuden takaamiseksi tietoja on kerättävä säännöllisesti. Tällöin ei ole kuitenkaan tarpeen siirtää kaikkea laitteeseen kerättyä dataa, vaan liikenteenohjauksen kannalta välttämättömät tiedot. Samassa yhteydessä voidaan laitteesta siirtää tallennetusta tiedosta laskettu tarkiste, joka säilytetään myöhempää tarvetta varten. Jos siihen asti tallennettua tietoa myöhemmin muutetaan, laitteesta sitä ennen saadut tarkisteet eivät enää täsmää. **V3**, **V5**

Vähäisempi tietojen manipulointi voidaan hoitaa lainsäädännöllisesti asettamalla sanktiot tilanteisiin, joissa ilmenee tietojen sormeilu jälkikäteen. **V3, P4**

Käyttäjän paikkatieto ja identiteetti voidaan useimmiten eriyttää ja säilyttää eri paikoissa. Kaupallisen palvelun tuottaja ei todennäköisesti tarvitse kaikkea saatavilla olevaa tietoa, ja toisaalta viranomaisella ei ole tarvetta seurata yksityisten henkilöiden palveluiden käyttöä. Liikennemäärien keräämiseen tai muihin liikennesuunnittelun pohjana oleviin tietovarantoihin ei ole tarpeen kerätä käyttäjät yksilöivää tietoa. **K5**, **K6, P5**

Laitteeseen verotusta varten kerättävät tiedot voidaan salata esimerkiksi laitekohtaisella symmetrisellä avaimella, joka on vaihdettavissa esimerkiksi katsastuksen yhteydessä. Laitteesta langattomasti luettavissa oleva tallennettu tieto ei tällöin ole hyödynnettävissä sellaisenaan. **K1**

Osa lisäpalveluiden tarvitsemasta paikkatiedosta tai paikkatietoon liittyvistä muista tiedoista voidaan säilyttää käyttäjällä itsellään (maksimaalinen tiedon hallinta) ja tarvittaessa käyttäjän suostumuksella tietoja voidaan luovuttaa palveluntarjoajalle. **K2**

Itse laitteeseen tallennettua kattavaa paikkatietoa ajankohtineen ja reittitietoineen voidaan tarvittaessa hyödyntää myöhemmin laitteen toiminnan auditointiin ja tietosisällön verifiointiin. Näin voidaan havaita väärinkäytökset tehokkaasti ja siten myös ehkäistä niitä syntymästä. **V1**, **V2**, **V3**

Kun viranomainen lukee tietoja, lukija täytyy tunnistaa ennen tiedonsiirron aloittamista tai vaihtoehtoisesti kerättyjen tietojen on oltava salattuja ja vain viranomaisen avattavissa. Jälkimmäisessäkin tapauksessa lukijan tunnistus voi olla tarkoituksenmukaista, jotta laitetta suojataan hyökkäyksiltä. Käyttäjän omaan käyttöön ja palveluntarjoajaa ajatellen laite voi kuitenkin sisältää erillisen rajapinnan identiteetin ilmaisuun ja osaan paikkatietoa. **K2**, **K4**, **K5**

4.2 Yleisiä suosituksia

Kuluttajan näkökulma:

- Omien tietojen hallinta – vastuu omien tietojen käsittelystä kasvaa, ja jokainen päätös sallia tietojen luovutus on punnittava tarkoin. Tärkeää on, että kuluttajat saavat riittävästi tietoja ja ohjeita omien tietojensa käsittelyn seurantaan.
- Yksityisten lisäpalvelujen osalta kuluttajalla on mahdollisuus valita, käyttääkö palvelua vai ei – viranomaispalveluiden tai -rekisterien osalta tällaista valinnanvapautta ei yleensä ole.
- Kuluttajalla on myös oikeus muuttaa mieltään ja kieltää tietojen käsittely sekä pyytää poistamaan tiedot, joiden säilyttämiseen ei ole lakiin perustuvaa velvollisuutta.

Viranomaisnäkökulma:

- Viranomaisrekisterit
  - Kuluttaja ei yleensä voi vaikuttaa rekisteröintiin.
  - Tietojen luovutus on säänneltyä, ja rekisteröity voi kieltää sen.
- Julkisen toiminnan (esimerkiksi liikennesuunnittelu) tarvitsemat liikennetiedot anonymisoidaan.
- Palveluiden käyttämiseksi tarvittavaa tietoa ei luovuteta suoraan palveluntarjoajalle, vaan se kierrätetään kuluttajan kautta.
- Rekisteröityä käyttäjää informoidaan tietojen keräämisestä, käsittelystä ja säilytyksestä sekä tietojen tuhoamisesta.

Yrityksille/palveluntarjoajille:

- Kuluttajalta on aina saatava suostumus tietojen käsittelyyn tai luovutukseen edelleen.
- Ajoneuvolla voi olla useita käyttäjiä. Lisäpalveluihin rekisteröitymisen tulisi edellyttää salasanaa.
- Vain palvelun kannalta tarpeellista tietoa kerätään:
    - ensisijaisesti käyttäjältä itseltään
    - käyttäjän suostumuksella muista lähteistä
    - palvelun kannalta tarpeettomaksi muuttunut tieto hävitetään.
- Tietoja ei luovuteta edelleen ilman käyttäjän suostumusta eikä tietoja käytetä muuhun tarkoitukseen kuin johon ne on alun perin kerätty ja johon on saatu suostumus.
- Käyttäjää informoidaan tietojen keräämisestä, käsittelystä ja säilytyksestä sekä tietojen tuhoamisesta.

Tietoturvauhkien hallintaan ja palveluiden kehittämiseen on palveluntarjoajien käytettävissä myös aiemmin tuotettu ohjeisto (LVM 2005).

Koska palveluiden käytettävissä olevaa järjestelmää ei ole määritelty saati toteutettu, ei eri osapuolten käytettävissä olevia menetelmiä ole tiedossa. Kuluttajan kannalta olisi tärkeää, että järjestelmä tarjoaisi anonymiteetin paikkatiedon hyödyntämiseen palveluissa. Yksi tällainen menetelmä on esitetty MobiSys ’03 tapahtumassa (ACM 2003).

5. Satelliittipaikannuksen häirintämenetelmät

5.1 Signaalin vastaanoton häirintä

Kuluttajamarkkinoilla olevia GPS-vastaanottimia on teknisesti yksinkertaista häirittä: Koska satelliittien lähettämä signaali on maahan saavuttuaan jo hyvin heikko, sen vaimentamiseen riittää sopivalla taajuuskaistalla lähetetty, tietyt signaaliominaisuudet omaava ja riittävän voimakas signaali. Häirintää voi tapahtua myös tahattomasti, rikkoontuneiden laitteiden lähettäessä RF-taajuista signaalia. Esimerkiksi aktiivinen GP-antenni voisi rikkoonnuttuaan muuttua lähettimeksi.

Suomessa häirintälaitteiden tekniikkaa on tutkittu Geodeettisessä instituutissa (Ruotsalainen ym. 2014). Maanpuolustuksen tieteellisen neuvottelukunnan MATINEn rahoittamassa DETERJAM-projektissa (2012–2014) tutkittiin häirinnän vaikutuksia markkinoilla oleviin GPS-vastaanottimiin. Lisäksi tutkittiin häirinnän havaitsemista ja vaikutusten minimointia.

Häirintälaitteita myydään nettikaupoissa edullisimmillaan noin 15 euron hintaan. Kuva 2 esittää markkinoiden edistyneimmäksi mainostettua häirintälaitetta, jonka hinta on 170 puntaa (218 euroa). Sen lähetysteho on 0,5 W kanavaa kohti, ja se kykenee häiritsemään kaikkia GPS-taajuuksia. Lisäksi se häiritsee Galileo, Compass, WAAS, EGNOS, QZSS ja GAGAN -järjestelmien signaaleita. Venäläisen Glonass-järjestelmän taajuuksista se pystyy häiritsemään vain osaa. Laite häiritsee myös matkapuhelinverkkoja. Kantamaksi on mainittu 15 m, mutta testeissä laitteen on havaittu aiheuttavan häiriötä jopa muutaman mailin etäisyydellä. (Curry 2014.)

Kuva 2. Markkinoiden edistyneimmäksi väitetty GPS-häirintälaite.

Häirintäsignaali voidaan paljastaa käyttämällä vastaanotinta, joka on viritetty GPS-taajuudelle. Laite mittaa taajuusalueen signaalien tehoa. Koska GPS-signaali on luontaisesti heikko ja häirintä tehdään lähettämällä sitä huomattavasti voimakkaampaa signaalia, äkillinen tehon kasvu paljastaa häirintälaitteen. Toinen menetelmä on mitata kunkin satelliitin signaali-kohinasuhdetta. Sen putoaminen asetettua rajaa alemmaksi pidemmäksi aikaa paljastaa häirinnän. Jälkimmäinen voidaan toteuttaa ilman erikoislaitteita.

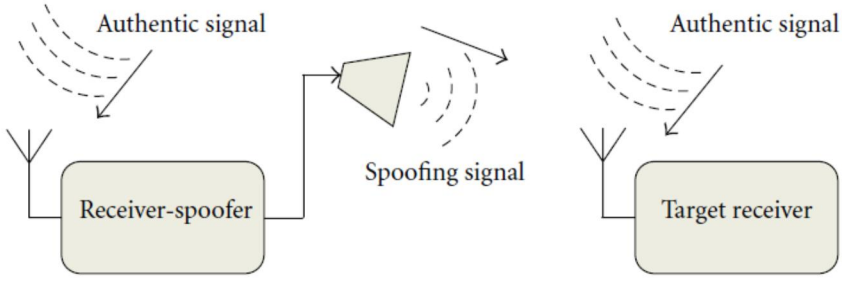
Kuva 3. Signaali-kohinasuhteen putoaminen ja signaalien energian nousu häirinnän aikana (Curry 2014).

Häirinnän havaitsemiseen ja laitteiden paikantamiseen on kehitetty laitteita. Kuva 4 esittää Chronos Technology Ltd:n kehittämää kannettavaa laitetta. Vastaanotin on hyvin kapeakeilainen, joten häiriösignaalin suunta on mitattavissa ja laitteen sijainti löydettävissä.

Kuva 4. Kannettava häirintälaitteiden paikannin (Chronos 2013).

5.2 Signaalin väärentäminen

GPS-signaalin väärentäminen (spoofing) toteutetaan lähettämällä joko väärennettyjä signaaleja, jotka muistuttavat oikeita, tai lähettämällä uudelleen jossain muualla tai eri aikaan tallennettua oikeaa signaalia. Näin saadaan paikannustulos, joka osoittaa paikkaan, jossa ei oikeasti olla, tai paikka on oikein mutta aika väärä. Tyypillisesti hyökkäyksessä synkronoidutaan oikean signaalin kanssa ja nostetaan väärennetyn signaalin lähetysvoimakkuutta asteittain. Oikeista väärennyshyökkäyksistä ei ole saatavilla paljon tietoja, mutta tekniikoita on kokeiltu proof-of-concept-tyyppisissä testeissä (Humpreys , 2008). Väärentämistä on hyvin vaikeaa havaita vastaanottimessa, joten periaatteessa se muodostaa suuremman uhan kuin häirintä.



Kuva 5. GPS-signaalin väärentämisen periaate (Jafarnia-Jahromi 2012).

Ainoa julkinen tapaus, jossa väärentämisen käyttöä on epäilty, tapahtui vuonna 2011. Tällöin Iran kaappasi amerikkalaisen miehittämättömän lennokin Lockheed RQ-170:n (Kuva 6). Iranin antaman tapauskuvauksen perusteella lennokin kommunikointiyhteydet oli ensi häiritty toimimattomaksi ja sen jälkeen GPS-sijainti oli

väärennetty, jolla keinoin lennokki olisi saatu laskeutumaan Afganistanin sijasta Iranin puolelle. Amerikkalaisten selitys oli, että laite olisi ainoastaan rikkoontunut ja tehnyt pakkolaskun Iranin puolelle.

Kuva 6. Iranilaisten kaappaama miehittämätön lennokki Teheranissa (Bora 2012).

5.3 Aikasynkronoinnin estäminen

Satelliittipaikannuksessa sijainnin mittaus on itse asiassa aikaerojen mittaamista. Jokainen paikannussatelliitti sisältää peräti neljä atomikelloa. Lisäksi koko satelliittijärjestelmän kellot synkronoidaan maa-aseman kanssa. Ilman synkronointia satelliitin kelloon tulisi noin kymmenen nanosekunnin virhe päivässä. Ajassa se ei ole paljon, mutta valonnopeudella syntyvä etäisyysvirhe olisi kolme metriä (Parker 2015). Näin ollen etäisyysvirhe kasvaisi joka päivä aina kolmella metrillä. Vastaanottimessa on myös kello, jonka virhe pitää ratkaista tarkan paikannustuloksen saavuttamiseksi. Sen vuoksi 3D-paikan laskentaan tarvitaan vähintään neljä satelliittia, vaikka sijainnin laskennassa tuntemattomia suureita on vain kolme (x, y, z). Kellovirhe on se neljäs tuntematon suure.

Internetissä käytetään aikasynkronointiin yleisesti NTP (Network Time Protocol) -protokollaa. Se on suunniteltu ottamaan huomioon verkon muuttuvat viiveet. NTP-palvelimet toimivat hierarkkisesti siten, että yksi tai useampi 1-tason (stratum) palvelin saa aikansa suoraan ulkoisesta aikalähteestä (stratum 0). Stratum-taso ei siis kerro palvelimen kellon tarkkuudesta, vaan palvelimen sijainnista verkkohierarkiassa. Stratum-tasot ovat hierarkkisia. 2-tason palvelimet hakevat aikansa vähintään yhdeltä 1-tason palvelimelta. Stratum 3-tason kellot hakevat aikansa 2-tason palvelimilta jne. Tasoja voi olla 16. Tavallisesti loppukäyttäjät hakevat ajan

stratum 2 -tason palvelimilta. Asiakas voi käyttää joko yhtä tai useampaa palvelinta. Kolme NTP-palvelinta on vähimmäismäärä, jotta asiakas voi päätellä, mikä kelloista on väärässä. NTP-protokollalla saavutettava tarkkuus on korkeintaan hieman alle 100 ms hyvässä verkossa. (NTP 2016.)

Uudempi ja NTP:tä tarkempi aikasynkronointiprotokolla verkossa on IEEE 1588 PTP (Precision Time Protocol). Siinä verkossa olevat kellot synkronoidaan verkon parhaan kellon mukaan (PTP). Tiedonsiirtoverkon tulee tukea multicast-protokollaa. Aikareferenssinä voidaan käyttää GPS-pohjaista ratkaisua (PTP 2016).

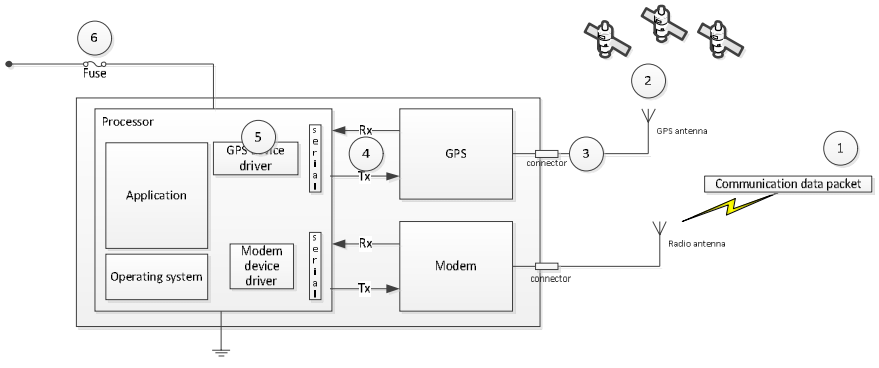
GPS-vastaanotinta voi käyttää myös aikasynkronointiin. Se voi toimia stratum 0 -tason referenssikellona. Vastaanotin generoi PPS (pulse per second) -signaalia, jolla saadaan hyvin tarkka aikareferenssi tietokoneelle. Aikareferenssin tarkkuus on +/- 100 ns. GPS onkin halpa tapa saada aikaan erittäin tarkka aikasynkronointi. Tämä johtaa houkutukseen käyttää pelkästään GPS-vastaanottimia toimintojen synkronointiin.

Häirittäessä paikannusta häiritään luonnollisesti myös aikasynkronointia. Toisin kuin paikannuksessa, jossa häiritty GPS-laite ei enää voi laskea uutta arviota paikasta, aikavirhe kertyy hitaammin. Aikareferenssin hävittyä järjestelmän kellot alkavat erkaantua toisistaan kellojen laadun määräämässä tahdissa. Toimintahäiriöiden ilmaantumisen aikajänne riippuu sitten toiminnan vaatimasta synkronointitarkkuudesta.

6. Ajoneuvolaitteen manipulointi

6.1 Ajoneuvolaitteen manipulointitavat

Ajoneuvolaitetta voi manipuloida monella eri tavalla. Kuva 7 esittää tyypillisen ajoneuvolaitteen lohkokaaviota. Laiteen pääosat ovat prosessoriyksikkö, satelliittipaikannuksen piirisarja ja tietoliikennemodeemi. Laitteessa voi olla myös (kosketus)näyttö ja näppäimistö sekä massamuisti.



Kuva 7. Tyypillinen ajoneuvolaite. Numerointi viittaa luetteloon alla.

1. Laitteen väärentäminen

Laite pitää jatkuvasti yhteyttä palvelimeen, jonne välitetään vähintään viestin aikaleima, laitteen tunnistekoodi sekä sijaintitieto. Jos käytetty tiedonsiirtoprotokolla on tiedossa, väärennettyjen viestien lähettäminen on mahdollista hyvin yksinkertaisella laitteistolla. Muita tarvittavia tietoja ovat palvelimen IP-osoite ja portti. SIM-kortti voidaan siirtää väärennettyyn laitteeseen.

Suojautumiskeinona on salattu tietoliikenne, joka vaatii prosessointikapasiteetin kasvattamista ja salausavaimien hallintaa järjestelmätasolla. SIM-kortti on mahdollista sulauttaa rautatasolle, jolloin sen siirtäminen toiseen laitteeseen ei ole mahdollista.

2. Satelliittisignaalien väärentäminen ja estäminen

Satelliittisignaalien estäminen ulkoisella laitteella (jamming, ks. 5.1). Ajoneuvoon asennetaan häirintälaite, jonka lähettämä aktiivinen signaali estää vastaanotinta kuulemasta aitoja satelliitteja.

On mahdollista lähettää radiolla GPS-vastaanottimelle väärennettyjä satelliittien viestejä (spoofing, ks. 5.2) ja estää muiden signaalien kuuluminen. Tavoitteena on uskotella laitteelle, että ajoneuvo on jossain muualla kuin se todellisuudessa on. Vaikka tämä on teknisesti mahdollista, se on monimutkaisuutensa vuoksi epätodennäköinen tapa manipulointiin.

Häirinnän havainnointia on jo käsitelty luvussa 5.1. Häirintälaitteet voidaan havaita tarkoitukseen tehdyllä mittalaitteella. Paikannuksen puuttuminen voidaan havaita ulkoisella valvonnalla. Häirintälaitteiden kantama on kuitenkin useita satoja metrejä, ja kaikki kantoalueen sisällä olevat ajoneuvot ovat ilman paikannustietoa. On otettava myös huomioon, ettei häirintälaite ole välttämättä ajoneuvossa, vaan jossain lähistöllä.

3. GPS-antennin vaimennus

Signaalin vaimennus esimerkiksi peittämällä antenni sähköä johtavalla materiaalilla tai vaihtoehtoisesti antennikaapelin irrotus johtaa tilanteeseen, jossa paikannusta ei saada. Laite on edelleen kykenevä tietoliikenteeseen, jos yhteys palvelimelle säilyy. Tilannetta ei voida suoraan tulkita manipulointiyritykseksi, koska on tilanteita, jossa paikannusta ei saada normaalistikaan. Maanalaiset pysäköintiluolat ovat tästä hyvä esimerkki. Myös sääolot ja satelliittien huono sijainti voivat aiheuttaa tilanteen, jossa paikannusta ei saada.

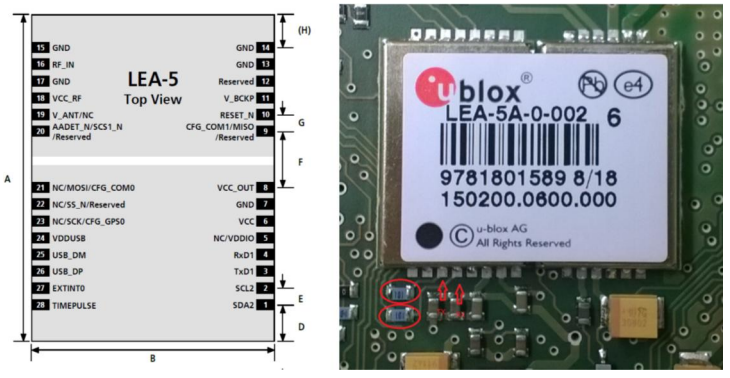
Manipuloinnin todentaminen pitää tehdä ulkopuolisella valvonnalla (esim. automaattisella kameravalvonnalla). Sijaintien, joissa satelliittivastaanotto ei toimi, kartoittaminen on käytännössä mahdotonta. Pelkät parkkiluolat eivät riitä, koska suurin osa autotalleista ja muista sisätiloista aiheuttaa saman ilmiön.

Mikäli laitteessa on esimerkiksi kiihtyvyysanturi, se voi arvioida liikkumisen määrää ja kestoa sinä aikana, kun GPS-paikannus ei onnistu. Näiden tietojen perusteella voi havaita vähintäänkin järjestelmävirheitä.

4. GPS-piirin vaihtaminen

GPS-piirit käyttävät sarjamuotoista liikennöintiä prosessoripiirien kanssa. Liikennöintiyhteys voidaan katkaista ja vaihtaa GPS-piirin tilalle sen toimintaa emuloiva piirikortti. GPS-piirisarjoja valmistaa vain muutama yritys (esim. Sirf, uBlox), joten emulointikortin tekeminen on hyvinkin mahdollista. Kuva 8 esittää esimerkin, jossa ajoneuvolaite on purettu ja sen GPS-piiri (uBlox LEA-5A) paikallistettu piirikortilta. Kyseisen piirin datalehdestä (uBlox 2016) selviää helposti piirin pinnijärjestys. Sarjaportin lähetys- ja vastaanottosignaalit TXD1 ja RXD1 ovat pinneissä 3 ja 4. Kyseisiin pinneihin tulevissa johdotuksissa on sarjavastukset (ympyröity), jotka on helppo juottaa irti ja liittää emuloivan laitteen sarjaportin johdot niiden tilalle. GPS-

piiriin liittyy myös USB-portti (pinnit 24, 25 ja 26), joka on selvästi johdotettu piirikortille. Vaihtoehtoisesti laite voi käyttää kommunikointiin USB-väylää.



Kuva 8. Erään ajoneuvolaitteen GPS-piiristä on paikallistettu sarjaportin pinnit TxD1 (2) ja RxD2 (3). Yhteys GPS-piiriin voidaan katkaista irrottamalla ympyröidyt vastukset ja juottamalla niiden tilalle johdot. Johtoihin voidaan kytkeä GPS-piiriä emuloivan laitteen sarjaportti.

Kommunikointiprotokollat ovat julkisia joko NMEA-standardin mukaisia tai valmistajakohtaisia binaariprotokollia. Emulointikortti voitaisiin ohjelmoida lähettämään sijaintia ajoneuvolaitteelle valittua protokollaa käyttäen.

Suojautumiskeinona on käytännössä piirikortin valaminen epoksimuoviin. Ajoneuvolaitetta ei sen jälkeen voisi enää korjata.

5. Laitteen ohjelmiston muuttaminen

Myös itse päätelaitteen ohjelmointi voidaan muuttaa lataamalla siihen muunnettu ohjelmisto. Ohjelmoitavan laitteen ohjelmakoodi on luettavissa laitteelta, ja osaava ohjelmoija pystyy tekemään siihen muutoksia ilman lähdekoodiakin. Etenkin jos kyseessä on avoin monipalvelualusta, ohjelmiston täydellinen suojaaminen on mahdotonta. Ohjelmistoa voidaan muuttaa sitä esimerkiksi niin, että paikkaa ei enää lueta GPS-piiriltä, vaan sen sijaan käytetään väärennettyä sijaintia.

6. Laitteen poistaminen toiminnasta

Vaikka päätelaite olisi hyvin vähän tehoa vaativa, sen asentaminen ajoneuvoon vaatii virransyötön suojaamisen sulakkeella sekä virrankatkaisun tai valmiustilaan siirtymisen, kun ajoneuvo sammutetaan. Jatkuvatoimisena pienikin tehonkulutus tyhjentää ajoneuvon akun, mikäli ajoneuvolla ei ole säännöllistä ja pitkäkestoista ajoa. Suomessa talvisaikaan näin käy helposti etenkin, kun akun kunto alkaa ikääntyessään heiketä.

Laitteen saa toimimattomaksi periaatteessa helposti, kun poistaa laitteesta sulakkeen. Matkamittarin lukema voitaisiin samassa yhteydessä laittaa talteen ja

palauttaa lukema ennalleen esimerkiksi ennen katsastusta. Näin autolla ajetut kilometrit saadaan vastaamaan seurantajärjestelmän rekisteröimiä lukemia.

Lyhyitä virtakatkoksia varten ajoneuvolaitteessa tulisi mahdollisesti olla paristovarmennus ja toiminto, jossa virransyötön katkoksista ja liikeanturien lukematiedoista kommunikoidaan palvelimelle poikkeamien seuraamiseksi.

Sammunut laite ei itse havaitse tilaansa, joten toiminnasta poistettujen laitteiden havaitseminen liikennevirrasta on järjestettävä muulla tavoin. Todentaminen voidaan toteuttaa esimerkiksi kuvaamalla ajoneuvo ja rekisterikilven tunnistuksen jälkeen verrata seurantajärjestelmästä saatua sijaintitietoa havaintopaikan sijaintiin. Menetelmä edellyttää valvontaporttien rakentamista ja esimerkiksi poliisin ajoneuvojen varustamista tarkistuslaitteistolla. Rekisterikilpi saatetaan myös tuhria automaattisen tunnistamisen hankaloittamiseksi.

Koska tapoja saattaa ajoneuvolaite toimimattomaksi on useita, edellä mainittu havainnointitapa on sekin hieman ongelmallinen. Toimimattoman laitteen todentaminen on sinänsä periaatteeltaan yksinkertaista. Mutta esimerkiksi jos joku käyttää häirintälaitetta, on suuri joukko muitakin ajoneuvoja ilman paikannustietoa. Valvonnallakaan ei yksikäsitteisesti voida osoittaa, mikä ajoneuvo on tahallisesti manipuloitu ja mikä on lähistöllä olevan häirintälaitteen vaikutusalueella.

6.2 Ajoneuvolaitteen sertifiointi

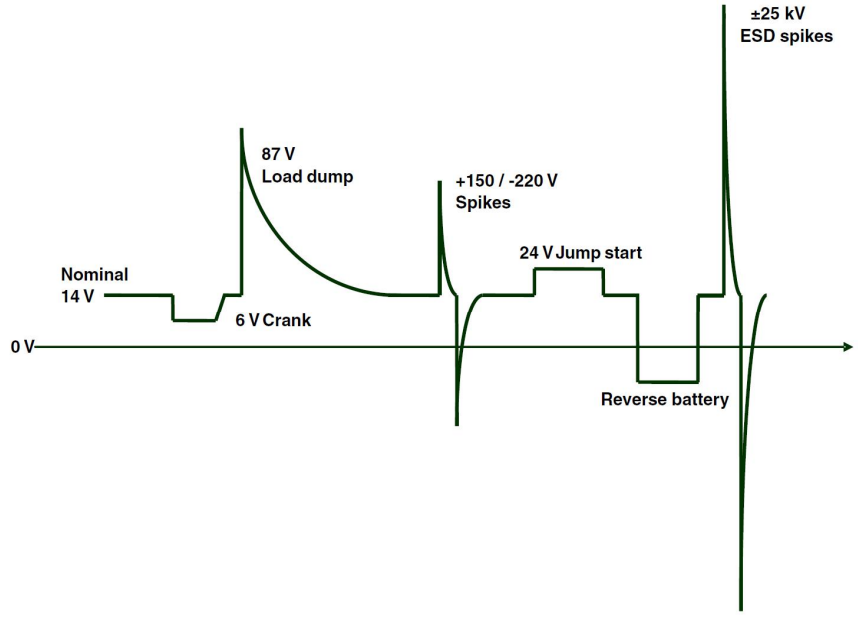
Kilometriveron keruujärjestelmään liitettävä ajoneuvolaite pitää sertifioida etenkin, jos järjestelmä on avoin eri valmistajien ajoneuvolaitteille. Sertifioinnissa pitää lähinnä ottaa huomioon kolme asiaa:

1. elektroniikan tulee kestää ajoneuvo-olosuhteissa
2. kommunikointi taustajärjestelmän kanssa tapahtuu määrittelyn mukaisesti
3. tuotettu matkan mittauksen lopputulos on annetuissa toleransseissa.

Ajoneuvo toimintaympäristönä on varsin vaativa. Ei kuitenkaan ole olemassa mitään yhtä standardia, jonka mukaisesti ajoneuvolaite pitäisi toteuttaa. Eri autovalmistajilla on omia spesifikaatioitaan, joita auton omiin järjestelmiin liitettävien komponenttien pitäisi täyttää. Lisälaitteen, joka ottaa autosta vain käyttösähköt, ei välttämättä tarvitse täyttää näitä ympäristövaatimuksia. Laitteen toimivuuden ja kestävyyden kannalta on kuitenkin enemmän kuin suotavaa, että suunnittelussa ja toteutuksessa noudatetaan spesifikaatioiden linjoja.

Käyttölämpötilojen osalta autoteollisuuden vaatimukset ovat yleisesti -40...+85 ºC ja moottoritilassa -40...+125 ºC. Käyttösähkön laatu on myös varsin huono, jännitealue on laaja 9–36 V ja jännitteessä voi olla yli 100 V piikkejä (ks. Kuva 9). Jännitteen napaisuus voi myös vaihtua. Häiriöitä on standardoitu muun muassa ISO 10605, IEC 61000-4-2, ISO 7637 ja SAE J1113-11 -standardeissa. Näistä ISO 10605 ja ISO 7637 ovat tärkeimmät. Suunnittelussa pitää ottaa huomioon tärinä, kosteus ja pöly, jotka aiheuttavat vaatimuksia koteloinnille ja piirilevyn suojaukselle. Ajoneuvokäytössä myös laitteen virrankulutuksella on merkitystä. Lait-

teen ottaman lepovirran tulisi olla mahdollisimman pieni, jotta se ei pura auton akkua. Lyijyakulla normaali itsepurkautumisvirta on luokkaa 50–100 mA. Laitteen lepovirran tulisi olla alle sen, jotta vältyttäisiin akun tyhjentymiseltä, jos autolla ei ajeta päivittäin.



Kuva 9. Ajoneuvon sähköjärjestelmässä esiintyviä häiriöitä (ST 2015).

Tietoliikenteen testaus edellyttää palvelusta rajapintakuvausta, jossa kuvataan välitettävät viestit ja viestiprotokolla. Laitteen tiedonsiirto testataan jokaista käyttötapausta vastaavalla testillä. Jos laite läpäisee hyväksyttävästi kaikki testit, saadaan varmistus siitä, että laitteen toiminta vastaa kaikilta osin vaadittua. Vasta sen jälkeen laite voidaan hyväksyä liitettäväksi osaksi järjestelmää.

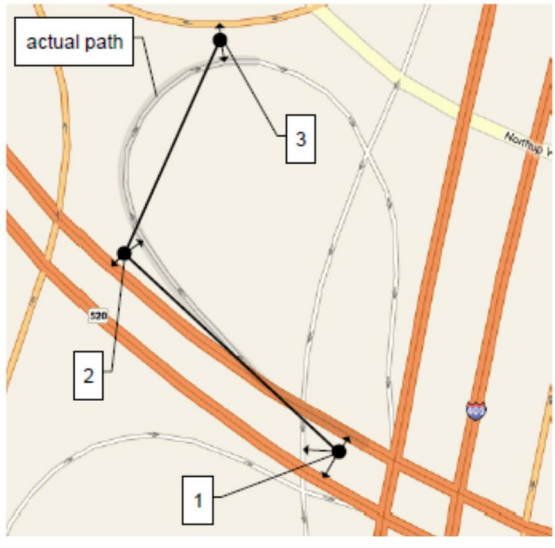
Laitteen matkanmittauksen oikeellisuudesta on hieman vaikeampi saada varmuus: kuljetun matkan laskennan tulos eri tariffialueilla on riippuvainen sekä paikannuksesta että karttamateriaalista. Jos karttatietoihin liittyvä laskenta tehdään taustajärjestelmässä, tariffialueiden rajoja tai tiekarttaa ei tarvitse päivittää ajoneuvolaitteeseen. Tällöin ajoneuvolaitteen tehtäväksi jäisi lähinnä koordinaattien (tarvittaessa myös niiden välillä liikutun tarkan matkan) välittäminen taustajärjestelmään. Karttamateriaalin päivitys ajoneuvolaitteeseen voisi aiheuttaa teknisiä haasteita riippuen esimerkiksi tarvittavan tiedon määrästä. Taustajärjestelmässä päivitysten hallinta on huomattavasti helpompi toteuttaa.

Toisaalta mikäli tariffi tulee voida määrittää yksittäisen tien tarkkuudella, ajoneuvolaitteen harvakseltaan (esim. kerran minuutissa) lähettämät koordinaattitiedot eivät riittäisi. Tietojen tiheä lähetys (esim. paikka 1–5 sekunnin välein) kasvat-

taisi huomattavasti tiedonsiirron sekä taustajärjestelmän laskentakapasiteetin vaatimuksia. Laskennan painotus ajoneuvolaitteen ja taustajärjestelmän välillä riippuu toisin sanoen kilometriverojärjestelmälle asetettavista tarkkuusvaatimuksista.

Ajoneuvon kulkemaa matkaa voidaan mitata summaamalla paikannustuloksien erotuksia yhteen. Syntynyt tulos ei kuitenkaan ole tarkka, koska ensinnäkin paikannusvirhettä kumuloituu kuljettuun matkaan (syntyy kuvitteellista sivuttaisliikettä) ja toisekseen mahdollinen harvaan (esim. kerran viidessä sekunnissa tai harvemmin) suoritettava koordinaattien määritys oikoo mutkia. Mikäli ajoneuvolaite arvioi kuljettua matkaa itse, sijaintivirheen vaikutus kuljetun matkan laskentaan on pieni. Mikäli arvio tehdään taustajärjestelmään tallennetuista harvoista koordinaattipisteistä, alkaa syntyä eroa ajoneuvon matkamittarin lukemaan verrattuna. Laitteen ollessa paikallaan paikannuksen epätarkkuus voi myös aiheuttaa laskentavirheen, jonka mukaan ajoneuvo liikkuisi. Tämä kuvitteellinen liikkuminen osataan kuitenkin suodattaa pois laskennassa.

Karttasovitus eli ajoneuvon koordinaattien sijoittaminen tiekartalle ei sekään ole teknisesti yksinkertaista. Osa karttasovitukseen käytettävistä algoritmeista toimii reaaliaikaisesti (käytössä autonavigaattoreissa), osaa voidaan soveltaa vasta, kun kaikki data on kerätty (etuna parempi tarkkuus esimerkiksi käännyttäessä tieltä toiselle). Kuva 10 esittää yhtä ongelmatilannetta, kun paikannus saadaan harvakseltaan ja epätarkkana. Ajoneuvo on todellisuudessa kulkenut kuvan keskellä olevaa ramppia. Karttasovituksessa on vaikea päätellä, millä tiellä ajoneuvo on todellisuudessa ollut (pisteet 1, 2 ja 3).



Kuva 10. Karttasovituksessa mitattujen koordinaattien perusteella yritetään selvittää, millä tiellä ajoneuvo on todellisuudessa kulkenut. Kuvassa ajoneuvo on ajanut harmaalla merkittyä ramppia pitkin. Pisteissä 1, 2 ja 3 mahdollisuuksia on useampia. (Newson & Krumm 2009.)

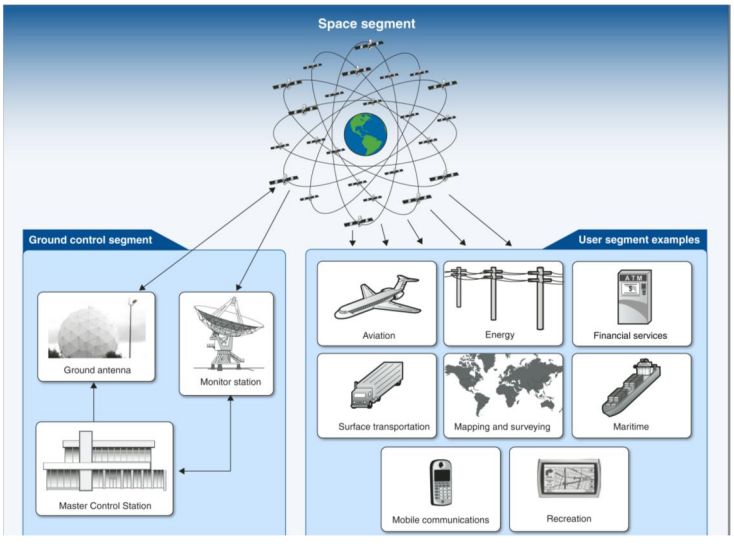
Periaatteessa matkanmittauksen testaus voitaisiin suorittaa ajamalla testilenkkejä ja vertaamalla saatua tulosta varmennettuihin tuloksiin. Tulosten ollessa asetetun toleranssin sisällä voitaisiin todeta, että laite on kelvollinen tehtäväänsä. Testilenkin tulisi sisältää kaikki paikannuksen ja karttojen osalta ongelmalliset tilanteet, esimerkiksi tunneleita, parkkiluolia ja kaupunkikanjoneita (tornitalojen aiheuttama häiriö satelliittipaikannukseen). Jos laskenta perustuu karttasovitukseen, myös sen kannalta ongelmallisia tilanteita eli esimerkiksi hyvin lähekkäin samaan suuntaan kulkevia katuja ja risteyksiä tulisi olla sisällytettynä testireitteihin.

Edellä kuvattu testimenettely sisältää pari ongelmaa: ensinnäkin tieverkolle tehtävät muutokset vaikuttaisivat testireitteihin, toisaalta satelliittipaikannuksen suorituskyky vaihtelee eri päivinä ja sääoloissa. Mahdollisesti testausta varten pitää ensiksi generoida oma karttatietokanta ja joko simuloida tai nauhoittaa satelliittien signaalit testireitiltä. Näin menetellen testit voitaisiin aina toistaa täsmälleen samanlaisina. Tulokset eri laitteiden välillä säilyisivät vertailukelpoisina. Mikäli laitteet kuitenkin käyttävät myös inertia-antureita tai ajoneuvolta saatavia tietoja matkan mittaukseen, testausta ei voi suorittaa ilman testireittiä.

Sertifioinnin pitää koskea myös asennusta. Ajoneuvolaitteen asentamiseen tarvitaan sertifioitu asennusliike, joka asennuksen jälkeen pystyy todentamaan laitteen toimintakunnon. Epäiltäessä laitteen toimivuutta myös huolto ja sen jälkeinen testaus täytyy pystyä järjestämään. Yksi kysymys on, pitäisikö laitteen toimintakunto pystyä tarkastamaan esimerkiksi katsastuksen yhteydessä.

7. Satelliittipaikannuksen häirinnälle kriittiset toiminnot

GPS:n käyttö on levinnyt voimakkaasti eri toimialoille, kuten Kuva 11 esittää. GPS-järjestelmästä ja sen käytöstä siviilisovelluksissa saa hyvän kuvan GPS.gov (http://www.gps.gov) -sivustolta, joka tarjoaa virallista tietoa GPS-järjestelmästä. Yhteiskunnan GPS-riippuvuudesta on herännyt huoli etenkin Yhdysvalloissa (GAO 2013, Coffed 2014,). Esimerkiksi puolustusjärjestelmien tutkimuksen ja kehittämisen organisaatio Defence Advanced Research Project Agency DARPA (http://www.darpa.mil) toimii aktiivisesti GPS-järjestelmän korvaamiseksi ja täydentämiseksi sotilassovelluksissa rahoittamalla esimerkiksi atomikellojen kehittämistä ajoitussovelluksiin (DARPA 2015) ja inertianavigointia (Yasin 2015). DARPAn tutkimusta motivoivat konfliktitilanteet, joiden aikana GPS:n häirintä on enemmän kuin todennäköistä.



Kuva 11. GPS-järjestelmä koostuu järjestelmää ohjaavasta maasegmentistä sekä avaruussegmentin satelliiteista. Paikannusta hyödyntävään käyttäjäsegmentiin kuuluu useita eri toimialoja. (GAO 2013.)

Sotilaskäytössä paikannuksen häirintävarmuutta voidaan parantaa inertianavigoinnin lisäksi esim. suuntaamalla lentolaitteiden GPS-antennit suoraan taivaalle. Kalliissa laitteissa ja rajatulla alueella voi olla käytössä lukuisia vaihtoehtoisia paikannustekniikoita.

Seuraavassa on lyhyt katsaus Suomen tilanteeseen eri toimialoilla.

7.1 Palo- ja pelastustoimi, poliisi

7.1.1 KEJO

Käynnissä on viranomaisten yhteiskäyttöisen kenttäjohtojärjestelmän (KEJO) hankinta. KEJOlla on tarkoitus korvata esimerkiksi pelastustoimessa käytössä oleva kenttäjärjestelmä PEKE ja poliisin kenttäjärjestelmä POKE sekä sairaanhoitopiirien kenttäjärjestelmät (HäKe 2013). Johtojärjestelmissä esitetään yksiköiden sijainti kartalla. Paikannuksen puuttuessa johtamisjärjestelmä ei toki mene toimintakyvyttömäksi, vaikkakin tilannekuva voi hieman hämärtyä. Yksiköiden sijaintihan voidaan kysyä puheyhteyden kautta. Häirintä aiheuttaa kyllä selkeästi harmia, mutta ei estä toimintaa.

7.1.2 Hätäpaikannus

Hätäkeskuksen käytössä hädänalaisen paikantamiseen on vanhempi matkapuhelinverkkoon perustuva paikannus ja älypuhelimen paikannusta hyväksikäyttävä Smart Locator -sovellus. Hätäpaikannus suoritetaan GSM-liittymänumeron perusteella ja paikkatieto saadaan liittymän kotiverkko-operaattorin paikannuspalvelimelta (HäKe 2016). Paikannuspyynnön avulla hätäkeskuspäivystäjä voi saada tiedon liittymän sijainnista alle kymmenessä sekunnissa. Useiden operaattoreiden järjestelmä antaa viimeisimmän solutiedon sammutetusta puhelimesta noin vuorokausi sulkemisen jälkeen.

Käytännössä paikannustarkkuus on kaupunkialueilla noin 50–400 metriä, esikaupunkialueilla noin 100–1000 metriä ja taajamien ulkopuolella sekä isoilla vesistöalueilla noin 1–5 kilometriä (harvaan asutuilla alueilla ja merialueilla mahdollisesti kymmeniäkin kilometrejä). Paikannuksen perustuessa matkapuhelinverkon antamiin tietoihin GPS-häirintä ei vaikuta siihen. On kuitenkin mahdollista, että häirintä aiheuttaa häiriöitä myös matkapuhelinverkkoon, joten ei ole täysin poissuljettua, että hätäpaikannukseen ei tulisi häiriöitä.

7.1.3 Smart Locator

Smart Locator on GPS-sijaintitietoon perustuva paikannuspalvelu. Paikantaminen toimii käytännössä niin, että hätäkeskuspäivystäjä kysyy hätäpuhelun soittajalta, onko hänellä käytössään älypuhelin, jossa on internetliittymä. Hätäkeskuspäivystäjä lähettää hätäpuhelun soittajan älypuhelimeen viestin, jossa on applikaation latauslinkki. Avaamalla linkin ja sallimalla sijaintitiedon lähettämisen hätäpuhelun

soittaja antaa paikkatietonsa hätäkeskuksen käyttöön. Palvelun perustuessa puhelimen GPS-paikannukseen sovellus ei toimi, jos soittaja sattuu olemaan häirityllä alueella. Matkapuhelinverkon solupaikannus toimii varajärjestelmänä.

7.1.4 eCall

Tulevaisuudessa ajoneuvojen automaattiset törmäyshälyttimet voivat hälyttää apua kolaripaikalle. eCall on ajoneuvoihin asennettava automaattinen törmäyshälytin, joka lähettää onnettomuudesta saatavat tiedot datapakettina (Minimum Set of Data, MSD) sopivimpaan hätäkeskukseen. eCall-hälytys voi aktivoitua esimerkiksi turvatyynyn laukeamisesta. Hälytys lähtee matkapuhelinverkkoa pitkin hätäkeskukseen. Hälytyksen mukana siirtyvä datapaketti sisältää satelliittinavigointijärjestelmän kautta saatavan ajoneuvon tarkan sijaintitiedon sekä tiedon ajoneuvon suunnasta, tyypistä ja matkustajien määrästä. Ajoneuvoihin asennetaan myös manuaalipainike, jolla eCall-hälytys voidaan tehdä esimerkiksi sairaskohtauksen vuoksi. eCall-palvelu perustuu sekin GPS-paikannukselle, joten paikannustietoa ei saada, jos ajoneuvossa tai sen läheisyydessä on häirintälaite. Puheyhteys toimii tässäkin tapauksessa, ja varajärjestelmänä voi toimia puhelimen solupaikannus.

7.2 Puolustusvoimat ja Rajavartiolaitos

Puolustusvoimat ja Rajavartiolaitos ovat varautuneet häirintään varajärjestelmillä eikä suuria ongelmia synny. Puolustusvoimilla on lennokkeja, ja rajavalvontaan niiden hankkimista harkitaan. Lennokit ovat etäohjattuja eivätkä lennä pelkästään GPS-tiedon varassa. Häirinnästä ei näin ollen pitäisi olla ylitsepääsemätöntä haittaa.

7.3 Viestintä

7.3.1 Viranomaisverkko VIRVE

Käyttäjän sijainti voidaan määritellä karkeasti tukiasemien perusteella ja tarkemmin lyhytsanomilla tapahtuvan GIS-paikannuksen avulla. Sijaintia voivat seurata esimerkiksi hätäkeskus tai muut kiinteiden päätelaitteiden, kuten DWS- ja VIRVE-käyttöpaikan, käyttäjät sekä esimerkiksi kenttäjohtamisjärjestelmien käyttäjät (pelastuslaitoksen yksiköt, johtokeskus ja valvomo). Päätelaitteiden antaman paikannustiedon tarkkuus on kymmenen metrin luokkaa. Päätelaitteen sisäisen GPS:n tuottamaa tietoa voidaan seurata reaaliaikaisesti (Vastamaa 2012). Häirintäalueella VIRVE-päätelaitteen paikannuskyky katoaa ja jäljelle jää vain karkea solupaikannus. Puheyhteys luonnollisesti säilyy.

7.3.2 Matkapuhelinverkot

Matkapuhelinverkot tarvitsevat toimiakseen tarkan aikasynkronoinnin, ja GPS on laajassa käytössä matkapuhelinverkoissa, koska se tarjoaa kustannustehokkaan

tavan ajoituksen toteutukseen (Symmetricon 2013). Verkkojen ajoitusta ei määräysten mukaan saa kuitenkaan perustaa ainoastaan GPS:n varaan. 3G (CDMA2000) -standardi määrittää tukiasemien synkronoinnin vaatimukseksi alle 10 µs GPS-ajasta (Humpreys, 2013).

Synkronointiin on tarjolla IEEE 1588 Precision Timing Protocol (PTP), jonka avulla kiinteässä Ethernet-verkossa olevien tukiasemien ajoitus voidaan hoitaa verkon kautta (Nuss 2013). Epäselvää on, kuinka laajasti IEEE 1588 on käytössä kotimaisissa verkoissa. LTE-tekniikassa tukiasemia on kuitenkin myös sellaisissa paikoissa, joihin GPS-satelliitit eivät kuulu, joten ainakin niiden ajoitus pitää hoitaa verkon kautta.

Syntyvät häiriöt ovat puhelun katkeamisia, tukiasemaan kytkeytymisen vaikeuksia ja sitä, että siirtyminen tukiasemasta toiseen vaikeutuu. Erityisesti LTE (4G) -tekniikkaan perustuva matkapuhelinverkko on haavoittuva (Talbot 2012) hyökkäyksille. Hyökkäys tehdään tässä tapauksessa suoraan tiedonsiirtoprotokollaan, ei ajoitukseen.

Lyhyen kantaman GPS-häirintä ei voi aiheuttaa ongelmia kuin korkeintaan paikallisesti. Valtiollinen häirintä tai sähköjärjestelmään tai ohjelmistoihin perustuva hyökkäys voisi oletettavasti aiheuttaa vakaviakin häiriöitä.

7.3.3 Televisio/radio

Digitaalinen maanpäällinen televisioverkko käyttää GPS-pohjaista aikasynkronointia saman taajuuden (SFN, Single Frequency Network) lähetysten toteuttamiseen (Viljasjärvi 2015). SFN-verkossa lähettimet, joiden peittoalueet menevät päällekkäin, lähettävät samalla taajuudella. Lähetykset synkronoidaan GPS:n avulla. Päällekkäin menevällä alueella vastaanotin lukittuu signaaleista voimakkaampaan, heikomman häiritsemättä vastaanottoa.

Mikäli GPS-signaali menetetään, jatkavat lähettimet lähettämistä oman sisäisen oskillaattorinsa tahdissa, mutta useiden tuntien kuluessa synkronointi ajautuu niin eri tahtiin, että lähettimet alkavat hiljalleen häiritä toisiaan ja signaalin vastaanottaminen alueella estyy. Digita ei ole tutkinut vaihtoehtoisia tapoja toteuttaa synkronointi. GPS:n käyttö SFN-verkoissa on alan standardi.

Digitan antaman tiedon perusteella voi päätellä, että häirintä sopivassa paikassa aiheuttaa häiriöitä televisiolähetysten vastaanotossa. Tämä koskee kuitenkin vain antenniverkon lähetyksiä, kaapeliverkkoon ei pitäisi tulla häiriöitä.

7.4 Energiasektori

Riskiraporttien perusteella Yhdysvalloissa kannetaan suurta huolta GPS-häirinnän sähköverkoille aiheuttaman riskin suuruudesta (GAO 2013). Amerikkalainen sähköverkko eroaa rakenteeltaan kotimaisesta jo senkin vuoksi, että Suomen sähköverkon koko on vain murto-osa Pohjois-Amerikan vastaavasta.

Perinteisesti sähköverkon synkronointi hoidetaan vaihtosähkön vaihetta seuraamalla ja tahdistamalla generaattori muun sähköverkon mukaan. Kun tahdistus

on kohdallaan, generaattori voidaan kytkeä verkkoon. Perinteinen sähköverkko ei reagoi GPS-häirintään.

Tilanne on muuttumassa älykkään sähköverkon kehittymisen myötä. Tarkan aikasynkronoinnin tarve syntyy mittausautomatiikasta ja vikadiagnostiikasta. Sähkötehon ja laadun mittauksissa tarvitaan hyvinkin tarkkoja aikaleimoja (Mikes 2015). PTP-synkronointi olisi mahdollinen, mutta se ei välttämättä toimi käytettyjen verkkotekniikoiden yli (Tuomaala 2013). Houkutus käyttää GPS-synkronointia on näin ollen varsin suuri. Tulevaisuuden kehityshankkeissa pitäisi ottaa huomioon häirintäriski ja suunnitella verkko immuuniksi sille.

7.5 Rahoitussektori

Kansainvälisissä riskiraporteissa (Coffed 2014, Curry 2014, GAO 2013) kannetaan huolta myös rahoitusmarkkinoiden mahdollisesta haavoittuvuudesta. Osakemarkkinoilla transaktioiden aikaleimaus esittää tärkeää roolia ja jos se perustuu GPS-aikasynkronointiin, häirinnällä voisi olla vaikutusta markkinoiden toimintaan. Esitetyt uhkakuvat (Attewill 2010) ovat kuitenkin varsin teoreettisia. Niissä rikolliset siirtävät pörssin kelloja, tekevät kauppoja ja siirtävät kellot takaisin. Uhkakuva ei vaikuta todennäköiseltä.

San Diegosta on raportoitu, että armeijan radiohäirintäkokeiden seurauksena pankkiautomaatit lakkasivat toimimasta (Coffed 2014). Kyseessä on tapaus vuodelta 2007. Pankkiautomaattien toimimattomuus johtui niiden käyttämän langattoman tiedonsiirron häiriintymisestä. Tiedusteluun Suomen tilanteesta Automatia Pankkiautomaatit Oy, joka vastaa pankkiautomaateista Suomessa, kertoi, ettei kotimaisilla pankkiautomaateilla ole minkäänlaista kytköstä GPS-teknologiaan (Makkonen 2015).

7.6 Metrologia (kaupunkimittaus, tienrakennus)

Kaupunkimittaus perustuu GPS:n käyttöön. Jos paikannus on häiritty toimimattomaksi, ei mittauksia luonnollisesti pystytä suorittamaan.

Maanrakennuksessa pyritään kohti 3D-malleja ja automaatiota. GNSS (RTK-GPS) on tässä merkittävässä roolissa (Nieminen 2011). Erityisesti jos häirintälaitteita käytetään liikennevälineissä, jotka ajavat jatkuvasti työmaan ohi, saattaa niistä aiheutua huomattavaakin haittaa koko rakennusprosessille. Haittaa voidaan vähentää käyttämällä useampaa GNSS (GPS, Glonass, Galileo, dou) -järjestelmää hyödyntävää vastaanotintekniikkaa.

7.7 Maatalous

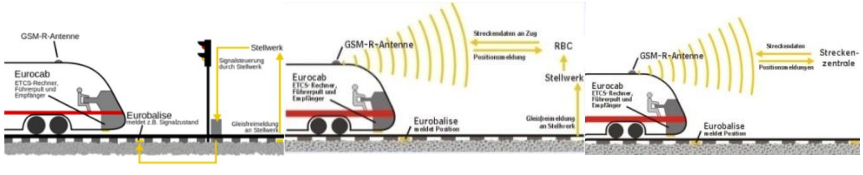
Maataloudessa ollaan siirtymässä täsmäviljelyyn, joka perustuu tilan olosuhteista kerättyyn paikkatietoon. Paikkatieto kerätään käyttämällä GPS-paikannusta referenssinä, samoin lannoitteiden ja ruiskutuksien ohjauksessa käytetään paikannusta. Ennustetaan, että maatilat robotisoituvat tulevaisuudessa. Suomen pellot ja tilat

ovat varsin pieniä automaattisille koneille. Yhdysvalloissa laajat preeriapellot tarjoavat automaattisille koneille paremmat olosuhteet. Paikannuksen puuttuminen estää automaattikoneiden toiminnan. Jos oletetaan, että häirintälaitteita käytetään lähinnä liikenteessä, häirinnän vaikutus ei ole kovin suuri, sillä pellot sijaitsevat useimmiten kaukana valtaväylistä. Täsmäviljelyssä laajamittainen häirintä tarkoittaa paluuta vanhoihin menetelmiin.

7.8 Liikenne

7.8.1 Rautatiet

Rautatieliikenteessä suunnitellaan eurooppalaista hallintajärjestelmän uudistusta. ETCS (European Train Control System) on jaettu tasoihin 0–3. Tasolle 3 on suunniteltu junan paikantamista GNSS-järjestelmällä, jolloin voitaisiin luopua eurobaliiseista (kulunvalvonnan komponentti) radalla (ks. Kuva 12). Tästä tietenkin seuraisi, että häirinnällä olisi mahdollista halvaannuttaa raideliikenne kokonaan. Suomessa ei ole suunnitelmia tasolle 3 menemisestä. Kotimaisessa raideliikenteessä on perinteinen signalointijärjestelmä. Junissa ohjataan GPS-pohjaisesti ainoastaan henkilöliikenteen kuulutuksia. Veturit on kylläkin varustettu paikannuslaitteistolla ja sijaintitietoa käytetään esimerkiksi *Junat kartalla* -palvelussa (https://www.vr.fi/cs/vr/fi/junat_kartalla). Häirintä ei siis haittaisi varsinaista liikennöintiä, mutta aiheuttaisi häiriöitä informaatiopalveluihin.



Kuva 12. ETCS-tasot 1, 2 ja 3.

7.8.2 Kuljetus

Kuljetusliikkeillä on käytössä kaluston seurantajärjestelmiä. Ajoneuvojen liikkeitä seurataan laitteistoilla, joissa on GPS-vastaanotin ja kommunikointi taustajärjestelmään. Kommunikointi hyödyntää joko matkapuhelinverkkoa tai satelliittipohjaista tiedonsiirtoa. Tyypillistä seurantajärjestelmille on suhteellisen harva sijainnin päivitysväli, esimerkiksi kerran 15 minuutissa.

Käyttökohteita voivat olla esimerkiksi seuraavat:

- Varastettujen autojen seuranta. Varkaiden hyödyntäessä häirintälaitetta, joka pimentää niin GPS:n kuin kommunikoinnin, seuranta ei toimi.
- Kaluston seurannassa voidaan ajoneuvojen reaaliaikaisen sijainnin avulla reitittää tehokkaammin ajoneuvoja kulloisenkin tilanteen mukaisesti. Kuljetusyritykset voivat seurata perävaunujen sijaintia.

- Arvokkaan omaisuuden seuranta ja turvaaminen esimerkiksi vakuutusyhtiön vaatimuksesta. Seurannalla voidaan varmistaa arvolastin kulkeminen suunniteltua reittiä ja ilman ylimääräisiä pysähdyksiä.
- Kenttähenkilökunnan, esimerkiksi huoltomiesten ja myyntimiesten, käyntikohteiden hallinta tehokkaasti edellyttää ajoneuvojen paikantamista.
- Ajoneuvojen huoltojen ennakointi ja kustannusten seuranta monitoroimalla polttoaineen kulutusta, ajotapaa ja kuljettua matkaa.

Tutkittaessa häirintälaitteiden käyttöä suurinta osa laitteista epäillään käytettäväksi kuljetusten seurannan estämiseen (Curry 2014). Sähköiset ajopiirturit eivät käytä paikannusta, joten ajoaikojen seurantaan tällä ei ole vaikutusta. Sähköinen ajopiirturi saatetaan sen sijaan tehdä toimintakyvyttömäksi voimakkaalla magneetilla, joka asennetaan vaihteiston kylkeen (Yle 2015), tai estämällä muuten nopeustiedon lukeminen autosta.

Satunnaisella häirinnällä ei juuri ole vaikutuksia kalustonhallinnan sovelluksiin, mutta laajempi häirintä aiheuttaa toiminnallista haittaa. Jos ajoneuvojen sijainti tiedetään vain satunnaisesti, järjestelmät eivät toimi kunnolla.

Tavaraliikenteessä on myös kokeiluja pakettien toimittamisesta lennokeilla asiakkaille. Esimerkiksi Posti on kokeillut pakettien toimittamista mantereelta Suomenlinnaan (http://www.posti.fi/lennot/). Suuryritykset, kuten Amazon (Gross 2013, Kuva 13), DHL ja Walmart, ovat esitelleet omia suunnitelmiaan. Lennokit ovat nyt teleoperoituja, mutta myös satelliittipaikannukseen perustuva automaattiohjaus on teknisesti mahdollinen toteuttaa.

Kuva 13. Amazonin tavaran toimitusta kokeillaan lennokilla (Gross 2013).

Kun lennokit kuljettavat jotain rahanarvoista, mahdollisesti arvokastakin lastia, rikolliset todennäköisesti kiinnostuvat niiden kaappaamisesta. Myös yksityisyyden suojasta huolestuneet tahot ovat osoittaneet halukkuutta lennokkien torjuntaan. Häirintälaitteiden käyttö (paikannus ja kommunikointi) on yksi mahdollinen tekniikka kaappaamiseen. Kuva 14 esittää Battelle-tutkimuslaitoksen kehittämää pitkän matkan häirintälaitetta DroneDefender, jonka kantomatkaksi on ilmoitettu 400

metriä (Terndrup 2015). Radioyhteytensä ja paikannuksensa menettänyt lennokki yleensä jää paikalleen ilmaan, yrittää laskeutua tai palata lähtöpaikkaansa riippuen toteutuksesta. Internetistä löytyy myös rakennusohjeita yksinkertaisten lentolaitteiden torjuntaan tarkoitetuille häirintälaitteille.

Kuva 14. Lennokkien torjuntaan kehitetty DroneDefender-radiohäirintälaite. Sillä on kyky häiritä sekä kommunikointia että paikannusta. (Terndrup 2015.)

7.8.3 Bussiliikenne

Bussiliikenteessä paikannusta käytetään matkustajainformaation tuottamiseen ja ohjaamiseen, rahastuslaitteessa sekä liikennevaloetuuksien tuottamiseen normaalin kalustoseurannan lisäksi.

Bussin sisällä olevia pysäkkinäyttöjä ohjataan paikannuksen perusteella. Samoin pysäkillä ja netissä olevat reaaliaikasovellukset ovat riippuvaisia satelliittipaikannuksesta. Häirintä aiheuttaa näin ollen palvelun heikkenemistä, jonka suuruus riippuu häirinnän yleisyydestä. Laajamittainen häirintä johtaa siihen, että palvelu muuttuu käyttökelvottomaksi ja hukkainvestoinniksi.

Rahastuslaitteissa paikannusta käytetään maksuvyöhykkeiden tunnistamiseen. Rahastuslaitteet käyttävät myös kellonaikaa, joka voidaan lukea GPS-vastaanottimelta. Häirintä aiheuttaa näin ollen ongelmia maksuvyöhykkeiden tunnistamisessa. Vyöhykkeiden tunnistaminen voidaan toteuttaa myös aikataulu- ja reittipohjaisesti, jolloin kuljettajan vastuulle jää pysäkin asettaminen manuaalisesti oikeaksi (Pusatec 2016). Bussit ajavat tunnettuja reittejä, jolloin paikantamisen voisi toteuttaa myös mittaamalla reitillä kuljettua matkaa ja täsmäyttämällä matkan mittaus aina pysäkillä ovien avautuessa. Vaihtoehtoisesti paikantamisen pysäkkitasolla voi toteuttaa käyttämällä pysäkillä RFID-tunnistetta, jonka ajoneuvo lukee saapuessaan pysäkille.

Vaihtoehtoisia tapoja siis on olemassa, joten häirinnällä ei ole suurta vaikutusta linja-auton maksuliikenteeseen, jos varakeinot huomioidaan järjestelmäsuunnittelussa.

Bussiliikenteen liikennevaloetuus perustuu paikannukseen. Lähestyessään liikennevaloristeystä bussi voi saada liikennevaloetuuden, jos se on aikataulustaan jäljessä. Laajamittainen häirintä sotkee etuusjärjestelmän, ja myös siitä saatavat taloushyödyt jäävät saamatta. Lisäksi joukkoliikenteen palvelutaso heikkenee.

7.8.4 Merenkulun järjestelmät ja laitteet

GPS-signaali on tällä hetkellä merenkulun järjestelmien ja laitteiden paikannus-, navigointi- ja aikatiedon ensisijainen lähde. Meriliikenne on suuresti riippuvainen tarkoista GPS-signaaleista monin tavoin.

Viime aikoina huoli GPS-järjestelmän häiriöiden vaikutuksista meriliikenteeseen on kasvanut (Jones 2014). Maihin sijoitettujen häirintälaitteiden uhkaa pidetään suurempana verrattuna mahdollisiin aluksilla oleviin häirintälaitteisiin. Laivojen GPS-antennit on sijoitettu mahdollisimman ylös alusten rakenteisiin eli standardikomentosillalle, joten antennien ja lastikansilla ajoneuvoissa olevien häirintälaitteiden etäisyys kasvaa aina noin 200 metriin, jolloin häiriöriski pienenee. Laivan rakenteet rajoittavat häiriösignaalien kulkua, vaikkakin aluksilla useimmiten käytetään UHF-taajuuksien turvaamiseksi vahvistimia, jotka samalla voivat vahvistaa häiriöitä.

Navigointi

GPS-koordinaatteja syötetään moniin aluksen tietoteknisiin järjestelmiin, kuten elektroniseen karttajärjestelmään (ECDIS, electronic chart display and information system), automaattiseen tunnistusjärjestelmään (AIS, automatic identification system) tai merenkulkututkiin (Inside GNSS 2009). Sen vuoksi erityisesti navigointi, tilannetietoisuus, aluksen positio suhteessa karttakuvaan ja esimerkiksi hätäliikenteessä käytetty automaattinen selektiivikutsu (DSC, digital selective call) voivat olla alttiita häiriöille, mikäli ne saavat keskeisen tiedon GPS-datasta (Grant ym. 2008).

Grant ym. (2008) testasivat laajasti GPS-häirinnän vaikutuksia turvalliseen navigointiin merikokeiden sarjassa. Erilaiset häiriölähteet ja niiden vaikutukset koostuivat rannikolle sijoitetusta häirintälaitteesta, joka aiheutti GPS-signaalin kadottamisia sekä häiriöitä AIS- ja tutkalaitteisiin, sekä alukselle sijoitetusta hyvin vähätehoisesta häirintälaitteesta, joka aiheutti vaarallisesti harhaanjohtavaa tietoa. Navigointijärjestelmät eivät hälyttäneet automaattisesti GPS-signaalin häiriöistä, vaikka ne tuottivat harhaanjohtavaa tietoa ja johtivat virheellisiin paikannuksiin ja nopeuksiin.

Merikokeissa vähätehoiset häirintälaitteet aiheuttivat hälytyksiä ja ääniä sekä johtivat ECDIS-järjestelmän, autopilotin, DGPS:n, helikopterikannen vakautusjärjestelmän, satelliittikommunikointijärjestelmän, tutkan, gyrokompassin, AIS-järjestelmän ja DSC-GMDSS-hätähälytysjärjestelmän vikoihin komentosillalla (Last 2010). Nämä komentosiltajärjestelmät hyödyntävät GPS-signaalia ajan, keulasuunnan ja paikan määrittämiseen. GMDSS-järjestelmän viat voivat johtaa

mahdollisten hätäsignaalien sekä rutiininomaisen ja kaupallisen radioliikenteen häiriöihin.

Häirintälaitekokeissa aluksilla voitiin säilyttää jonkinasteinen hallinta ja riittävän laadukas data. Merikokeisiin osallistuneiden asiantuntijoiden mukaan testit osoittivat, että komentosiltajärjestelmät voisivat vikojen ilmaantuessa kuitenkin hyötyä uusista laitteistoista, kuten eLoran-datasta (enhanced Loran, radionavigointijärjestelmä) (Jones 2014). GPS-häiriöiden vaikutusten vakavuus riippuu miehistön kyvystä hyödyntää perinteisiä navigointi- ja paikannuskeinoja (kuten tavallista tutkasignaalia) sekä käytettävissä olevista perinteisistä keinoista (Grant ym. 2008).

Kriittisten komentosiltajärjestelmien lisäksi toissijaiset järjestelmät voivat romahtaa, jos GPS-signaalia häiritään pitkään. Monet alusten etäohjatut järjestelmät hyödyntävät GPS-signaalia. Etäohjatut järjestelmät muun muassa tukevat dynaamista paikannusjärjestelmää, ohjailupotkurien hallintajärjestelmää, integroituja komentosiltajärjestelmiä, alusten muita automaatiojärjestelmiä ja alusten kommunikointia. (Jones 2014.)

Meriliikenteen kaukovalvonta ja alusliikennepalvelut

GPS-signaalin häiriöt lisäävät merialueiden valvontaan ja alusliikennepalveluihin liittyviä riskejä. Kaukovalvontapisteissä toimivat merivartijat ja alusliikenneohjaajat todennäköisesti hämmentyvät järjestelmien antamista virheellisiä sijainteja ja nopeuksia sisältävistä AIS-tiedoista, jotka ovat ristiriitaisia tutkatietoon verrattuna (Grant ym. 2008). Alusten seurantaa on ylläpidettävä yksinkertaista tutkapaikantamista hyödyntäen.

Merimerkit (AtoNs)

Merimerkkijärjestelmät koostuvat kiinteistä, kelluvista ja virtuaalisista merimerkeistä, joista osa hyödyntää GPS-signaalia. Esimerkiksi merimerkkien synkronoidut valosignaalit käyttävät GPS-järjestelmän aikatietoa (Inside GNSS 2009). Merimerkkinä voidaan käyttää myös AIS-laitetta, joka häiriötapauksessa lähettää virheellistä tietoa merenkulkijoille samoin periaattein kuin alukseen sijoitettava AIS-laite häiriintyisi GPS-signaalin häiriöstä (Grant ym. 2008).

Satamatoiminnot

Kokonaan ja osittain automatisoiduissa satamissa hyödynnetään satelliittipaikannusta lastiyksiköiden paikantamiseen ja lastinkäsittelyjärjestelmien operointiin. Konttikentät on järjestetty konttien sijaintitietoon perustuen. Kaukoohjausjärjestelmien ja automaation haavoittuvuus voi johtaa erilaisiin seurauksiin paikannushäiriön ilmetessä. Yhä useammasta isommasta satamasta ja terminaalista on tullut osittain tai kokonaan automatisoitu, kun nostureita, kulunvalvontaa, hallintoa ja rahdin siirtelyä ohjataan kaukohallintapisteistä (Jones 2014).

Sataman toiminnot edellyttävät riippumattomuutta säästä ja GPS-paikannuksen tarkkuuden vaihtelusta. Konttikentälläkin esiintyy GPS-katvealueita. Näistä syistä

paikannus rajatuilla satama-alueilla on yleensä toteutettu alueen erityispiirteet huomioon ottaen ja useita paikannusjärjestelmiä yhdistelemällä.

Merenkulun häiriöt suomalaisesta näkökulmasta

Suomen rannikko on hyvin kartoitettu, ja väylät ovat monin eri tavoin merkittyjä. Niinpä rantaväyliä voidaan kulkea GPS-signaalin häiriintyessä varsin turvallisesti perinteisiä merenkulkutaitoja ja visuaalisia navigointimerkkejä hyödyntäen, mikäli niitä on ylläpidetty elektronisten apuvälineiden rinnalla. Pakollinen luotsaus ja linjaluotsin tutkinnot edesauttavat liikennöintiä muunkin kuin GPS-tiedon turvin. Perinteisiä paikannusmenetelmiä käytettäessä alusten kulkunopeutta voidaan joutua vähentämään ja lastausoperaatiot todennäköisesti kestävät odotettua kauemmin. Lisäksi näkyvyyden ollessa rajoittunutta esimerkiksi sumun tai sateen vuoksi kulkunopeuksia joudutaan alentamaan entisestään, ja silti onnettomuusriski voi olla suuri.

Merialueilla ja erityisesti Suomenlahdella, jossa on paljon tankkeri- ja matkustaja-alusliikennettä, GPS-signaalin häiriöt voivat olla kohtalokkaita. Avomerellä komentosillalla ei välttämättä noudateta yhtä suurta huolellisuutta kuin rannikon läheisyydessä, eikä meriliikennekeskuskaan välttämättä voi varoittaa navigaattoria, jos kommunikointimahdollisuus on poissa tai rajoittunut.

Satamatoimintoihin GPS-häiriöt vaikuttavat tällä hetkellä lähinnä suurimmissa satamissa, joissa automaatio ja kauko-ohjaus ovat edenneet pisimmälle. Toistaiseksi Suomessa ei ole ollut kiinnostusta lisätä automaatiota satama-alueilla entisestään, koska rahtivolyymit ovat verrattain pieniä.

GPS-signaalin häirintämahdollisuus jarruttaa merkittävästi automaation etenemistä merenkulussa. Automatisoidut toiminnot niin aluksilla kuin kauko-ohjauspaikoilla voivat vaarantua, eikä aikaa välttämättä ole häiriölähteiden todentamiseen ja virheellisen datan ohittamiseen.

7.8.5 Automaattinen ja kooperatiivinen tieliikenne

Tulevaisuuden älyliikenteen sovelluksia on kehitelty pitkään eri tutkimus- ja kokeiluhankkeissa. Yhteistoiminnallisessa (cooperative ITS, myös connected vehicles) liikenteessä ajoneuvot vaihtavat tietoja sekä keskenään että tieverkoston eri järjestelmien kanssa. Myös suunnitelmat automaattisten ja autonomisten autojen tuomisesta liikenteeseen ovat pitkällä.

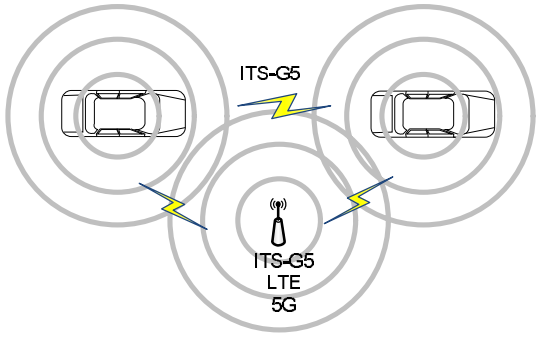
Yhteistoiminnallisen liikenteen sovelluksista suuri osa perustuu ajoneuvojen tarkkaan ja taajaan (1–10 Hz) paikantamiseen satelliittipaikannuksella. Korkeimmat tarkkuusvaatimukset liittyvät ajoneuvojen väliseen törmäyksenestoon esimerkiksi risteystilanteissa. Tällaiset toiminnot ovat toistaiseksi vasta tutkimusvaiheessa. Ensimmäiseksi kuljettajille tullaan tarjoamaan informaatiopalveluita siitä, mitä tiellä kohta on edessä. Lähestyvästä tietyöstä saatetaan varoittaa parin kilometrin etäisyydeltä. Niidenkin informaatiopalveluiden, joissa perustasoon riittää kilometrien ja minuuttien tarkkuus, kehityssuunnitelmiin saattaa liittyä paikannuksen tar-

kentaminen; varoitukset haluttaisiin kohdistaa vain niille kuljettajille, jotka ajavat tiettyä tietä tiettyyn suuntaan.

Ohitustilanteiden tukemisessa ja törmäyksistä varoittamisessa ponnistellaan vaadittavan paikannustarkkuuden saavuttamiseksi. Käytetyt menetelmät perustuvat erilaisiin GNSS-algoritmien sovelluksiin. Satelliittipaikannuksen tukena käytetään inertiamittausta, odometriaa (matkan mittausta), tutka- ja kamerajärjestelmiä sekä ajoneuvojen välistä tiedonvaihtoa esim. yksittäisten GPS-satelliittien mitatuista etäisyyksistä. Maa-ajoneuvoissa inertiamittauksen menetelmillä pystytään paikantamaan ajoneuvo lyhyitä aikoja satelliittipaikannuksen katkojen aikana. Ilman satelliittipaikannusta paikan arvio alkaa kuitenkin heiketä.

GPS-häirinnällä saadaan liikenteen kooperatiiviset sovellukset lähes käyttökelvottomiksi, koska useimmat niistä perustuvat satelliittipaikannukseen. Kommunikointi perustuu ITS-G5-standardin mukaiseen lyhyen kantaman radiotekniikkaan (IEEE 2006), jonka kantama on hyvissäkin olosuhteissa muutama sata metriä. Paikannuksen puuttuessa saadaan tieto lähistöllä olevista muista ajoneuvoista (myös ruuhkista, hälytysajoneuvoista, rikkinäisistä ajoneuvoista jne.), mutta niiden sijainti- ja suuntatieto jää puuttumaan tai on vanhaa/virheellistä.

ITS-G5 käyttää paikkasidonnaista protokollaa, jolla viestien lähetys voidaan rajata halutulle maantieteelliselle alueelle. Tämäkään mekanismi ei toimi ilman tietoa globaalista paikasta. Radioliikenteessä käytetty taajuus on 5,9 GHz, joka on varsin etäällä satelliittipaikannuksen taajuudesta. Häirintälaitteet eivät näin ollen vaikuta kommunikointiin.

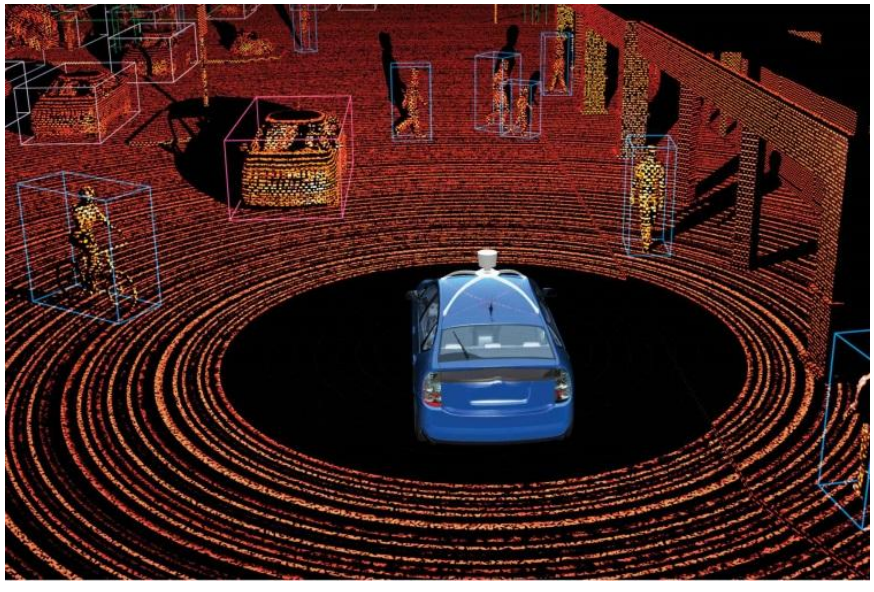


Kuva 15. Yhteistoiminnallisen liikenteen periaate.

Yksittäisiä automaattisia toimintoja (esim. mukautuva vakionopeudensäädin, kaistavahti, pysäköintiavustaja) sisältävissä ajoneuvoissa on aina kuljettaja ja automatiikkaa voidaan hyödyntää liikenteessä vain osan aikaa. Teknisesti automaatio perustuu ympäristön havainnointiin antureilla. Ajoneuvon nopeutta säädetään esim. tutkaan perustuvalla mukautuvalla vakionopeussäätimellä, ja kaistalla pysyminen perustuu kaistaviivojen havainnointiin kameralla. Pelkästään lähialueen

havainnointiin perustuvat järjestelmät eivät tarvitse satelliittipaikannusta toimiakseen, joten ne eivät myöskään ole alttiita häirinnälle.

Seuraava mahdollinen askel kehityksessä ovat autonomiset ajoneuvot, jotka voivat siirtyä paikasta toiseen ilman kuljettajaa. Autonomisessa autossa reitin suunnitteluun ja reitin seurantaan vaaditaan paikannustietoa, jonka tuottamiseen satelliittipaikannus olisi luonteva valinta. Toistaiseksi riittävän tarkkaa satelliittipaikannusta ei voi taata aina ja kaikkialla. Googlen robottiautoissa satelliittipaikannuksen tarkkuus- ja luotettavuusongelma on ratkaistu tarkalla ympäristömallilla. Kun auton laserskannerin mittaustuloksia verrataan ympäristömalliin, auton globaali paikka voidaan selvittää tarkasti. Kuva 16 esittää Velodyne-laserskannerin antamaa pistepilvikuvaa ympäristöstä (Fischer 2013). Menetelmä edellyttää, että reitit on ajettu etukäteen ja antureiden tuottama ympäristödata on tallennettu. Syntyvä tietokanta on varsin massiivinen ja rajaa robottiauton toiminta-aluetta.



Kuva 16. Googlen käyttämän Velodyne 64 -laserskannerin antama kuva ympäristöstä (Fischer 2013).

Yksittäiset toteutukset vaihtelevat: autonomisten ajoneuvojen navigaatiojärjestelmät voivat painottaa GPS-tietojen ja ympäristötietojen käyttöä eri tavoin. Satelliittipaikannus voisi myös auttaa toipumaan sellaisesta virheestä, että karttanauhoitukseen perustuva autonominen ajoneuvo ei jonain hetkenä kykene päättelemään, mihin kohtaan nauhoitettua reittiä on edetty. Paikannus tukisi myös selviytymistä tilanteessa, jossa ympäristöön on tullut muutoksia esim. lumisateen vuoksi.

Muiden valmistajien autonomisten ajonevojen lopullinen teknologiatoteutus ei ole tiedossa, joten häirinnän vaikutusta on vaikeaa arvioida. Valistunut arvaus on, että toteutus vastannee Googlen käyttämää tekniikkaa. Ostivathan Daimler AG,

Audi AG ja BMW Group Nokialta HERE-yksikön tuottamaan kartta-aineistoa yhteenliittymän autoihin (von Bell 2015). Ympäristön havainnoinnin käyttäminen paikannuksen tukena auttaa merkittävästi, mutta häirintä aiheuttanee todennäköisesti jonkinlaisia ongelmia.

Automaattisen joukkoliikenteen kokeiluja on tehty eri puolilla Eurooppaa, esimerkiksi CityMobil2-hankkeen kokeilut Vantaalla, Lausannessa ja viimeksi Wageningenissa (Muio 2015). Kokeiluissa käytettiin Ligier EZ10 -ajoneuvoa (Kuva 17). Kokeiluissa ajoneuvojen paikannus on perustunut satelliittipaikannukseen. Joukkoliikenteen autonomisen ajoneuvon ero henkilöautoon verrattuna on sen liikkuminen kiinteällä reitillä ja maantieteellisesti pienemmällä alueella. Tällöin satelliittipaikannuksen varmistavan vaihtoehtoisen paikannusmenetelmän toteutus on paljon helpompi ratkaista. Asentamalla reitille täsmäyttimiä voidaan globaalia paikkaa pitää yllä häirinnästä huolimatta. Samalla kuitenkin menetetään joustavuus; reittimuutokset vaativat täsmäyttimien uudelleenasentamisen ja koko järjestelmän kalibroinnin. Jos vaihtoehtoista paikannustapaa ei ole käytössä, häirinnällä pystyy pysäyttämään liikennöinnin kokonaan.

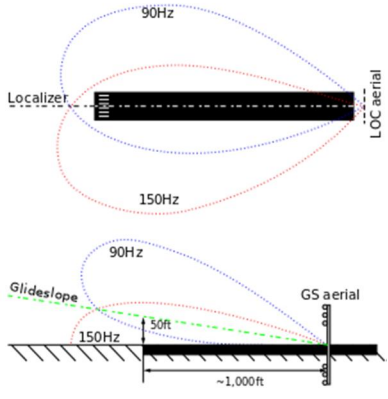
Kuva 17. CityMobil2-hankkeen käyttämä EZ10-pienoisbussi.

7.8.6 Lentoliikenne

Yhdysvalloissa on ollut tapauksia, joissa lentoliikenne on häiriintynyt. Tunnetuin näistä tapahtui Newarkin lentokentällä, jossa seurantaa pakoillut kuljetusliikkeen työntekijä onnistui häirintälaitteella pimentämään lentokentän GPS-pohjaisen lähestymisjärjestelmän vuonna 2013.

Suomessa tällä hetkellä käytössä olevat konventionaaliset navigaatiolaitteet perustuvat maalaitteista tuotettuun signaaliin ja sen käyttöön/koodaamiseen ilma-aluksessa. Eri maalaitteiden tuottaman paikannustiedon lopputuloksena ilma-alus pystyy määrittämään maantieteellisen sijaintinsa tarkasti. Eri järjestelmien tuottaman paikannustiedon tarkkuus riippuu ko. järjestelmän teknologiasta, ilma-aluksen sijainnista suhteessa maa-asemaan, laitteen fyysisestä asennuspaikasta ja olosuhteista. Nämä Suomessa käytössä olevat konventionaaliset navigaatiolaitteet ovat yleisesti jo ikääntyneitä. (Trafi 2012.) Kun konventionaaliset ilmailun valvontajärjestelmät perustuvat maalaitteilla tuotettuun ilmatilannekuvaan, uuden teknologian mukainen ilmailun valvontajärjestelmä perustuu ilma-aluksien tuottamaan paikkatietoon. Tämä edellyttää uuden teknologian mukaista navigaatiojärjestelmää (satelliittipaikannusta hyödyntävä RNAV).

Suomen kansallinen ilmailun navigaatio- ja valvontastrategia on laadittu huomioiden kansainvälinen ATM Master Plan (http://www.atmmasterplan.eu). Ilmailun navigaatio- ja valvontalaitejärjestelmää on tarkoitus kehittää tämän kansallisen strategian mukaisesti. Kehittämistyö tarkoittaa uusien navigaatio- ja valvontalaitejärjestelmien käyttöönottoa ja asteittaista luopumista perinteisistä järjestelmistä. Konventionaaliset (perinteiset) suunnistuslaitteet paitsi ILS (Instrumental Landing System, ks. Kuva 18) korvataan vähitellen satelliittiperusteisilla menetelmillä. Pidemmällä aikavälillä myös ILS tultaneen korvaamaan satelliittipaikannukseen perustuvalla EGNOS-avusteisella järjestelmällä. (Trafi 2012.)



Kuva 18. Lentoliikenteen ILS (Instrumental Landing System) -periaate.

RNAV ei perustu pelkästään satelliittipaikannukseen. Järjestelmän käytössä on myös muita paikannusmenetelmiä, ja lisäksi sijaintia valvoo lennonvalvonnan tutkaseuranta. Täten häirinnällä ei pitäisi olla vaikutusta liikennelentokoneisiin, jotka lentävät matkalentoa. Lentokorkeuden ollessa 5–11 km on epätodennäköistä, että autossa olevan häirintälaitteen kantama olisi edes riittävä häiritsemään koneen paikannusta. Nostamalla lähetystehoa saadaan kantamaa lisättyä, joten häirintä ei ole poissuljettua. Pienkoneille riski on suurempi, koska niiden laitteistot

eivät ole niin kehittyneitä ja kalliita kuin liikennelentokoneissa. Häiritty pienkone ei toki putoa maahan, mutta se voi harhautua reitiltään ja aiheuttaa törmäysriskin muun ilmaliikenteen kanssa. Ilmavalvonnan perustuessa koneen itsensä määrittämään paikkaan virheellinen paikka välittyy myös ilmavalvonnalle. Toisaalta taustalla on ilmavalvonnan tutkaseuranta, jolla paikkatiedon virheellisyys voidaan havaita.

Suurin riski onkin laskeutumisessa. Niin kauan kuin ILS on käytössä, häirinnän vaikutus on olematon. Mutta suuntaus näyttää olevan kohti satelliittipohjaisia järjestelmiä, joten riski on syntymässä, kuten Newarkin tapaus osoittaa. Lentoliikenteen järjestelmissä on myös aikasynkronoituja komponentteja, joiden ajoituksiin häirinnällä on vaikutusta.

8. Yhteenveto

Suoriteperusteisen kilometriveron kaltaisen järjestelmän edellyttämään toiminnallisuuteen liittyy tietoturvauhkia. Eri toimijoihin kohdistuvat riskit ovat erityyppisiä, ja niiltä suojautuminen edellyttää joiltakin osin erilaisia ratkaisuja. Järjestelmän suunnittelun ja toteutuksen kannalta avainasemassa on viranomaistaho, sillä muilla ei ole juuri mahdollisuutta vaikuttaa perusjärjestelmän määrittelyyn tai toteutukseen. Perusjärjestelmän tarjoaman toiminnallisuuden ja turvallisuuden parantaminen jälkikäteen esimerkiksi palveluntarjoajan näkökulmasta – käyttäjästä puhumattakaan – on vaikeaa tai mahdotonta. Osa ehdotetuista toimenpiteistä on puhtaasti teknisiä, mutta osa on toteutettava lainsäädännöllä tai muulla sääntelyllä.

Useat tunnistetuista riskeistä ovat hyvin hallittavissa, mikäli ne huomioidaan järjestelmän toteutuksessa. Tietoturvauhkien tarkempi tarkastelu tulee tehdä järjestelmän määrittelyvaiheessa, ja riskien todennäköisyyttä pitää arvioida uudestaan määrittelyn mukaisen toiminnallisuuden ja häiriöttömän toiminnan takaamiseksi harkittujen suojaustoimenpiteiden perusteella.

Kuluttajan vastuu omien tietojen käsittelystä kasvaa, ja jokainen päätös sallia tietojen luovutus on punnittava tarkoin. Tärkeää on, että kuluttajat saavat riittävästi tietoja ja ohjeita omien tietojensa käsittelyn seurantaan. Yksityisten lisäpalvelujen osalta kuluttajalla pitää olla mahdollisuus valita, käyttääkö palvelua vai ei – viranomaispalveluiden tai -rekisterien osalta tällaista valinnanvapautta ei yleensä ole. Kuluttajalla pitää olla myös oikeus muuttaa mieltään ja kieltää tietojen käsittely sekä pyytää poistamaan tiedot, joiden säilyttämiseen ei ole lakiin perustuvaa velvollisuutta.

Viranomaisrekistereiden osalta kuluttaja ei yleensä voi vaikuttaa rekisteröintiin, mutta tietojen luovutus on säänneltyä ja rekisteröity voi sen kieltää. Rekisteröityä on informoitava tietojen keräämisestä, käsittelystä ja säilytyksestä sekä tietojen tuhoamisesta. Käytettäessä tietoja johonkin muuhun tarkoitukseen, kuten liikennesuunnitteluun, tiedot anonymisoidaan. Palveluiden käyttämiseksi tarvittavaa tietoa ei luovuteta suoraan palveluntarjoajalle, vaan sen on kierrettävä kuluttajan kautta.

Palveluntarjoajien on aina saatava suostumus kuluttajalta tietojen käsittelyyn tai edelleen luovutukseen. Ajoneuvolla voi olla useita käyttäjiä. Lisäpalveluihin rekisteröitymisen tulisi edellyttää salasanaa. Kerättävän tiedon pitää olla vain palvelun kannalta tarpeellista, ensisijaisesti käyttäjältä itseltään saatavaa tietoa ja vain käyttäjän suostumuksella muista lähteistä kerättyä. Palvelun kannalta tarpeetto-

maksi muuttunut tieto hävitetään, tietoa ei saa luovuttaa edelleen ilman käyttäjän suotumusta, eikä tietoja käytetä muuhun tarkoitukseen kuin johon ne on alun perin kerätty ja johon on saatu suostumus. Käyttäjää on informoitava tietojen keräämisestä, käsittelystä ja säilytyksestä sekä tietojen tuhoamisesta.

Ajoneuvoon asennettavan satelliittipaikannuslaitteen on kestettävä vaativia olosuhteita. Laaja käyttölämpötila-alue, kosteus, tärinä ja sähköiset häiriöt asettavat elektroniikan kestokyvyn koetukselle. Paikannuslaitteen virrankulutusta on myös hallittava ajoneuvon käytön mukaan, jotta ajoneuvon akku ei tyhjenisi. Nykyaikaiset pienet integroidut piirit ja ajoneuvokäyttöön suunnitellut tuotteet kuitenkin selviävät hyvin tällaisista vaatimuksista. Muut verotuskäytöstä seuraavat suunnitteluparametrit asettavat suurempia haasteita. Kerättävien tietojen manipuloinnin estämiseksi on käytettävä tietoliikenteen salausta, laitteen elektroniikka mahdollisesti suojattava epoksipinnoitteella ja sen ohjelmiston muokkaaminen estettävä. Laitteen suojaaminen manipuloinnilta nostaa suunnittelu- ja valmistelukustannuksia.

Suojauksista huolimatta ajoneuvoon asennettava paikannuslaite on helpoilla toimenpiteillä tehtävissä toimintakyvyttömäksi. Tähän riittää GPS-antennin peittäminen esimerkiksi foliolla paikannuksen estämiseksi, antennikaapelin irrotus, laitteen energiansyötön katkaisu tai paikannussignaalin häirintä ulkopuolisella häirintälaitteella. Näistä toimista osa voitaneen havaita laitteen lähettämien käyttötietojen perusteella, mikäli laite sisältää diagnostiikkaa varten esimerkiksi liikeantureita ja paristovarmennuksen.

Ajoneuvo, josta seurantalaite on poistettu tai tehty kokonaan toimintakyvyttömäksi, voitaisiin havaita tienvarren tarkastuslaitteilla, jotka kuvaavat rekisterikilpiä ja vertaavat taustajärjestelmän sijaintitietoja tarkastuspisteen havaintoihin. Jos havainnot eivät täsmää, ajoneuvolaitteessa on joko vikaa tai sen toiminta on estetty. Tarkastusta voidaan tehdä joko kiinteitä asemia käyttäen tai liikutettavilla laitteilla.

On syytä huomata, että satelliittipaikannuksen häirintälaitteen kantama voi olla esimerkiksi 500 metriä, jolloin yksi häirintälaite pimentää useita ajoneuvolaitteita. Näin ollen tietojen puuttuminen ei välttämättä johdu tarkastettavan autoilijan epärehellisyydestä vaan lähistöllä olevan toisen ajoneuvon käyttämästä häirinnästä. Mahdollisten väärinkäytösten tarkastus voi osoittautua monimutkaiseksi ja resursseja vaativaksi.

Satelliittipaikannuksen estäminen radiohäiriötä lähettävillä laitteilla on helppoa ja edullista. Monimutkaisemmat paikannussignaalin häirintätavat ajoneuvojen ulkopuolelta, kuten signaalien väärentäminen, edellyttäisivät sen sijaan syvällisiä tietoja ja nykyään huomattavan arvokkaita sotilastason lähetyslaitteita.

Paikannuksen häirintä aiheuttaa vaikutuksia liikenteen lisäksi myös muille sovellusalueille, kuten pelastustoimi, rahoitussektori, sähköverkot ja maatalouden automaatio. Paikannuksen estyminen ei suurimmassa osassa tarkastelluista sovellusalueista aiheuta välitöntä vahinkoa, harmia kylläkin. Paikannukseen perustuvat palvelut pätkivät, ja niiden käyttäjilleen antama lisäarvo heikkenee. Turvallisuuskriittiset sovellukset saattavat nekin häiriytyä, mutta varajärjestelmien ansiosta toimintaa kyetään jatkamaan. GPS-häirinnän mahdollisuuteen on varauduttu erityisesti puolustusvoimissa ja rajavalvonnassa.

Yhteiskunnan kannalta merkittäviä, häiriöille mahdollisesti alttiita järjestelmiä ovat esimerkiksi matkapuhelinliikenne ja älykkäät sähköverkot. Niissä hyödynnetään GPS-järjestelmän tarjoamaa tarkkaa aikatietoa. Aikavirheisiin perustuvia häiriöitä voi välttää käyttämällä aikasynkronointiin esimerkiksi internet-tiedonsiirtoon perustuvaa IEEE 1588 PTP (Precision Time Protocol) -protokollaa GPS:n tukena. Varajärjestelmien käyttö onkin usein huomioitu järjestelmien suunnittelussa, mutta niiden todellista häiriönsietoa on tärkeää testata.

Kohteet, joissa häirintä aiheuttaa ongelmia, kuten satamat ja lentokentät, tulisi varustaa häirinnän havaitsemislaitteilla. Sijoittamalla niitä tuloväylille käyttäjiä voisi paljastaa ennen kuin häirinnällä saadaan aikaan vahinkoa.

Uusista tie-, lento- ja laivaliikenteen sovelluksista monet perustuvat suoraan satelliittipaikannuksen käyttöön. Tällaisten sovellusten osalta häiriöriski on ilmeinen. Useat paikannussovelluksista tuottavat kuitenkin käyttäjilleen lähinnä avustavaa informaatiota. Satelliittipaikannuksen käyttö suoraan ohjaukseen tai turvallisuuskriittisiin toimintoihin on ongelmallista ilman häirintääkin, koska paikannuksen tarkkuus ja saatavuus vaihtelevat sään ja maaston mukaan.

Suurimpia riskejä tunnistettiin toistaiseksi laivaliikenteessä, jossa laivoja ohjataan kapeilla väylillä GPS-pohjaisella automaattiohjauksella. Mikäli GPS-häirintään ei ehditä reagoida ajoissa tai se on erityisen taitavaa, laiva voisi ehkä ohjautua karille ja aiheuttaa suuronnettomuuden.

Lentoliikenteen kehitys kohti satelliittipaikannukseen perustuvia laskeutumisjärjestelmiä sisältää sekin riskejä. Niin kauan kuin varajärjestelmiä, kuten analoginen ILS-järjestelmä, on käytössä, häirinnällä on vain rajallisia vaikutuksia liikennelentokoneisiin. Pienkoneiden kohdalla turvallisuusriski on suurempi, mikäli niissä ei ole vastaavia varajärjestelmiä kuin liikennelentokoneissa.

Automaattisen ja yhteistoiminnallisen liikenteen kohdalla häirinnän vaikutuksia on vaikea välttää. Yhteistoiminnalliset järjestelmät perustuvat paikannustietojen välittämiseen muille ajoneuvoille. Monet muut kuljettajaa tukevat järjestelmät, kuten kaistavahdit ja törmäysvaroittimet, perustuvat sen sijaan ympäristöä havainnoiviin antureihin eivätkä satelliittipaikannukseen. Antureita, kuten kameraa, käytetään niissä mittaamaan ajoneuvon tarkka sijainti esim. kaistaviivoihin nähden. Viime aikoina useat autonvalmistajat ovat esitelleet myös tarkkoihin ympäristömalleihin ja antureihin perustuvia automaattisen navigoinnin toteutuksia. GPS:n tarkkuus ja saatavuus eivät yksinään tunnu riittävän automaattiseen ajamiseen.

Lähdeviitteet

ACM 2003. Anonymous usage of location-based services through spatial and temporal cloaking. Marco Gruteser & Dirk Grunwald. MobiSys '03, pp. 31–42. http://dl.acm.org/citation.cfm?id=1189037

Attewill, F. 2010. GPS jammers could make criminals millions on the stock market. Metro UK, February 21. http://metro.co.uk/2012/02/21/gps-jammers-could-make-criminals-millions-on-the-stock-market-327410/#ixzz3pTpE303o

Babar 2010. Proposed security model and threat taxonomy for the internet of things (IoT). Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, Ramjee Prasad, N. Meghanathan et al. (Eds.) CNSA 2010, CCIS 89, pp. 420–429. http://link.springer.com/10.1007/978-3-642-14478-3_42

Bora M. 2012. Analyzing the pictures and mystery behind capture of the U.S. stealth drone RQ-170. DefenceAviation Jan 12. http://www.defenceaviation.com/2012/01/analyzing-the-pictures-and-mystery-behind-capture-of-the-u-s-stealth-drone-rq-170.html

Chronos 2013. Chronos announces the release of CTL3520 handheld GPS Jamming Detector and Locator System. Chronos Technology Ltd. Lehdistötiedote 2013. http://www.chronos.co.uk/index.php/en/legal/364-news-a-press-releases/newsa-pr-all/1289-chronos-announces-the-release-of-ctl-3520-handheld-gps-jamming-detector-and-locator-system

Coffed J. 2014. The Threat of GPS Jamming: The Risk to an Information Utility. Feb, 2014. Exelis Inc. http://www.exelisinc.com/solutions/signalsentry/Documents/ThreatOfGPSJamming_February2014.pdf

Curry C. 2014. SENTINEL Project – Report on GNSS Vulnerabilities. April 4, 2014. 59 p. Chronos Technology Limited, UK. http://www.chronos.co.uk/files/pdfs/gps/SENTINEL_Project_Report.pdf

Darpa 2015. DARPA plans GPS Replacement With Atomic Clocks For Military Applications. www.defenceworld.net 26.12.2015.

DEFCON22 2014. Hacking US Traffic Control Systems. Cesar Cerrudo. https://defcon.org/images/defcon-22/dc-22-presentations/Cerrudo/DEFCON-22-Cesar-Cerrudo-Hacking-Traffic-Control-Systems-UPDATED.pdf

FiCoRA 2016. Ohjeita viestinnän suojaamiseen. Viestintävirasto, Helsinki. http://www.viestintavirasto.fi/attachments/Ohjeita_viestinnan_suojaamiseen.pdf

Fischer A. 2013. Inside Google's Quest to Popularize Self-Driving Cars; Robots can already outdrive humans. Now everyone needs to get out of their way. Popular Mechanics, 18.9.2013. http://www.popsci.com/cars/article/2013-09/google-self-driving-car

GAO 2013. GPS DISRUPTIONS: Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced. United States Government Accountability Office Report to Congressional Requesters. Nov 2013. GAO-14-15.

Grant A., Williams P., Ward N. & Basker S. 2008. GPS Jamming and the Impact on Maritime Navigation. GNSS Vulnerabilities and solutions conference, Croatia, 8th September 2008. Available at Internet: www.gla-rrnav.org/file.html?file=e1927d5a1087d8b1d06c6ee428ad17e1

Gross D. 2013. Amazon's drone delivery: How would it work? CNN 2.12.2013. http://edition.cnn.com/2013/12/02/tech/innovation/amazon-drones-questions/

HäKe 2013. Hätäkeskusuudistuksen toteutuminen. Arviointiryhmän loppuraportti. Sisäasiainministeriön julkaisut 10/2013. ISBN 978-952-491-841-1.

HäKe 2016. Hätäkeskuslaitos http://www.112.fi/hatatilanne/uusi_tekniikka

Heino I. 2016. Yksityisyys ja luottamus älyliikenteen palveluissa. VTT, Espoo. 101 s. (vielä julkaisematon)

HSL 2015. HLJ 2015 Helsingin seudun liikennejärjestelmäsuunnitelma 2015. HSL:n julkaisuja 3/2015. ISSN 1798-6184, ISBN 978-952-253-249-7 (pdf). https://www.hsl.fi/sites/default/files/uploads/2015-03-03-hlj_2015-raportti.pdf

Hu Y.-C. 2003. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. Hu, Yih-Chun, Perrig, Adrian & Johnson, David B. ACM Workshop on Wireless Security (WiSe 2003), September 19.

Humphreys T.E., Ledvina B.M., Psiaki M.L., O'Hanlon B.W. & Kintner, Jr. P.M. 2008. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. Proceedings of the ION GNSS international technical meeting of the satellite division, Sept. 16, 2008. Vol. 55. 56 p.

Humpreys T. 2013. Secure Time. GPS Vulnerabilities and Implications for Telecom Thursday, February 7. https://www.atis.org/events/webinar-pptslides/GPSwebinar_020713.pdf

IEEE 2006. Enhancing security and privacy in traffic-monitoring systems. IEEE Pervasive Computing, Vol. 5, Issue 4. ISSN 1536-1268. 30.10.2006. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1717364

Innamaa S., Malin F. & Rämä P. 2015. Kilometriveron vaikutukset liikkumiseen. VTT Technology 227. VTT, Espoo. 62 s. + liitt. 45 s. ISBN 978-951-38-8321-8. http://www.vtt.fi/inf/pdf/technology/2015/T227.pdf

Inside GNSS 2009. What about GPS jamming and maritime safety, and linear carrier phase combinations? Available at: http://www.insidegnss.com/node/1122

Jafarnia-Jahromi A., Broumandan A., Nielsen J. & Lachapelle G. 2012. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. International Journal of Navigation and Observation, Vol. 2012, Article ID 127072, 16 p. http://dx.doi.org/10.1155/2012/127072

Jones S. 2014. Addressing cyber security risks. In: Security, Surveillance and Detection, edition 62: May 2014, pp. 194–195. http://www.porttechnology.org/images/uploads/technical_papers/SAMI.pdf

Karlof C. 2003. Secure routing in wireless sensor networks: attacks and countermeasures. Karlof, Chirs & Wagner, David. Ad Hoc Networks 1, 293–315.

Khoo B. 2011. RFID as an Enabler of the Internet of Things: Issues of Security and Privacy. IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6142169

Last D. 2010. The Effect of Jammers on GPS in a Maritime Environment. http://www.google.fi/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCAQFjAA&url=http%3A%2F%2Fwww.gps.gov%2Fgovernance%2Fadvisory%2Fmeetings%2F2010-10%2Flast.ppt&ei=Uqq3VLfGM6XkyAPemoK4Dw&usg=AFQjCNFtdYAx0VIKwQDQ34wi47w1T6x-oQ&sig2=MrQgk1eoOqxwCHav_ZXsRQ&bvm=bv.83640239,d.bGQ

LVM 2005. Mobiilimaailman tietoturvauhkat ja ratkaisut – Palvelunkehittäjän näkökulma. Luoti-julkaisuja 1/2005. ISBN 952-201-286-6, 952-201-287-4 (web).

LVM 2006. Tietoturvaopas sähköisen palvelun tarjoajalle. Luoti-julkaisuja 8/2006. ISBN 952-201-788-4 (painotuote), ISBN 952-201-789-2 (verkkojulkaisu).

http://www.lvm.fi/-/tietoturvaopas-sahkoisen-palvelun-tarjoajalle-luoti-ohjelma--825103

LVM 2011. Helsingin seudun ruuhkamaksu. Jatkoselvitys. LVM 5/2011. ISBN 978-952-243-214-8, URN: http://urn.fi/URN:ISBN:978-952-243-214-8

LVM 2013. Oikeudenmukaista ja älykästä liikennettä. Työryhmän loppuraportti. Liikenne- ja viestintäministeriön Julkaisuja 37/2013. ISBN 978-952-243-372-5.

Makkonen E. 2015. Vastaus sähköpostikyselyyn 14.10.2015.

Mikes 2015. Sähköverkon kolmivaihetehon ja sähkön laadun mittaukset. Uusi aikakausi sähkötehon mittauksiin. http://www.mikes.fi/s%C3%A4hk%C3%B6verkon-kolmivaihetehon-s%C3%A4hk%C3%B6n-laadun-mittaukset

Muio D. 2015. Driverless shuttles are hitting public roads in the Netherlands. Tech Insider 21.9.2015. http://www.techinsider.io/driverless-wepod-shuttle-is-coming-to-netherlands-2015-9

Newson P. & Krumm J. 2009. Hidden Markov Map Matching Through Noise and Sparseness. GIS '09 Proceedings of the 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems. Pp. 336–343.

Nieminen J.-M. 2011. Koneohjaus maanrakennustyössä. Opinnäytetyö. Lappeenrannan ammattikorkeakoulu, Lappeenranta. 40 s.

Ning H. 2011. Cyber-physical-social based security architecture for future internet of things. Huansheng Ning & Hong Liu. Advances in Internet of Things, 2012, 2, 1–7. http://file.scirp.org/Html/17031.html

NTP 2016. Network Time Protocol. https://en.wikipedia.org/wiki/Network_Time_Protocol

Nuss M. 2013. 1588 Precision Timing Protocol Saves LTE From GPS Jamming. Wired Innovation Insights. September 10. http://insights.wired.com/profiles/blogs/1588-saves-gps-jam#axzz3oXJUlGeG

Parker S. 2015. Sharper GPS needs even more accurate atomic clocks. The Conversation, August 3. http://theconversation.com/sharper-gps-needs-even-more-accurate-atomic-clocks-38109

PTP 2016. IEEE 1588 unplugged – An Introduction to IEEE 1588. http://www.rtaautomation.com/technologies/ieee-1588/

Pulkkinen K. 2005. Reitityksen ja tietoturvan sensoriverkon simulointiympäristölle asettamat vaatimukset. Pulkkinen Katja & Lehtonen Sami. Julkaisematon tutkimusraportti, VTT 12.12.2005.

Pusatec 2016. Puhelinkeskustelu Pusatec Oy:n edustajan kanssa 19.1.2016.

Riahi A. 2013. A systemic approach for IoT security. Arbia Riahi, Yacine Challal, Enrico Natalizio, Zied Chtourou & Abdelmadjid Bouabdallah. IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS), May 2013. ISBN 978-1-4799-0206-4. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6569455

Ruotsalainen L., Kuusniemi H., Zahidul H., Bhuiyan M., Söderholm S., Kirkko-Jaakkola M., Thombre S. & Honkala S. 2014. DETERJAM – Detection, analysis, and risk management of satellite navigation jamming (Satelliittipaikannuksen häirinnän tunnistaminen, analysointi ja riskinhallinta). Matine-julkaisuja 2014 / 2500M-006. ISSN 1797-3457.

ST 2015. ST Microelectronics. Protection of automotive electronics from electrical hazards, guidelines to for design and component selection. Application note AN2689.

Symmetricon 2013. Timing and Synchronization for LTE-TDD and LTE_Advanced mobile Networks. Symmetricon White Paper. https://www.aventasinc.com/whitepapers/WP-Timing-Sync-LTE-SEC.pdf

Talbot D. 2012. One Simple Trick Could Disable a City's 4G Phone Network. MIT Technology Review, 14.10.2012. https://www.technologyreview.com/s/507381/one-simple-trick-could-disable-a-citys-4g-phone-network/

Terndrup M. 2015. Long-Distance Jammer Is Taking Down Drones. Makezine, 16.10.2015. http://makezine.com/2015/10/16/research-company-takes-aim-uavs-portable-anti-drone-rifle/

Trafi 2012. Ilmailun navigaatio- ja valvontalaitejärjestelmien strategia Suomessa vuosille 2012–2030. 20.6.2012. Trafi, Helsinki.

Tuomaala M. 2013. Älykkään sähköverkon tietoliikenneratkaisut palveluntarjoajan näkökulmasta. Diplomityö. Vaasan yliopisto, Vaasa.

uBlox 2016. LEA-5 u-blox 5 GPS Modules Data Sheet. LEA-5x_DataSheet_(GPS.G5-MS5-07026).pdf, www.u-Blox.com. 19.1.2016.

Vastamaa I. 2012. Pelastustoimen operatiivisten viestiyhteyksien mallintaminen. Diplomityö. Kesäkuu 2012. 53 + 8 s. Tampereen teknillinen yliopisto, Tampere.

Viljasjärvi H. 2015. Vastaus Digitalle lähetettyyn kyselyyn GPS:n käytöstä lähetysverkoissa 16.10.2015.

von Bell C. 2015. Nokian Heren myynti varmistui. Uusi-Suomi, 9.12.2015. http://www.uusisuomi.fi/autot/149318-nokian-heren-myynti-varmistui

Yasin R. 2015. After GPS: The future of navigation. C4ISR&Networks, 31.3.2015. http://www.c4isrnet.com/story/military-tech/geoint/2015/03/31/gps-future-navigation/70730572/

Yle 2015. Ajopiirtureita huijaavat keksivät keinot – laitteen saa sekaisin magneetilla. Yleisradion liikenneuutinen 26.3.2015.

Zhao K. 2013. A survey on the internet of things security. Kai Zhao & Lina Ge. IEEE 9th International Conference on Computational Intelligence and Security (CIS). ISBN 978-1-4799-2548-3. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6746513

Julkaisun sarja ja numero

VTT Technology 253

Nimeke	**Liikenteen sähköisten palveluiden tietoturva – niihin kohdistuvat tietoturvariskit ja häirintämenetelmät sekä näiden vaikutukset ja ennaltaehkäisy**
Tekijä(t)	Sami Lehtonen, Ari Virtanen & Hanna Askola
Tiivistelmä	Satelliittipaikannukseen perustuvat liikenteen sähköiset palvelut, joissa hyödynnetään tietoja käyttäjän sijainnista, kulkuneuvosta ja matkoista, sisältävät monia tietoturvauhkia. Tässä raportissa käsitellään erityisesti suoriteperusteisen ajoneuvoverotuksen ja sen yhteydessä kuluttajille mahdollisesti tarjottavien lisäpalveluiden tietoturvaa. Riskejä on käsitelty viranomaisten, palveluntarjoajien ja kuluttajien näkökulmista. Viranomaisten kannalta tietoturvariskit liittyvät lähinnä vastuukysymyksiin ja kerätyn tiedon manipulointiin. Palveluntarjoajien riskit ovat tietovuotoja lukuun ottamatta pienet. Ajoneuvon mahdollisesti useat käyttäjät voivat kuitenkin hämärtää lisäpalveluiden hallinnassa esimerkiksi sitä, kuka käyttäjistä on antanut luvan paikannustietojen jatkokäyttöön. Kuluttajien kannalta mahdollisia riskejä liittyy niin yksityisyyden suojaan kuin verotietojen oikeellisuuteenkin. Raportissa annetaan myös suosituksia, joilla tunnistettuja tietoturvariskejä voi pienentää. Tällaisia ovat esimerkiksi kommunikaation salaus, ajoneuvolaitteen keräämien tietojen säännöllinen keruu toiminnan tarkistamista varten ja käyttäjien identiteettitietojen säilyttäminen erillään muista kerätyistä tiedoista. Suunnitelmat auto- ja ajoneuvoveron korvaamisesta käyttöön perustuvalla kilometriverolla ovat nostaneet keskustelunaiheeksi myös menetelmät vältellä tätä uudentyyppistä veroa. Kilometriveron määrittämiseksi ajoneuvoihin tulisi asentaa päätelaite, joka satelliittipaikannukseen perustuen mittaa ajetun matkan eri tariffialueilla. Ajoneuvolaite lähettäisi verotusta varten kerättyjä tietoja matkapuhelinverkon kautta taustajärjestelmän palvelintietokoneille. Tässä raportissa tarkastellaan erilaisia teknisiä keinoja manipuloida ajoneuvolaitetta ja keinoja estää manipulointiyritykset. Erityisesti raportissa käsitellään mahdollisuuksia häiritä satelliittipaikannusta. Väärinkäytösten tehokas estäminen edellyttää ajoneuvolaitteelta useita suojausta parantavia ominaisuuksia. Satelliittipaikannusta käytetään hyvin monilla eri alueilla yhteiskunnassa. Jos paikannuksen häirintälaitteet tilapäisesti yleistyisivät esimerkiksi veronkiertoyritysten vuoksi, sillä olisi vaikutuksia muuallakin kuin tieliikenteessä. Raportin jälkimmäisessä osiossa tarkastellaan satelliittipaikannuksen sovellusalueita ja häirintälaitteiden mahdollista vaikutusta niiden toimintaan. Häirinnällä voi vaikeuttaa tai hidastaa jopa yhteiskunnan turvallisuuskriittisten järjestelmien toimintaa, mutta niissä varajärjestelmät mahdollistavat toiminnan jatkamisen. Riskejä liittyy esimerkiksi aikakriittisten järjestelmien kellovirheisiin, koska satelliittipaikannuksen tarjoama tarkka aika on otettu laajasti käyttöön. Lukuisat laiva-, lento- ja tieliikenteen uudet palvelut perustuvat suoraan satelliittipaikannukseen. Näiden osalta häiriöriski on ilmeinen. Palveluiden suunnittelussa tulee huomioida paikannuksen varajärjestelmien käyttö sikäli kuin häiriöistä aiheutuisi merkittävää haittaa.
ISBN, ISSN, URN	ISBN 978-951-38-8406-2 (URL: http://www.vtt.fi/julkaisut) ISSN-L 2242-1211 ISSN 2242-122X (Verkkojulkaisu) http://urn.fi/URN:ISBN:978-951-38-8406-2
Julkaisuaika	Maaliskuu 2016
Kieli	Suomi, englanninkielinen tiivistelmä
Sivumäärä	57 s.
Projektin nimi	Liikenteen sähköiset palvelut -tutkimus
Rahoittajat	Tekes, Liikennevirasto, Trafi, LVM
Avainsanat	Liikenne, sähköiset palvelut, tietoturva
Julkaisija	Teknologian tutkimuskeskus VTT Oy PL 1000, 02044 VTT, puh. 020 722 111

Series title and number

VTT Technology 253

Title	**Information security in digital mobility services – security threats and data manipulation methods, influences and prevention**
Author(s)	Sami Lehtonen, Ari Virtanen & Hanna Askola
Abstract	New traffic services that are based on satellite positioning to identify the location, transport means and journeys of users pose a number of security threats. We review the security risks engendered by kilometre taxation and its accompanying traffic services. The risks are assessed from the viewpoint of the authorities, service providers and consumers. From the point of view of the authorities, their primary concern is liability and manipulation of data. Service providers consider the main risk to be data seepage, other risks being negligible. In some cases where several travellers are using the same vehicle, it could be tricky to identify which user granted permission for exploitation of location data. Consumers, for their part, identify privacy and taxation correctness as the main areas of concern. This report makes several recommendations to minimise recognised risks. Useful methods are communication encryption, regular checking of the data collection system, and a separate database of consumer identity information. Plans to replace the current taxation system with a kilometre tax scheme raises the question of how easy it would be to manipulate the system to avoid payment. The planned scheme would include an in-vehicle device that records the mileage driven in different tariff zones and sends the data at regular intervals to a back-end server system via the mobile phone network. Although technical means do exist with which to manipulate the in-vehicle device, countermeasures are also available to prevent it. We briefly review these methods, with special focus on satellite positioning jamming and spoofing technologies. Satellite positioning and timing services are widespread across different application areas. Should the use of jamming devices become widespread as a means of avoiding payment, the implications could reach beyond the road traffic scenario to critical systems in society. Our main findings show that the use of proper backup systems protects against total blackouts and allows for the continuation of operations. We look at the risks posed to time-critical systems that employ satellite-based precision timing. With numerous features of naval, air and road transport services being based increasingly on satellite positioning, the inherent risks of jamming are evident. In the planning of services, attention should be given to the use of backup positioning systems where disruption could cause significant harm.
ISBN, ISSN, URN	ISBN 978-951-38-8406-2 (URL: http://www.vttresearch.com/impact/publications) ISSN-L 2242-1211 ISSN 2242-122X (Online) http://urn.fi/URN:ISBN:978-951-38-8406-2
Date	March 2016
Language	Finnish, English abstract
Pages	57 p.
Name of the project	Liikenteen sähköiset palvelut -tutkimus
Commissioned by	Tekes, FTA, Trafi, MinTC
Keywords	Transport, digital services, security
Publisher	VTT Technical Research Centre of Finland Ltd P.O. Box 1000, FI-02044 VTT, Finland, Tel. 020 722 111

VTT TECHNOLOGY 253

Liikenteen sähköisten palveluiden...

Liikenteen sähköisten palveluiden tietoturva – niihin kohdistuvat tietoturvariskit ja häirintämenetelmät sekä näiden vaikutukset ja ennaltaehkäisy

Satelliittipaikannukseen perustuvat liikenteen sähköiset palvelut, joissa hyödynnetään tietoja käyttäjän sijainnista, kulkuneuvosta ja matkoista, sisältävät monia tietoturvauhkia. Tässä raportissa käsitellään erityisesti kilometriveron ja sen yhteydessä kuluttajille mahdollisesti tarjottavien lisäpalveluiden tietoturvaa. Riskejä on käsitelty viranomaisten, palveluntarjoajien ja kuluttajien näkökulmista.

Suunnitelmat auto- ja ajoneuvoveron korvaamisesta käyttöön perustuvalla kilometriverolla ovat nostaneet keskustelunaiheeksi myös menetelmät vältellä tätä uudentyyppistä veroa. Tässä raportissa tarkastellaan erilaisia teknisiä keinoja manipuloida ajoneuvolaitetta ja keinoja estää manipulointiyritykset. Erityisesti raportissa käsitellään mahdollisuuksia häiritä satelliittipaikannusta.

Satelliittipaikannusta käytetään hyvin monilla eri alueilla yhteiskunnassa. Jos paikannuksen häirintälaitteet tilapäisesti yleistyisivät esimerkiksi veronkiertoyritysten vuoksi, sillä olisi vaikutuksia muuallakin kuin tieliikenteessä. Raportin jälkimmäisessä osiossa tarkastellaan satelliittipaikannuksen sovellusalueita ja häirintälaitteiden mahdollista vaikutusta niiden toimintaan.

ISBN 978-951-38-8406-2 (URL: http://www.vtt.fi/julkaisut)
ISSN-L 2242-1211
ISSN 2242-122X (Verkkojulkaisu)
http://urn.fi/URN:ISBN:978-951-38-8406-2