MAANPUOLUSTUSKORKEAKOULU

ÄLYPUHELIMIEN PAIKKATIEDON MERKITYS OPERAATIO-TURVALLISUUDELLE

Kandidaatintutkielma

Kadetti
Miikka Nynäs

Merikadettikurssi 81
Laivasto- opintosuunta

Huhtikuu 2013

MAANPUOLUSTUSKORKEAKOULU

Kurssi Merikadettikurssi 81	Linja Laivasto- opintosuunta
Tekijä Kadetti Miikka Nynäs	
Tutkielman nimi **ÄLYPUHELIMIEN PAIKKATIEDON MERKITYS OPERAATIO-TURVALLISUUDELLE**	
Oppiaine, johon työ liittyy Sotatekniikka	Säilytyspaikka Kurssikirjasto (MPKK:n kirjasto)
Aika 28.3.2014	Tekstisivuja 21 Liitesivuja 4

TIIVISTELMÄ

Ihmisten omistamien älypuhelimien määrä, jotka kykenevät paikantamaan itsensä, on kasvanut huomattavasti. Myös älypuhelimien määrä puolustusvoimissa palvelevilla henkilöillä on kasvanut samalla. Tutkielmassa on tutkittu, mikä merkitys älypuhelimien paikkatiedolla on operaatioturvallisuudelle. Älypuhelimet tuottavat paikkatietoa satelliittipaikanmääritysmenetelmillä ja puhelinverkkoon perustuvilla paikanmääritysmenetelmillä.

Tutkimuskysymyksinä ovat:

- Miten älypuhelinten paikkatieto vaikuttaa operaatioturvallisuuteen?
- Mitä paikanmääritysmenetelmiä älypuhelimet käyttävät ja mihin tarkkuuteen niillä kyetään?
- Miten ulkopuolinen ihminen voi saada haltuunsa älypuhelinten tuottamaa paikkatietoa ja miten tämä tieto voi uhata operaatioturvallisuutta?

Tutkielman lähdeaineisto pohjautuu korkeakoulujen tutkimuksiin, kirjoihin ja eri lehtien internet-sivuihin. Älypuhelimien paikkatiedon merkityksestä operaatioturvallisuudelle ei ollut tehty aiempaa tutkimusta. Kuitenkin pitää huomioidan, että älypuhelimien paikkatietoa on hyödynnetty maalittamisessa.

Tutkielmassa päädyttiin lopputulokseen, että älypuhelimien paikkatiedon merkitys operaatioturvallisuudelle jää pieneksi, sillä älypuhelimen käyttäjä kykenee helposti estämään paikkatiedon jakamisen.

AVAINSANAT

Paikkatieto, Operaatioturvallisuus, Paikanmääritys

ÄLYPUHELIMIEN PAIKKATIEDON MERKITYS OPERAATIO-TURVALLISUUDELLE

SISÄLLYS

ÄLYPUHELINTEN PAIKKATIEDON MERKITYS OPERAATIOTURVALLISUUDELLE

1 JOHDANTO

Nykyään suurin osa suomalaisista omistaa älypuhelimen ja käyttää sitä. Älypuhelinten ominaisuuksiin kuuluu lähes poikkeuksetta kyky paikantaa itsensä käyttäen hyväksi esimerkiksi satelliittipaikanmääritysmenetelmiä GPS ja GLONASS, tukiasemapohjaista paikannusta ja WLAN-paikannusta. Puhelimen tuottamaa paikkatietoa voidaan myös jakaa muille ihmisille eri sovellusten kautta.

Nykyään varusmiehiä kielletään jakamasta paikkatietoa sosiaalisessa mediassa [1]. Paikkatiedon jakamista esim. Facebook-päivityksissä voi estää yksityisyys asetuksia säätämällä. Kuitenkin nämä asetukset voivat ajoittain muuttua itsestään. Lisäksi paikkatiedon jakamista on hankala valvoa.

1.1 Tutkimuskysymykset ja tutkimuksen tarkoitus

Älypuhelimien määrä myydyistä puhelimista arvioidaan olevan 90 % vuoteen 2014 mennessä [2]. Valtaosalla puolustusvoimien joukkoihin kuuluvista sotilaista on jonkinlainen älypuhelin. Mikäli älypuhelimien tuottama paikkatieto päätyy vihollisen haltuun, voi sen avulla seurata sotilaiden liikkeitä. Tutkielman tarkoituksena on selvittää, millä tavoin älypuhelimien tuottama paikkatieto voi uhata operaatioturvallisuutta.

Tutkimuskysymyksenä on: Miten älypuhelinten paikkatieto vaikuttaa operaatioturvallisuuteen. Apukysymyksinä on: Mitä paikanmääritysmenetelmiä älypuhelimet käyttävät ja mihin tarkkuuteen näillä kyetään, miten ulkopuolinen ihminen voi saada haltuunsa älypuhelimien tuottamaa paikkatietoa, sekä miten tämä tieto voi uhata operaatioturvallisuutta.

1.2 Tutkielman rajaus

Älypuhelinten paikanmääritysmenetelmien käytettävyydellä on suuria eroja riippuen siitä missä päin maailmaa niitä käytetään. Tämän takia tutkielma rajataan koskemaan Suomen puolustusvoimien toimintaympäristöä sotilaallisessa maanpuolustuksessa, eli alueena on käytännössä Suomen alue.

Lisäksi rajaan tutkielman koskemaan vain rauhan aikana tapahtuvaa toimintaa. Voidaan olettaa mm. Tshetshenian sodan kokemuksiin pohjautuen, että kriisitilanteissa matkapuhelinverkon toimintaa pyritään rajoittamaan. Tällöin on vaikeampaa arvioida, onko älypuhelimilla merkitystä operaatioturvallisuudelle.

1.3 Käsitteet ja määritelmät

Seuraavassa on esitetty tutkielman kannalta olennaiset käsitteet.

1.3.1 Älypuhelin

Älypuhelin on puhelin, jossa on yhdistettynä matkapuhelimen ja kämmentietokoneen ominaisuuksia. Älypuhelimissa on graafinen käyttöjärjestelmä, joka sallii yleensä sen, että kolmas osapuoli voi tehdä sovelluksia älypuhelimiin. Ne käyttävät myös 3G tai 4G-puhelinverkkoa mikä mahdollistaa nopean tiedonsiirron. [3]

Tutkielman kannalta olennaista sovelluksissa on se, että niillä älypuhelimen käyttäjä voi jakaa oman sijaintinsa muille saman sovelluksen käyttäjille. Tällainen sovellus on esimerkiksi Google Maps.

Älypuhelimet pystyvät tuottamaan paikkatietoa eri menetelmin kuten satelliittipaikanmääritysmenetelmillä, tukiasemapohjaisella menetelmällä ja WLAN-paikannuksella. Uusimmissa älypuhelimissa on käytössään kaksi satelliittipaikanmääritysmenetelmää: yhdysvaltalainen GPS ja venäläinen GLONASS. [4; 5; 6]

.

1.3.2 Paikkatieto

Paikkatieto on yhdistelmä tiedoista, jotka käsittelevät kohteen ominaisuuksia ja sijaintia. Paikkatieto on luokiteltua eli kohteella on tunnus, josta se kyetään tunnistamaan. Tämän lisäksi paikkatieto on rakenteellisesti järjestetty. Tässä tutkielmassa keskitytään paikkatiedon osalta eteenkin älypuhelinten tuottamaan sijaintitietoon.

1.3.3 Operaatioturvallisuus

Operaatioturvallisuus käsitetään Suomessa osaksi informaatio-operaatiota, jolla tuetaan puolustusvoimien operaatioita suojaamalla oman päätöksenteon edellytykset ja heikentämällä vastustajan tilannetietoisuutta ja tahtoa [7, s. 129]. Älypuhelinten tuottamatta paikkatieto voi vastustajalle päätyessään auttaa heitä luomaan tilannekuvaa, mikäli paikkatiedon perusteella kyetään tunnistamaan omat joukot.

1.4 Käytettävät lähteet

Tutkielma perustuu kirjallisuuskatsaukseen. Lähdemateriaalin muodostavat erilaiset artikkelit, opinnäytetyöt, kirjat ja internetsivut. Operaatioturvallisuutta käsittelevässä luvussa lähdemateriaali muodostuu Maanpuolustuskorkeakoulun tutkimuksista ja puolustusvoimien kirjallisuudesta. Paikanmääritysmenetelmiä käsittelevässä luvussa on hyödynnetty pääasiassa eri paikanmääritysmenetelmistä kertovia kirjoja ja artikkeleita, mutta mukana on myös muutamia internet-lähteitä. Paikkatiedon jakamista käsittelevä luvun lähdeaineisto muodostuu pääasiassa eri internet-lähteistä.

1.5 Dispositio

Toinen luku käsittelee operaatioturvallisuutta käsitteenä ja älypuhelimien merkitystä operaatioturvallisuudelle sotilastoiminnassa. Toisessa luvussa pyritään vastaamaan kysymykseen, mikä merkitys älypuhelimella on operaatioturvallisuudelle.

Kolmannessa luvussa on esitettynä älypuhelimien käyttämät paikanmääritysmenetelmät. Luvun tarkoitus on vastata kysymykseen: Mitä paikanmääritysmenetelmiä älypuhelimet käyttävät ja mihin tarkkuuteen näillä kyetään? Paikanmääritysmenetelmistä on esitetty niiden toimintatapa ja niihin liittyvät rajoitteet?

Neljäs luku keskittyy käsittelemään erilaisia tapoja, joilla älypuhelimien paikkatieto siirtyy älypuhelimista, muiden ihmisten käyttöön. Johtopäätösluvussa tehdään yhteenveto tutkielmassa käsitellyistä asioista. Sen tavoitteena on myös arvioida kunkin uhkan vaikuttavuutta älypuhelimen paikkatiedon tietosuojaan.

Sen lisäksi siinä pohditaan mitä hyötyä älypuhelimista voisi olla puolustusvoimien toiminnalle. Viimeisenä johtopäätösluvussa esitellään tutkijan omia ideoita mahdollisiksi tuleviksi tutkimuskohteiksi.

2 OPERAATIOTURVALLISUUS

Pääesikunnan suunnitteluosasto määrittelee operaatioturvallisuuden seuraavasti ”Operaatioturvallisuus on operatiivisen toiminnan kannalta kriittisen tietojen ja tavoitteiden määrittämistä sekä käytettävyyden ja saatavuuden turvaamista oman päätöksenteon tukena sekä niiden paljastumisen estämistä vastustajalle. Yleisesti kriittiseen tietoon voidaan lukea kuuluvaksi tilannekuvaan, operatiivisiin suunnitelmiin sekä puolustusjärjestelmän keskeisiin osiin liittyvät tiedot.” [7]

Operatiivisella tasolla operaatioturvallisuus käsitetään operaatioihin liittyvien tietojen turvaamisena. Taktisella tasolla operaatioturvallisuus puolestaan on yksittäiseen sotilaaseen kohdistuvaa kriittisen tiedon turvaamista. Tällainen tieto voi johtaa pahimmillaan sotilaan omaan tai hänen palvelustoverinsa hengenmenetykseen. Mahdollisia ovat myös toiminnan kannalta merkittävät kalustotappiot.[7, s.131]

Mika Huttunen käsittelee kirjassaan Monimutkainen taktiikka turvallisuutta osana sodankäynnin yleisiä periaatteita. Tietoturvallisuudella on suuri merkitys yllätyksen ja harhautuksen toteutuksessa, sillä vastustaja pitää tuntea, jotta kykenee suunnittelemaan yllätyksen ja harhautuksen. Turvallisuudella pyritään myös suojaamaan omat joukot vihollisen tekemältä yllätykseltä ja harhautukselta. [8, s.144]

Operaatioturvallisuus voidaan ymmärtää eräänlaisena tiedustelun vastatoimena. Operaatioturvallisuutta kohottavien toimenpiteiden tarkoituksena on estää vastustajan tiedustelua hankkimasta tietoa omista joukoista. Parhaimmillaan operaatioturvallisuutta edistävillä toimenpiteillä pakotetaan vastustajan komentajat tekemään vääriä päätöksiä väärään tai puutteelliseen tietoon pohjautuen.

2.1 Tilannekuva ja paikkatieto

Sotilasjoukon johtamisen kannalta on oleellista muodostaa tilannekuva ja tilannetietoisuus omista ja vastustajan joukoista. Kaikki päätökset perustuvat joukon tai organisaation johdon tilannekuvaan. Tilannekuvan muodostaa tieto:

- joukkojen sijainnista ja määrästä
- huoltotarpeesta
- toimintamahdollisuuksista

- tulevasta toiminnasta

Nykyaikaisessa sodankäynnissä, missä pieniä joukkoja käytetään laajoilla alueilla, paikkatiedon merkitys kasvaa. Liikkuvuus on oleellista ja tilanteet muuttuvat tiheään. Paikkatietoa voidaan käyttää mm.
- tilannekuvan luomiseen ja ylläpitoon
- operaatioiden suunnitteluun ja johtamiseen
- kouluttamiseen
- toimintamahdollisuuksien sekä voimasuhteiden kartoittamiseen.[9]

Yhdysvalloissa operaatioturvallisuus on prosessi, jolla tunnistetaan vihollisen haluama omien operaatioiden kriittinen tieto ja jolla analysoidaan operaatioihin liittyviä tekijöitä. Tämän tarkoituksena on: Tunnistaa asiat, jotka vastustajan tiedustelu voi havaita. Määrittää mistä indikaattoreista vihollinen voi kerätä tietoa. Valita ja kehittää vastatoimenpiteitä omaan käyttöön, jolla voidaan pitää haavoittuvuudet hyväksyttävällä tasolla.[9]

Omien sekä joukkojen paikantamisen ja toiminnan ennakoimisen merkitys on tilannekuvan luomisen kannalta ratkaisevaa. Tilannetietoisuuden avulla päätökset perustuvat olemassa olevaan tilanteeseen ja uusimpiin tiedustelutietoihin[10, s.59]. Rauhan aikana Puolustusvoimien toiminnasta älypuhelimien paikkatien avulla kerättyä tietoa voidaan lähinnä pitää tiedustelutietona. Tosin se voi myös paljastaa vastustajalle tietoa Puolustusvoimien rauhan ajan operatiivisesta toiminnasta. Esimerkiksi Merivoimien aluksien sijainteja voidaan saada selville, vaikka ne olisivat tutkilta suojassa saaristossa ja säteilynhallinnan keinoin niiden havaittavuutta elektronisen sodankäynnin keinoin olisi pienennetty. Tähän paikantamiseen voitaisiin käyttää hyväksi esimerkiksi tiedustelualukseen sijoitettua matkapuhelinverkon valetukiasemaa, johon aluksella oleva puhelin ottaisi yhteyden.

Tämä edellyttäisi sellaisen puhelimen paikantamista, jonka tiedetään olevan aluksella. Tällaisena puhelimena voidaan pitää esimerkiksi aluksen henkilöstön kuten päällikön puhelinta tai aluksen omaa puhelinta. Kuitenkin esimerkiksi valetukiasemaan liittyneet puhelimet ja niiden käyttäjät pitää kyetä tunnistamaan, jotta tiedustelutietoa voitaisiin käyttää hyväksi sotilasjoukkojen paikantamiseen. Matkapuhelimien signaalit ovat havaittavissa signaalitiedustelujärjestelmillä, mutta yksittäisten matkapuhelimien tunnistaminen on vaikeaa pelkän signaalin avulla, sillä samanaikaisesti havaitaan todennäköisesti useita lähes samanlaisia puhelimia.

Vuonna 2008 Israelin puolustusvoimat toteutti operaation Valettu lyijy. Sen tarkoituksena oli lopettaa rakettien ampuminen Gazan kaistalta Israeliin ja estää lisäaseistuksen saapuminen Gazaan. Operaatiota edelsi huolella toteutettu tiedustelu ja valmisteluvaihe tärkeiden kohteiden maalittamiseksi. Hankitun tiedon perusteella Israelin ilmavoimat pystyi tuhoamaan operaation ensimmäisillä iskuilla merkittävän osan Hamasin johtoportaasta. Operaatiossa oli onnistuttu hankkimaan tietoa Hamasin johtajista käyttäen hyväksi mm. henkilökohtaisten tietokoneiden ja puhelimien tiedustelua. Israelilaisten tiedustelulla oli halussa jopa heidän nimensä valokuvansa ja osoitteensa. Tämä osoittaa, että sotilaskäyttöä varten tiedustelua kyetään hankkimaan myös tiedustelemalla yksityisten henkilöiden henkilökohtaisia elektronisia laitteita, joihin älypuhelimet kuuluvat tietokoneiden ohella. Ovaska pitää tutkimuksessaan mahdollisena, että kohteena olevien henkilöiden puhelimien ja tietokoneiden tiedustelua voidaan käyttää myös uusien kohteiden löytämiseen. [11]

2.2 Elektroninen sodankäynti

Elektroninen tuki on osa elektronista sodankäyntiä. Elektronisen tuki tarkoittaa elektronisen toiminnan paikallistamista taistelukentällä passiivisella tiedustelulla. Elektronisen tuen päämääriä ovat mm.:

- vihollisen toiminta-alueella olevien joukkojen paikantaminen
- arvioidun tulevan toiminnan selvittäminen.
- mahdollisesti myös maalinosoitukseen [12; 13, s68]

Signaalitiedustelu (SIGINT, Signals Intelligence) on strategiseen tiedusteluun kuuluvaa vastustajan sähkömagneettisten lähetteiden tiedustelua. Signaalitiedusteluun kuuluvat elektroninen viestitiedustelu (COMINT, Communications Intelligence) ja elektroninen mittaustiedustelu (ELINT, Electronic Intelligence). COMINT keskittyy viestijärjestelmien tiedusteluun ja ELINT tutkiin ja muihin järjestelmiin. [13, s67-68]

Signaalitiedustelua voidaan suorittaa maalla olevista asemista, merellä olevista tiedustelualuksista ja tiedustelulentokoneista käsin. Signaalitiedustelua käytetään sodan ajan lisäksi jo rauhan aikana, joten se tulee huomioida jo rauhan ajan toiminnassa. Signaalitiedustelu voi kohdistua:

- Järjestelmien testausten ja kenttäkokeiden tiedusteluun
- Joukkojen koulutuksen ja sotaharjoitusten tiedusteluun

- Joukkojen perustamis- ja ryhmittymisvaiheen tiedusteluun
- Joukkojen perustamisen jälkeisen koulutuksen ja harjoittelun tiedusteluun. [13, s68]

Tshetshenian sodassa Venäjän armeijan signaalitiedustelun kohteeksi päätyi myös matkapuhelimia, sillä tshetsenialaiset joukot käyttivät niitä sodan edetessä pienissä määrin johtamisviestinnässä ensimmäisessä Tshetshenian sodassa. Tällöin tosin ei ollut käytössä vielä nykyaikaisia älypuhelimia ja hankittu tiedustelutieto pohjautui enemmänkin puhelinkeskustelujen sisältöön, kuin puhelinten paikantamiseen niiden signaalien perusteella. [13, s.113] Kuitenkin tämä osoittaa, että puhelimien varomattomalla käytöllä voi olla haitallista vaikutusta operaatioiden turvallisuudelle.

3 PAIKANMÄRITYSMENETELMÄT

Älypuhelimet tarvitsevat paikkatiedon tuottamiseen paikanmääritysmenetelmän. Älypuhelimien käyttämiä menetelmiä ovat satelliittipaikanmääritys, lähiverkkopaikannus ja tukiasemapohjainen paikannus. Tutkielman kannalta on oleellista, millaiseen tarkkuuteen kyetään milläkin paikanmääritysmenetelmällä eri olosuhteissa ja mitä rajoitteita eri paikantamismenetelmiin liittyy.

Satelliittipaikanmääritysmenetelmät kykenevät parempaan tarkkuuteen kauempana kaupunkien keskustoista ja rakennetuilta alueilta. Verkkoon pohjautuvat paikanmääritysmenetelmät ovat puolestaan tarkempia kaupungeissa [14, s.14].

Taulukko 1. Paikanmääritysmenetelmien tarkkuus.

Paikanmääritysmenetelmä	tarkkuus
Satelliittipaikanmääritysmenetelmät	
GPS	Tukipalveluiden avulla jopa 1m
GLONASS	Nimellinen 50-70m vaaka 70m pysty. Todellisuudessa tarkempi
Puhelinverkon paikannusmenetelmät	
Solupaikannus	300-500m. Kaupungeissa parempi kuin harvaan asutulla alueella.
Saapumiskulman mittaus	0,1-2km
Korrelaatiopaikannus	30-50m
WLAN paikannus	Jopa 2m. Tukiasemien tiheys vaikuttaa suuresti

3.1 Satelliittipaikanmääritys menetelmät

Älypuhelimissa satelliittipaikanmääritysmenetelminä toimivat yhdysvaltalainen GPS ja venäläinen GLONASS paikanmääritysmenetelmä. Näitä paikanmääritysmenetelmiä on käytetty puhelimissa jo yli 10-vuoden ajan, mutta niihin on tehty viimevuosina parannuksia, jotka parantavat paikannuksen käytettävyyttä. Tällainen parannus on mm. paikannuksen nopeutta parantava A-GPS järjestelmä. Vanhemmat puhelimet sisältävät yleensä vain GPS-paikannuksen, mutta uusimmissa on alettu käyttää rinnalla myös GLONASS-paikannusta.

Toimintatavoiltaan nämä satelliittipaikanmääritysmenetelmät muistuttavat paljolti toisiaan [15, s26]. Älypuhelimien satelliittipaikannusominaisuuden käyttö on puhelimen käyttäjän ohjattavissa. Esimerkiksi iPhone, Android ja Windows-phone älypuhelimissa käyttäjä kykenee yksinkertaisilla toimenpiteillä kytkemään paikannuksen pois päältä.

Satelliittipaikanmääritys perustuu etäisyyden mittaamiseen. Tiedetään, että satelliitin lähettämä signaali kulkee valonnopeudella. Tällöin satelliitin etäisyys paikantavasta laitteesta voidaan määrittää signaalin käyttämän kulkuajan perusteella.[15]

Satelliittipaikannusjärjestelmät muodostuvat neljästä eri lohkosta, joita ovat seuranta-, avaruus-, vastaanotinlohko ja tukipalvelut. Kaikille satelliittipaikannusjärjestelmille on yhteistä näiden lohkojen olemassa olo. Lohkoilla on omat tehtävänsä satelliittipaikannuspalvelun tuottamisessa ja niillä on myös omat haavoittuvuutensa, mitkä voivat olla syynä satelliittipaikannuksen epätarkkuuteen. [16]

Seurantalohkon tarkoituksena on satelliittien ratojen seuranta. Seurantalohkon kautta ohjelmoidaan satelliittien päälläolo ja satelliittien muut toiminnot kuten satelliittikello. Seurantalohkon haavoittuvuutena on mahdollinen väärän rata- ja seurantatiedon lataus. Ne ovat myös alttiina mahdolliselle terrorismille ja kyberiskuille. Avaruuslohko muodostuu satelliiteista. Ne toimivat paikannuksen tukipisteverkkona. Avaruuslohkon luotettavuutta heikentävät satelliittien liian vähäinen määrä (satelliitteja alle 24kpl), laitteiston mahdollinen vikaantuminen ja toimintahäiriöt. Myös signaalinmuodostuksessa voi olla häiriöitä. Auringon aiheuttamat magneettimyrskyt voivat aiheuttaa katkoksia palveluun, sillä ilmakehä ei tarjoa satelliiteille suojaa Auringon toiminnalta. [16]

Vastaanotinlohko muodostuu maassa olevista paikannuslaitteista. Niiden tehtävänä on paikantaminen satelliittisignaalin perusteella. Vastaanotinlohkon haavoittuvuudet liittyvät signaalin häiriöihin sekä laitteiston toimimattomuuksiin. Erityisen tärkeää on, että vastaanottimen kello pysyy oikeassa ajassa. Tukipalvelut tuottavat differentiaalipalvelua paikannuksen tarkkuuden parantamiseksi. Tästä esimerkkinä on mm. DGPS, jota ei tosin käytetä puhelimessa, sillä se tarvitsisi oman vastaanottimensa. Tukipalveluiden avulla paikannustarkkuus voi olla jopa 1m. [16]

Satelliittipaikanmääritysmenetelmien tarkkuus on suurempi erämaissa kuin kaupunkien keskustoissa [14]. Kaupunkiympäristössä satelliittipaikannusta heikentää rakennuksista

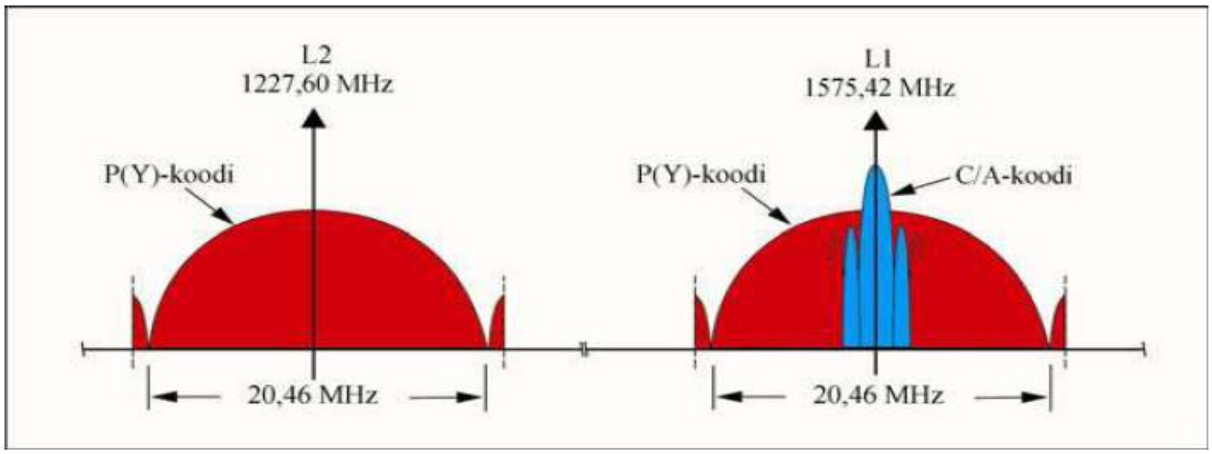
aiheutuvat heijastukset. Sisätiloissa satelliittipaikanmääritys ei yleensä toimi. Satelliittien lähettämät signaalit eivät tavoita sisällä olevia paikanmäärityslaitteita elleivät ne ole ovien tai ikkunoiden läheisyydessä. Niiden selvänä etuna muihin älypuhelinten paikanmääritysmenetelmiin on niiden tarkkuus ja kyky toimia missä tahansa maailmalla. Ainoastaan pohjoisimmilla ja eteläisimmillä leveysasteilla esiintyy merkittävää epätarkkuutta GPS-paikanmääritystä käytettäessä, mutta GLONASS toimii myös napa-alueilla. Suomen alueella tällä ei ole merkitystä.

3.1.1 GPS

Global Positioning System eli GPS on lähes kaikkialla maapallolla toimiva satelliittipaikanmääritysmenetelmä. Ensimmäinen GPS-satelliitti on laukaistu 1978 [15, s.19]. Tällä hetkellä GPS on maailman käytetyin satelliittipaikanmääritysmenetelmä.

GPS-paikanmääritys perustuu passiiviseen etäisyyden mittaamiseen. Paikanmäärityslaite paikantaa itsensä kolmiomittauksen tapaan kuuntelemalla eri satelliiteista tulevia signaaleja. Varsinaisen paikanmäärityksen suorittaa signaalin vastaanottava laite [17, s. 118] GPS:n päätavoitteena on tuottaa tieto sijainnista, nopeudesta ja ajasta sotilaskäyttöön. Sen lisäksi palvelua tarjotaan myös siviileille. Tästä johtuen GPS:ssa on kaksi eri palvelua: PPS (Precise Positioning Service) sotilas- ja viranomaiskäyttöön, sekä SPS (Standard Positioning Service) siviilikäyttöön. Vuoteen 2000 SPS palvelua heikennettiin tahallisesti [15, s.19].

GPS-singaalia lähetetään kahdella eri kantoaaltotaajuudella. Näitä merkitään kirjaimin L1 (1575,42 MHz) ja L2 (1227,60 MHz). L2 taajuutta käytetään lähinnä sotilas- ja viranomaiskäyttöön tarkoitetussa PPS palvelussa. GPS-satelliittien ratakorkeus on noin 20200 km ja inklinaatio 55 astetta [16].



Kuva 1. GPS-spektri [16]

Matkapuhelimia varten on kehitetty A-GPS järjestelmä (Assisted GPS). Sen tarkoitus on helpottaa ja nopeuttaa matkapuhelimen GPS-paikannusta. A-GPS järjestelmää käytettäessä puhelimelle annetaan tieto, mitä satelliitteja kannattaa seurata paikannuksessa. Tieto tulee tarkoitusta varten rakennetulta avustavalta palvelimelta ja se välitetään matkapuhelinverkon kautta. Tieto perustuu matkapuhelinverkon perusteella tapahtuvaan paikannukseen. Ilman avustusta GPS:ää käyttävä puhelin joutuu etsimään kaikki satelliitit ja valitsemaan niistä paikannukseen sopivat, jolloin paikannus hidastuu.[18]

3.1.2 GLONASS

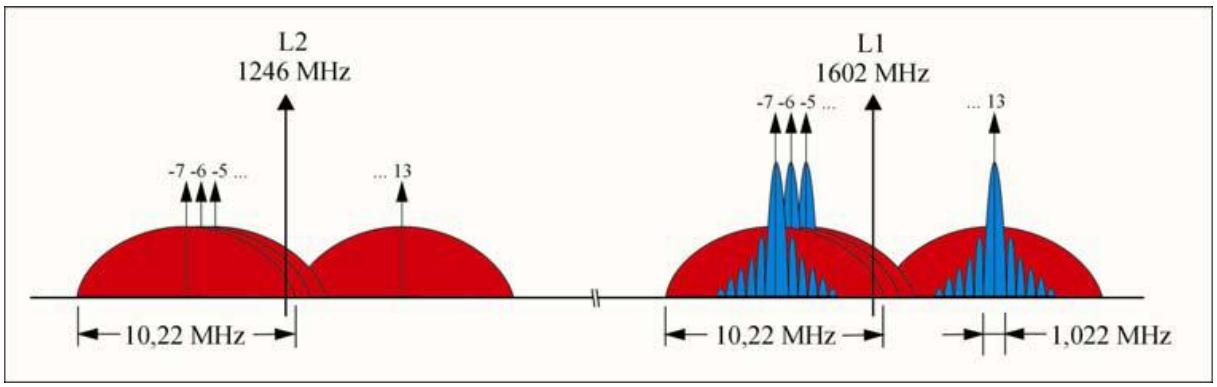
GLONASS (Global'naya Navigatsionnaya Sputnikowaya Sistema, Global Navigation Satellite System) on venäläinen satelliittipaikanmääritysjärjestelmä. Mm. Applen, Samsungin ja Nokian kalleimmat älypuhelimet on varustettu kyvyllä käyttää GLONASS-paikanmääritystä. Ensimmäistä kertaa GLONASS-paikanmääritystä käyttävä puhelin tuli myyntiin huhtikuussa vuonna 2011[19].

GLONASS muistuttaa hyvin paljon GPS-järjestelmää toiminnaltaan. Järjestelmän ensimmäinen satelliitti laukaistiin vuonna 1982, mutta vuosien 1982-1985 kokeiluvaiheen jälkeen satelliittien määrä kasvoi hitaasti. Vuosina 1994-1995 laukaistiin 18 satelliittia, mikä nosti satelliittien kokonaismäärän 24 satelliittiin. Määrä kuitenkin putosi nopeasti seuraavina vuosina satelliittien lyhyestä eliniästä johtuen, joka oli ennen laskennallisesti kolme vuotta. GPS-satelliitit ovat pitkään kestäneet käytössä yli kymmenen vuoden ajan. [15]

Vuonna 2014 GLONASS-satelliitteja on yhteensä 28 kappaletta avaruudessa, joista 24 on operatiivisessa toiminnassa. Kolme satelliittia on reservinä operatiivisille satelliiteille ja yhdellä satelliitilla on meneillään testaus. Kaikki nykyiset satelliitit on laukaistu vuoden 2005 jälkeen. Operatiivisista satelliiteista vanhimmat ovat iältään jo yli seitsemänvuotiaita ja vanhin reservissä oleva satelliitti on ollut avaruudessa jo lähes yhdeksän vuotta. Operatiivisista satelliiteista alle kolmen vuoden ikäisiä on vain viis kappaletta, joten GLONASS-satelliittien käyttöikä on kasvanut selvästi entisestä.[20]

GLONASS järjestelmään kuuluu GPS:n tavoin hallintasegmentti eli maa-asemat, avaruussegmentti, jonka muodostaa paikannussatelliitit ja käyttäjäsegmentti, joka muodostuu

loppukäyttäjien hallussa olevista paikannuslaitteista. GLONASS:n signaali muistuttaa ominaisuuksiltaan hyvin paljon GPS:n signaalia. Tosin GLONASS järjestelmässä satelliitit erotellaan toisistaan lähetystaajuuden, ei koodin, perusteella. Järjestelmässä perustaajuuksina ovat L1 1602 MHz ja L2 1246 MHZ. L1 taajuudella satelliittien välinen poikkeavuus on 562,5 KHz ja L2 taajuudella 537,5 KHz [15]. Satelliittien ratakorkeus on GLONASS-järjestelmässä 19100 km ja inklinaatio 64,8 astetta, mikä tuo sille GPS-järjestelmää paremman tarkkuuden lähellä napa-alueita, mutta tällä ei ole merkitystä Suomen alueella [16].



Kuva 2. GLONASS-signaalin spektri. [16]

GLONASS:n nimellinen tarkkuus on vaakatasossa 50-70m ja pystytasossa n. 70m. Todellisuudessa järjestelmän tarkkuus on suurempi, mutta vähäisestä käyttökokemuksesta johtuen tarkempaa tietoa ei ole.

3.2 Matkapuhelinverkkoon perustuva paikannus

Matkapuhelimen paikannus voidaan suorittaa myös matkapuhelinverkkoon perustuvana paikannuksena. Suomessa kaikki operaattorit tukevat matkapuhelimien puhelinverkkoon perustuvaa paikannusta mm. hätäpuheluiden vuoksi [14].

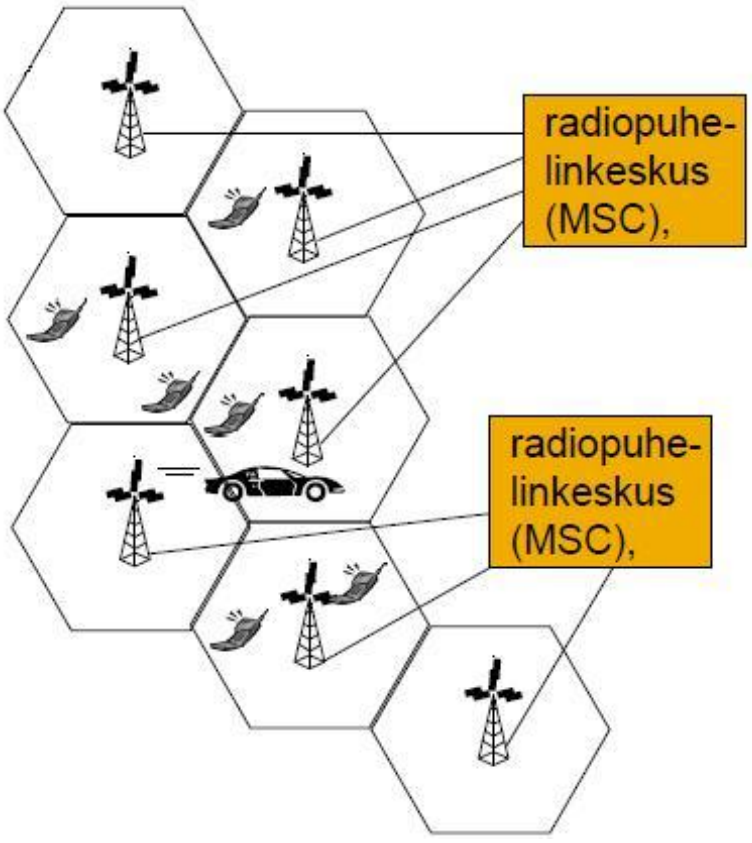
Suomessa Kajaanin eteläpuolella Elisan 3G-verkon kuuluvuusalue kattaa lähes kokonaan maa-alueet. Itäsuomessa lähellä valtakunnan rajaa on hieman laajempia alueita, joita verkko kata. Lapissa 3G-verkko kattaa lähinnä teiden varret ja suurimmat asutusalueet, mutta katvealueita esiintyy runsaasti. Tämän lisäksi verkko kantaa suurimmaksi osaksi myös sisäisten aluevesien rajalle saakka.[21]

2G-verkko kattaa Oulun eteläpuolella käytännössä koko maan. Lapissa 2G-verkon kattavuus on suurempi kuin 3G-verkon, mutta katvealueita suuria esiintyy myös 2G-verkossa [21]. 2G-

verkoissa toimivat lähes samat paikannusmenetelmät kuin 3G-verkossa, mutta tiedonsiirto ei ole niin nopeaa. Tämä saattaa vaikuttaa paikkatiedon jakamiseen eri sovellusten kautta. Elisan ja Sonera 2G- ja 3G-verkkojen kuuluvuusalueet on esitettynä tämän tutkielman liitteissä.

3.2.1 GSM-verkko

GSM-verkko on soluverkko. Se muodostuu useista tukiasemista, eli soluista, joiden avulla puhelimet viestivät keskenään. Kukin tukiasema on varustettu lähetin-vastaanotin komponentilla, mikä mahdollistaa saman tukiaseman käyttämiseen kokonaisuudessaan puheluiden ja viestien välittämiseen. Matkapuhelimen välittämä puhelu tai tekstiviesti kulkee puhelimelta siihen soluun, jonka alueella puhelin on [22]. Soluverkon eri solut ovat liittyneet toisiinsa MSC:n (Mobile Swichin Center) kautta. Sen tehtävänä on hallinnoida sekä puhelun muodostusta verkossa, että tilaajan liikkumista [23].



Kuva 3. Soluverkon toiminta [23]

3.2.2 Solupaikannus

Solupaikannus tapahtuu yksinkertaisesti määrittämällä minkä solun eli tukiaseman alueella puhelin on. Tukiaseman sijainti on tarkasti tiedossa ja tämän lisäksi tunnetaan myös melko tarkasti tukiaseman kuuluvuus alue. Solun kuuluvuusalueeseen vaikuttavat mm. antennien suuntaus, lähetysteho ja maastonmuodot. Tukiasemaa käyttävä puhelin on siis kyseisen tukiaseman kuuluvuusalueella. Solupaikannuksen tarkkuutta voidaan parantaa laskemalla signaalin kulkuaika puhelimen ja tukiaseman välillä ns. TA eli Time Advance tekniikalla [24]. Solupaikannuksen tarkkuus on solun koosta riippuen 2G-verkossa 300-500m [25]. Solujen koot vaihtelevat solun tarkoituksen mukaan välillä 50m-35km [23].

3.2.3 Saapumiskulman mittaus

Paikannus puhelinverkossa on mahdollista tehdä mittaamalla puhelimen signaalin saapumiskulma tukiasemalle. Mittaamiseen vaaditaan vähintään kaksi tukiasemaa. Järjestelmän tarkkuus vaihtelee 100 metristä 2 kilometriin. Vaihtelevuus on suuri, sillä paikannusmenetelmä on herkkä virheille. Virheitä syntyy mm. silloin, kun puhelimen signaali kulkee tukiasemalle heijastusten kautta. [24]

3.2.4 Aikaeropaikannus

Matkapuhelinverkon tekniikka voisi mahdollistaa myös aikaeromittauksella tapahtuvan paikannuksen. Aikaeropaikannuksessa signaaliin tulisi lisätä mittausyksiköt (Location Measurement Unit), jolla puhelimen sijainti lasketaan. Tätä ei kuitenkaan hyödynnetä vanhemmissa puhelinverkoissa, sillä se vaatisi lisäinvestointeja, eikä vanhojen puhelimien tekniikka kykenisi ilman ohjelmistopäivitystä hyödyntämään tätä paikannusmenetelmää. 3G-verkossa kyettäisiin hyödyntämään aikaeropaikannusta, jossa tukiasemien kuuluvuutta parannetaan toisia tukiasemia hetkellisesti heikentämällä. Yhdysvalloissa ei kuitenkaan aikaeropaikannuksen tarkkuus riitä hätäpuheluiden paikannukseen. Euroopassa kyseistä menetelmää ei hyödynnetä. [26]

3.2.5 Korrelaatiopaikannus

Puhelinverkossa tapahtuvan paikannuksen tarkin menetelmä on korrelaatiopaikannus. Sen käytettävyys on parhaimmillaan kaupunkien keskustoissa. Paikannuksen tarkkuus on n. 30-50 metriä. Korrelaatiopaikannuksessa tukiasemalle tulevaa puhelimen signaalia verrataan

tietokantoihin. Ne voivat sisältää tietoa signaalin voimakkuuksista, kulkuajoista ja muuta signaaliin liittyvää tietoa.

3.3 WLAN-paikannus

Langattomassa lähiverkossa voidaan hyödyntää korrelaatiopaikannusta. Sen tarkkuus on parhaimmillaan 2m, mutta paikannuksen tarkkuuteen vaikuttaa oleellisesti saatavilla olevien tukiasemien määrä [26, s.8]. Langattomia lähiverkkoja paikannuksessa hyödyntävät monet nykyaikaiset älypuhelimet. Puhelimissa on kuitenkin usein mahdollisuus valita, käyttääkö se langattomia lähiverkkoja hyväksi paikannuksessa.

Puolustusvoimien toiminta-alueilla langattomien verkkojen määrä on usein hyvin rajallinen. Kuitenkin kaupunkiympäristössä esiintyy runsaasti langattomia verkkoyhteyksiä, mikä pitää huomioida asutuskeskuksissa toimittaessa. Rakennetun ympäristön kannalta merkittävä etu langattomissa lähiverkoissa satelliittiperusteiseen paikantamiseen nähden on niiden kyky paikantaa sisätiloissa olevia laitteita, mikäli tukiasemia on saatavilla. Tämä tarkoittaa sitä, että puhelimen sijainti saatetaan tuntea puhelinverkkopaikannukseen verrattuna melko tarkkaan, vaikka sisätiloissa oleminen estäisi satelliittipaikannusjärjestelmien käytön. Useimmista puhelimista voidaan kuitenkin helposti kytkeä WLAN-verkon käyttö pois päältä.

4 PAIKKATIEDON JAKAMINEN

Älypuhelinten tuottama paikkatieto voi olla muiden ihmisten käytettävissä puhelimen käyttäjän tahtomatta [27]. Älypuhelinten paikkatieto voi päätyä muille tahoille kuin älypuhelinten käyttäjille useilla eri tavoilla. Laitteiden valmistajat keräävät käyttöehtosopimusten mukaan älypuhelinten paikkatietoa tunnistamattomassa muodossa laitteiden ja palveluiden kehittämistä varten. Puhelinoperaattorit kykenevät seuraamaan heidän verkossaan olevaa puhelinta. Jotkin kolmannen osapuolten tekemät sovellukset on tarkoitettu paikkatiedon jakamiseen muille ihmisille. Tämän lisäksi joidenkin sovellusten tarkoituksena on toimia vakoiluohjelmina, jotka mahdollistavat puhelimen vakoilun sovelluksen tuottajan toimesta.

4.1 Puhelinoperaattoreiden keräämä paikkatieto

Puhelimen käyttäjää kyetään seuraamaan hänen tietämättään. Puhelinoperaattorit pystyvät keräämään puhelimen käyttäjän sijaintitietoa ja tallentamaan tiedon erittäin tarkasti muistiin. Esimerkiksi saksalaisen kunnallispoliitikon puhelinkäyttäytymisestä operaattorilla oli erittäin tarkat tallenteet, joista selviää mm. puhelimen käyttäjän sijaintihistoria [28].

Puhelinoperaattorin keräämä tieto puhelimesta on myös valtioiden käytettävissä, mikäli lainsäädäntö mahdollistaa sen. Yhdysvalloissa puhelinoperaattori Verizon velvoitettiin luovuttamaan tietonsa Yhdysvaltojen kansalliselle turvallisuuspalvelulle NSA:lle [29]. Itärajan lähistöllä suomalaisten puhelimet saattavat hypätä venäläisen operaattorin puhelinverkkoon, kun puhelimissa on päällä automaattinen verkkohaku [30]. Tällöin venäläiset operaattorit kykenevät keräämään suomalaisten puhelinten paikkatietoa. Paikkatieto voisi olla myös Venäjän viranomaisten saavutettavissa, jolloin sitä pystyttäisiin mahdollisesti käyttämään tiedustelutietona.

Solupaikannusta käytettäessä, myös tukiasema kykenee tunnistamaan, mitkä puhelimet ovat liittyneenä siihen. Puhelimet lähettävät tukiasemalle IMEI-numeronsa ja SIM-kortin tunnistetiedon. IMEI-numero on aikoinaan otettu käyttöön, jotta voitaisiin jäljittää varastettu puhelin vaikka siihen vaihdettaisiin SIM-kortti. Tämä auttaa puhelimien paikannusta hätätilanteessa. Se myös luo mahdollisuuden valetukiaseman avulla selvittää mitä puhelimia on lähtistöllä. Tämä paikannustarkkuus tällä menetelmällä on ainoastaan sen suuruinen mitä on kyseisen valetukiaseman luoman solun pinta-ala.

IMEI numeroon perustuvassa puhelimen tunnistuksessa on kuitenkin ongelmansa. Puhelimen IMEI numeroa on mahdollista muokata tai peräti vaihtaa toisen puhelimen kesken. On myös mahdollista, että valmistajat rakentavat useita puhelimia, joilla on sama IMEI-numero, huolimatta kyseisen koodin alkuperäisestä tarkoituksesta [31].

4.2 Kolmannen osapuolen keräämät tiedot

Älypuhelimien paikkatieto voi päätyä tuntemattomien tahojen käyttöön usealla eri tavalla. Puhelimeen on voinut päästä esimerkiksi haittaohjelma, joka sallii puhelimen tietoihin kohdistuvan vakoilun. Jotkin sovellukset saattavat välittää tietoa muille käyttäjille, mikäli yksityisasetuksia ei ole säädetty niin, että tiedon välittämistä ei tapahdu. [30]

ENISA:n (European Network and Internet Security Agency) raportin mukaan GPS:llä varustettu älypuhelin voi olla hyödyllinen vakoilulaite. Tämän mahdollistaa kolmannen osapuolen tuottamat sovellukset. Ne voivat avata sovelluksen tekijälle mahdollisuuden päästä käsiksi älypuhelimen tuottamaan paikkatietoon. Esimerkiksi Tap Snake-niminen sovellus, joka näyttää harmittomalta peliltä, lataa älypuhelimen paikkatiedon palvelimelle, johon sovelluksen tekijä voi päästä ja käyttää tätä tietoa myöhemmin palvelimelta käsin.[30]

Yhdysvaltalainen tietoturvatutkija ja hakkeri Jacob Applebaum väittää, että Yhdysvaltain turvallisuusvirasto NSA pystyy ottamaan haltuunsa ja vakoilemaan kaikkia Applen valmistamia iPhone älypuhelimia [32]. NSA käyttää tähän tarkoitukseen vuonna 2008 kehitettyä DROPOUTJEEP haittaohjelmaa [33]. Applebaumin mukaan NSA:lla pitää olla valtavasti apuvälineitä, jotta he onnistuvat joka kerta istutuksessaan iOS-käyttöjärjestelmään, tai Applen pitää itse tahallisesti sabotoida tuotteitaan[32].

NSA:n on mahdollista kontrolloida kaikkea iPhonen tietoa DROPOUTJEEP:n avulla. Sitä löytyy Applen tuotteiden lisäksi myös muista järjestelmistä, mutta Applen mobiilituotteet ovat yleisimpiä, joita NSA vakoilee DROPOUTJEEP:n avulla. NSA pääsee tämän haittaohjelman avulla käyttämään puhelimen paikkatietoa. Se voi mm. selvittää minkä solun alueella kyseinen puhelin toimii. [34]

Paikkatietoa keräävät nykyään myös monet sosiaalisen median käyttöön tarkoitetut sovellukset kuten Facebook, jossa tilapäivitysten yhteydessä voidaan ilmaista käyttäjän sijainti

kirjoitushetkellä. Kuitenkin puhelimen käyttäjä kykenee yksinkertaisin toimenpitein estämään paikkatiedon jakamisen sosiaalisessa mediassa.

4.3 Laitteiden valmistajien keräämä paikkatieto

Mobiililaitevalmistajat vaativat laitteiden käyttäjää hyväksymään käyttöehdot ennen kuin laitetta pystyy käyttämään. Näiden ehtojen mukaan käyttäjä hyväksyy, että laitteen valmistaja kerää sijaintitietoa, joka tallennettaisiin sellaisessa muodossa, että puhelimen käyttäjää ei kyetä tunnistamaan [35]. Paikkatietojen käytettäisiin käyttöehtosopimusten mukaan palvelujen kehittämiseen.

Google kerää myös sovellustensa käyttäjiltä sijaintietoa. Tietoa kerätään mm. Google Maps –sovelluksen käyttäjiltä. Tiedon keruussa hyödynnetään kaikkia paikannusmenetelmiä, joita älypuhelimella voidaan käyttää. Googlen tietosuojakäytännöistä ei löydy mainintaa siitä, että tieto kerättäisiin anonyymina. Joissain tapauksissa kerättyyn tietoon saatetaan liittää näkyvillä olevan Google profiilin tiedot. Tällaista tietoa on mm. henkilön sähköpostiosoite. Applen tapaan Google ilmoittaa, että käyttäjiltä kerättyjä tietoja käytetään sovellusten kehittämiseen ja mainonnan kohdistamiseen.[36]

Laitevalmistajien keräämä paikkatieto voi kuitenkin olla sotilastoiminnan kannalta merkityksetöntä, mikäli sitä tarvitsevat tahot eli muut sotilaalliset toimijat eivät saa sitä käyttöönsä. Tiedossa ei ole, että älypuhelinten valmistajat jakaisivat tietojaan sotilaallista tiedustelua varten. Kuitenkin tässä pitää huomioida mahdollinen tietojen varastaminen palvelimilta, joille käyttäjiltä kerätty tieto tallennetaan.

5 JOHTOPÄÄTÖKSET

Älypuhelinten paikkatieto voidaan mieltää tiedustelutiedoksi operaatioturvallisuuden kannalta. Tiedustelutiedon osalta on tärkeää, että se perustuu tosiasioihin. Älypuhelimet ovat helposti paikannettavissa mm. solupaikannusmenetelmällä. Kuitenkin älypuhelinten paikkatietoa voidaan hyödyntää vain, kun tiedetään puhelimen käyttäjä ja hänen tehtävänsä sotilasorganisaatiossa. Tällöin älypuhelimen käyttäjän joukko on paikannettavissa älypuhelimen paikkatiedon perusteella. Kuitenkin tiedustelijan on vaikea tietää, että puhelimen ja liittymän omistaja käyttää juuri tietyllä hetkellä puhelinta.

Älypuhelimet käyttävät useita eri paikanmääritysmenetelmiä. Näistä tarkimpia ovat satelliittipaikanmääritysmenetelmät GPS ja GLONASS. Satelliittipaikanmääritystä hyödyntävät useat eri sovellukset, joista osa kerää puhelimen paikkatietoa sovellusten omalle palvelimelle. Kuitenkin puhelimen käyttäjä kykenee helposti kytkemään satelliittipaikanmääritysmenetelmät pois päältä puhelimestaan. Tosin satelliittipaikanmääritysmenetelmät voi kytkeä myös melko helposti vahingossa päälle. Älypuhelimet voidaan paikantaa myös puhelinverkkoon perustuvilla paikannusmenetelmillä, joilla voidaan paikantaa myös tavanomaiset matkapuhelimet. Puhelinverkkoon perustuva paikannus toimii koko sen ajan minkä älypuhelin on yhteydessä puhelinverkkoon. Puhelimen käyttäjä ei siis pysty vaikuttamaan tähän muulla keinolla kuin kytkemällä puhelimen pois päältä, mikä tekee siitä hyödyttömän käyttäjälleen. Voidaan siis olettaa, että mikäli käyttäjä kantaa tarkoituksellisesti älypuhelinta mukanaan on se yhteydessä puhelinverkkoon.

Älypuhelimen paikkatietoa voivat jakaa myös erilaiset haittaohjelmat. Toistaiseksi DROPOUTJEEP on ainoa valtiollisen toimijan haittaohjelma, jonka olemassaolo tiedetään. Kuitenkin tällaiset haittaohjelmat kerkeävät keräämään tietoa jonkin aikaa ennen niiden olemassaolon huomaamista.

Jotta älypuhelimen paikkatieto kyetään jakamaan eteenpäin, tulee sen olla yhteydessä puhelinverkkoon, jonka tiedonsiirtonopeus riittää paikkatiedon tehokkaaseen jakamiseen. Paikkatieto ei myöskään uhkaa operaatioturvallisuutta, mikäli siihen ei tiedustelua suorittava taho pääse käsiksi. Paikkatietoa tallennetaan nykyään tunnistamattomassa muodossa laitteiden valmistajien palvelimille. Erilaiset sovellukset voivat kerätä älypuhelimien paikkatietoa muodossa, josta puhelimen käyttäjä kyetään tunnistamaan. Myös sosiaalisen median kuten Facebookin kautta voi levitä paikkatietoa tunnistetussa muodossa.

Tehokkaammista tiedustelu- ja valvontamenetelmistä huolimatta huomioida pitää älypuhelimien paikkatiedon merkitys operaatioturvallisuudelle. Esimerkiksi alus, joka ei käytä tutkiaan tai radioitaan voidaan paikantaa, mikäli aluksen henkilöstölle kuuluva puhelin kyetään tunnistamaan ja paikantamaan aluksen sijaintiin. Älypuhelimen paikkatietoa on myös jo hyödynnetty maalinosoituksessa. Kuitenkin älypuhelimen käyttäjät kykenevät usein omilla teoillaan vaikuttamaan siihen jaetaanko älypuhelimen paikkatietoa eteenpäin.

5.1 Älypuhelimien paikkatiedon hyödyt sotilastoiminnassa

Älypuhelimien paikkatiedon avulla voidaan saada tietoa harjoitusjoukkojen harjoitusten aikaisista liikkeistä. Tästä tiedosta voi olla hyötyä jäljitettäessä eksyneitä sotilaita. Kuitenkin tässä tapauksessa sotilailla pitää olla älypuhelin mukanaan harjoituksessa. Paikkatietohistoriaa voitaisiin käyttää myös hyväksi kadonneiden sotavarusteiden etsinnässä. Mikäli kalliimpia sotavarusteita kuten aseita tai niiden lisävarusteita katoaa harjoituksen aikana esimerkiksi pimeässä, jolloin sotilaan käsitys omasta sijainnista ei ole niin hyvä kuin päivänvalossa, älypuhelimen paikkatietohistorian avulla voidaan selvittää, mistä näitä voitaisiin etsiä.

Älypuhelimien paikkatietoa voidaan myös hyödyntää luotaessa tilannekuvaa omista joukoista. Sopivalla sovelluksella kyettäisiin jakamaan puhelimen välityksellä esimerkiksi tieto joukkueiden sijainneista. Kuitenkin tässäkin menetelmässä olisi huomioitava puhelinverkon heikkoudet sota- ja kriisitilanteissa.

LÄHTEET

[1] Sosiaalisessa mediassa toiminnan ohje varusmiehille ja reserviläisille AH27977

[2] Tietoviikko 25.4.2013 [viitattu: 30.4.2013], saavutettavissa: http://www.tietoviikko.fi/kaikki_uutiset/suomessa+jo+puolet+alypuhelimia++90+prosenttia+vuonna+2014/a798141?service=mobile&page=2

[3] Tilastokeskus. *Internetyhteydet ja internetin* [viitattu 11.3.2014]. saatavissa: http://www.stat.fi/til/sutivi/2011/sutivi_2011_2011-11-02_kat_001_fi.htm

[4] Apple. *iPhone 5 tekniset tiedot.* [viitattu: 6.6.2013] saatavissa: http://www.apple.com/fi/iphone/specs.html

[5] Nokia. *Lumia 920 tekniset tiedot.* [viitattu: 6.6.2013] saatavissa: http://www.nokia.com/fi-fi/tuotteet/puhelimet/lumia920/tuoteseloste/

[6] Samsung. *Galaxy s4 tekniset tiedot.* [viitattu 6.6.2013] saatavissa: http://www.samsung.com/fi/consumer/mobile/mobilephones/smartphones/GT-I9505ZWANEE-spec

[7] *Strateginen kommunikaatio ja ingormaatio-operaatiot 2030*

[8] Mika Huttunen. *Monimutkainen taktiikka.* Helsinki. Maanpuolustuskorkeakoulu Taktiikan laitos 2010. 321s.

[9] *Sotatekninen arvio ja ennuste 2035 osa1.*

[10] Juha-Matti Hirvensalo. *Sotilaan paikkatiedon siirtäminen tietoverkossa* Pro-Gradu. 2011. Maanpuolustuskorkeakoulu Sotatekniikan laitos.

[11] Olli Ovaska. *Israelin puolustusvoimien maalittamistoiminta operaatiossa Valettu lyij.* Tutkimusraportti. Helsinki, 2013. Maanpuolustuskorkeakoulu, Taktiikan laitos. 109 sivua.

[12] Jyrki Kososla, Janne Jokinen. *Elektroninen sodankäynti osa2 – toimeenpano sotilasoperaatiossa*. Helsinki 2005. Maanpuolustuskorkeakoulu. Sotatekniikan laitos

[13] Jyrki Kososla, Janne Jokinen. *Elektroninen sodankäynti osa 1 – taistelun viides dimensio.* Helsinki 2005. Maanpuolustuskorkeakoulu. Sotatekniikan laitos

[14] *Paikannus älyliikenteessä.* Liikenne ja viestintäministeriö 2010.

[15] Esa Airos, Risto Korhonen, Timo Pulkkinen, *Satelliittipaikanmääritysmenetelmät.* PVTT. 2008

[16] Matti Rantanen. *Paikkatietotekniikka ja navigointi.* PVTK

[17] Poutanen Markku. *GPS-paikanmääritys*. 2. painos. URSA. 1998

[18] Nokia usein kysytyt kysymykset: Mikä on AGPS. Nokia [viitattu 31.7.2013]. saatavissa: http://www.nokia.com/fi-fi/tuki/faq/?action=singleTopic&topic=FA114913

[19] Puhelinvertailu.com. *Ensimmäinen GLONASS-paikannusta tukeva puhelin tuli myyntiin.* [viitattu: 4.8.2013]. saatavissa: http://www.puhelinvertailu.com/uutiset.cfm/2011/04/02/ensimmainen_glonass-paikannusta_tukeva_puhelin_tuli_myyntiin

[20] Federal Space Agecy, International-Analytical Centre. *GLONASS constellation status, 21.01.2014.* [viitattu: 21.1.2014] saatavissa: http://glonass-iac.ru/en/GLONASS/

[21] Elisa. Verkon kuuluvuus. [viitattu 15.1.2014]. Saatavissa: http://www.elisa.fi/kuuluvuus

[22] Robert C. Raciti. *Cellural Technology.* Heinäkuu 1995. [viitattu: 5.1.2014] saatavissa: http://scis.nova.edu/~raciti/cellular.html

[23] Jukka K. Nurminen. *Soluverkot.* [viitattu: 11.3.2014] saatavissa: http://www.cse.tkk.fi/fi/opinnot/T-110.2100/2010/luennot-files/Solukkoverkot%20(luonnos).pdf

[24] Ville Airu. *Paikannus GPS- ja GSM järjestelmissä.* Opinnäytetyö. Tampere, 2009. Tampereen ammattikorkeakoulu, Tietotekniikan koulutusohjelma. 32s.

[25] Paikannus.com. Matkapuhelinverkkoon perustuva paikannus. [viitattu: 31.7.2013] saatavissa: http://www.paikannus.com/matkapuhelinverkkoon-perustuva-paikannus

[26] Antti Rainio. *Paikannus mobiilipalveluissa ja sovelluksissa.* Teknologiakatsau 143/2003 ISSN 1239-758

[27] Sarah Jean Fusco, Katina Michael, M G. Michael, Roba Abbas *Exploring the social implications of location based social networking: an inquiry into the perceived positive and negative impacts of using LBSN between friends*

[28] Die Zeit. [viitattu 16.7.2013]. saatavissa: http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten

[29] Helsingin Sanomat. *NSA:n verkkourkinta on luultua laajempaa, sähköpostit ja hakuhistoria helposti luettavissa*. [viitattu: 4.8.2013]. saatavissa: http://www.hs.fi/ulkomaat/a1375241208888

[30] Yle. *Venäläinen puhelinoperaattori häiritsee Sallassa.* [viitattu: 4.8.2013]. saavutettavissa: http://yle.fi/uutiset/venalainen_puhelinoperaattori_hairitsee_sallassa/6314018

[31] MTV3. *Kännykoiden koodikupla voi linkittää puhelimesi rikokseen.* [viitattu 8.1.2014] saavutettavissa: http://www.mtv.fi/uutiset/it/artikkeli/kannykoiden-koodikupla-voi-linkittaa-puhelimesi-rikokseen-/1796028

[32] European Network and Information Security Agency. *Smartphone Security.* Joulukuu 2010. 61s.

[33] Spiegel online. *NSA-Software für iPhones: Apple verneint Kenntnis von Spionageprogramm.* [viitattu 10.1.2014] saavutettavissa: http://www.spiegel.de/netzwelt/netzpolitik/nsa-ueberwachung-apple-verneint-kenntnis-von-spionageprogramm-a-941414.html

[34] Talouselämä. *Väite: NSA pystyy vakoilemaan mitä tahansa iPhonea.* [viitattu: 10.1.2014] saavutettavissa: http://www.talouselama.fi/uutiset/vaite+nsa+pystyy+vakoilemaan+mita+tahansa+iphonea/a2223715

[35] Apple. iPad käyttöehtosopimus.

[36] Security Affairs. *DROPOUTJEEP – How NSA completely controls your iPhone.* [viitattu: 10.1.2014] saatavissa: http://securityaffairs.co/wordpress/20896/hacking/nsa-dropoutjeep-spy-iphone.html

[37] Google Käytännöt ja periaatteet. *Tietosuojakäytännöt.* [viitattu 13.1.2014] saavutettavissa: http://www.google.fi/policies/privacy/

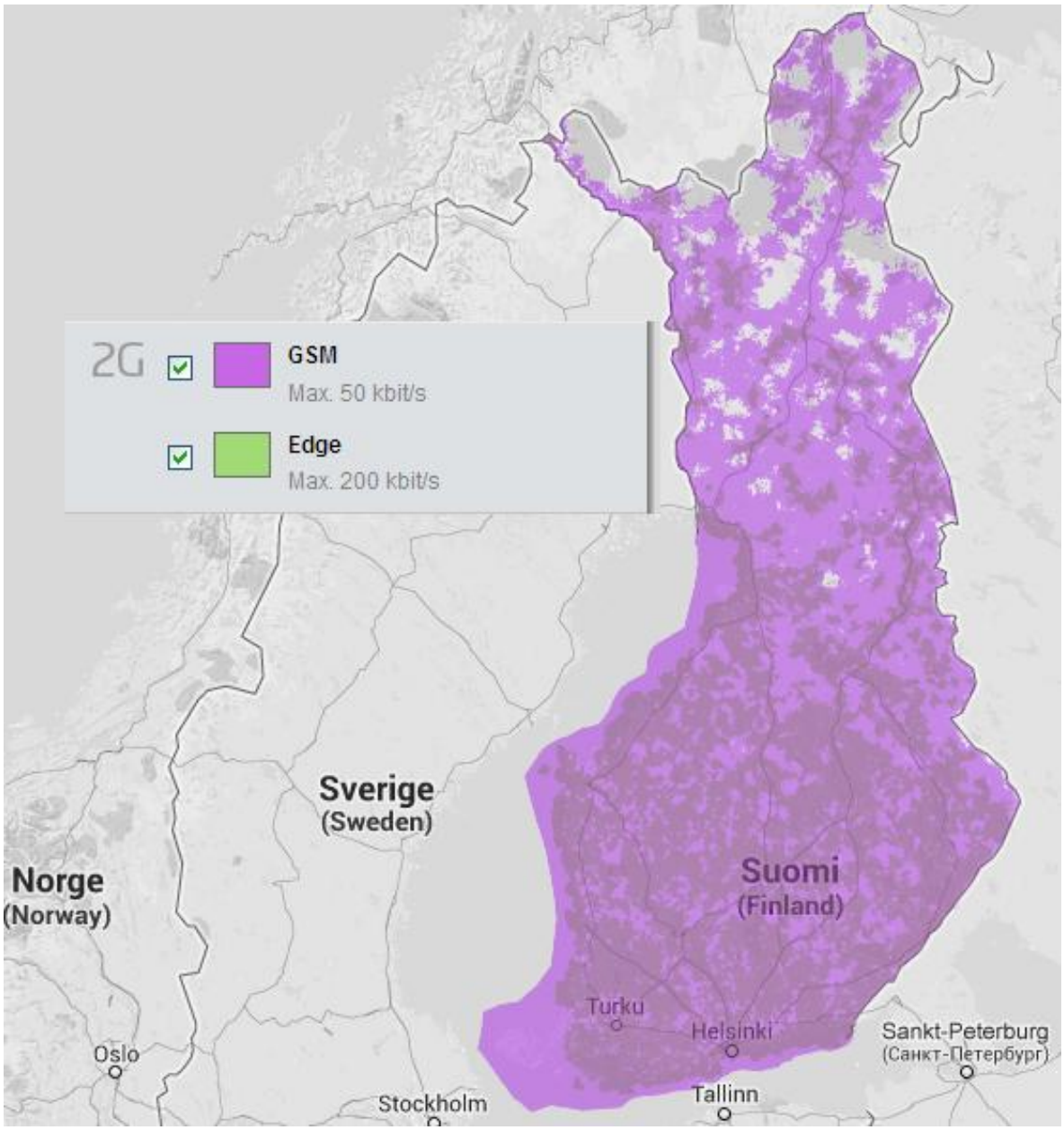
[38] Sonera verkon kuuluvuuskartta. [viitattu 15.1.2014]. Saavutettavissa: http://www.sonera.fi/etsi+apua+ja+tukea/verkkokartat/kuuluvuuskartta

Liite 1 Elisan 3g kuuluvuus Suomessa

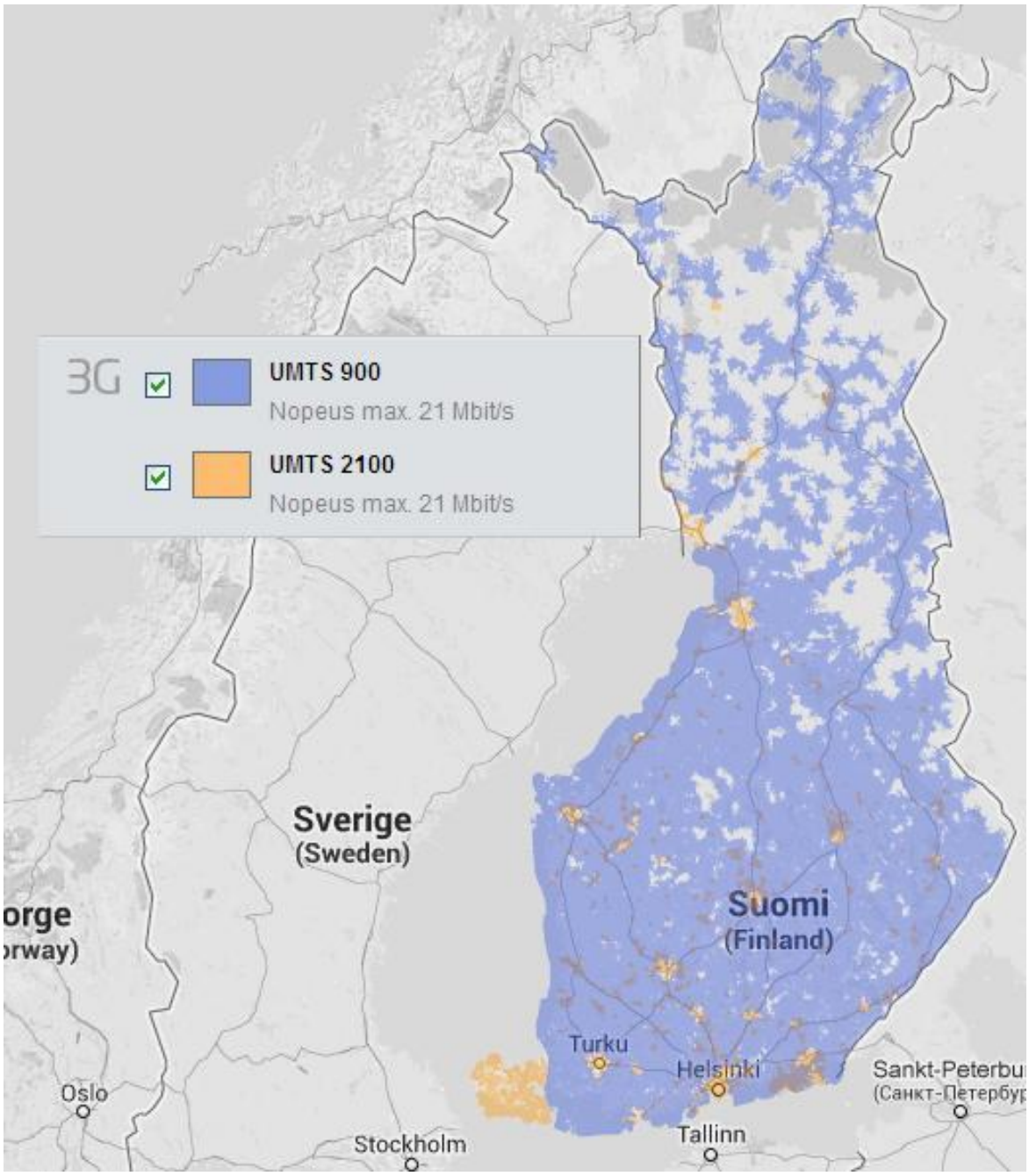
Liite 2 Elisan 3 verkon kuuluvuus

Liite 3 Soneran 2g verkon kuuluvuus

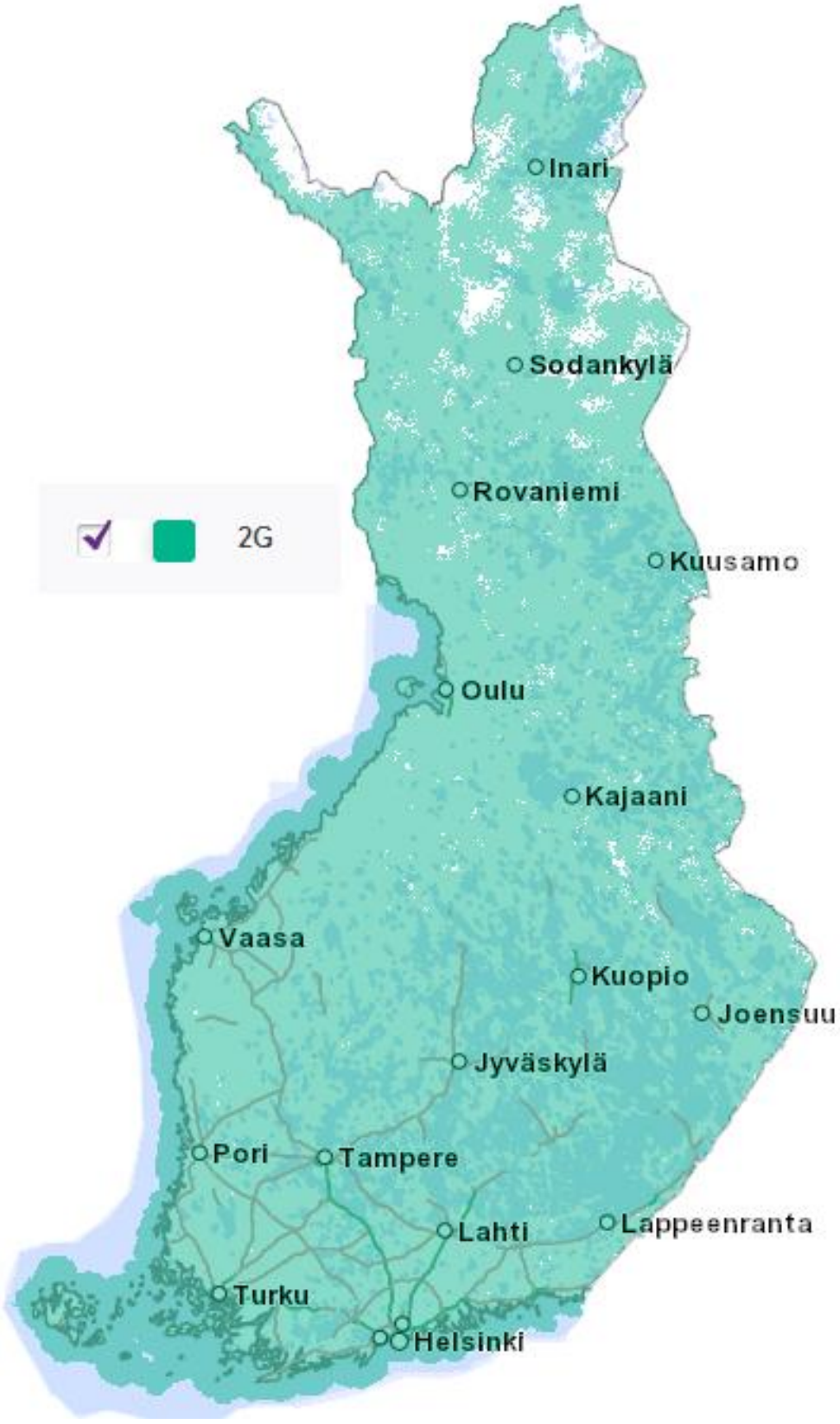
Liite 4 Soneran 3g verkon kuuluvuus



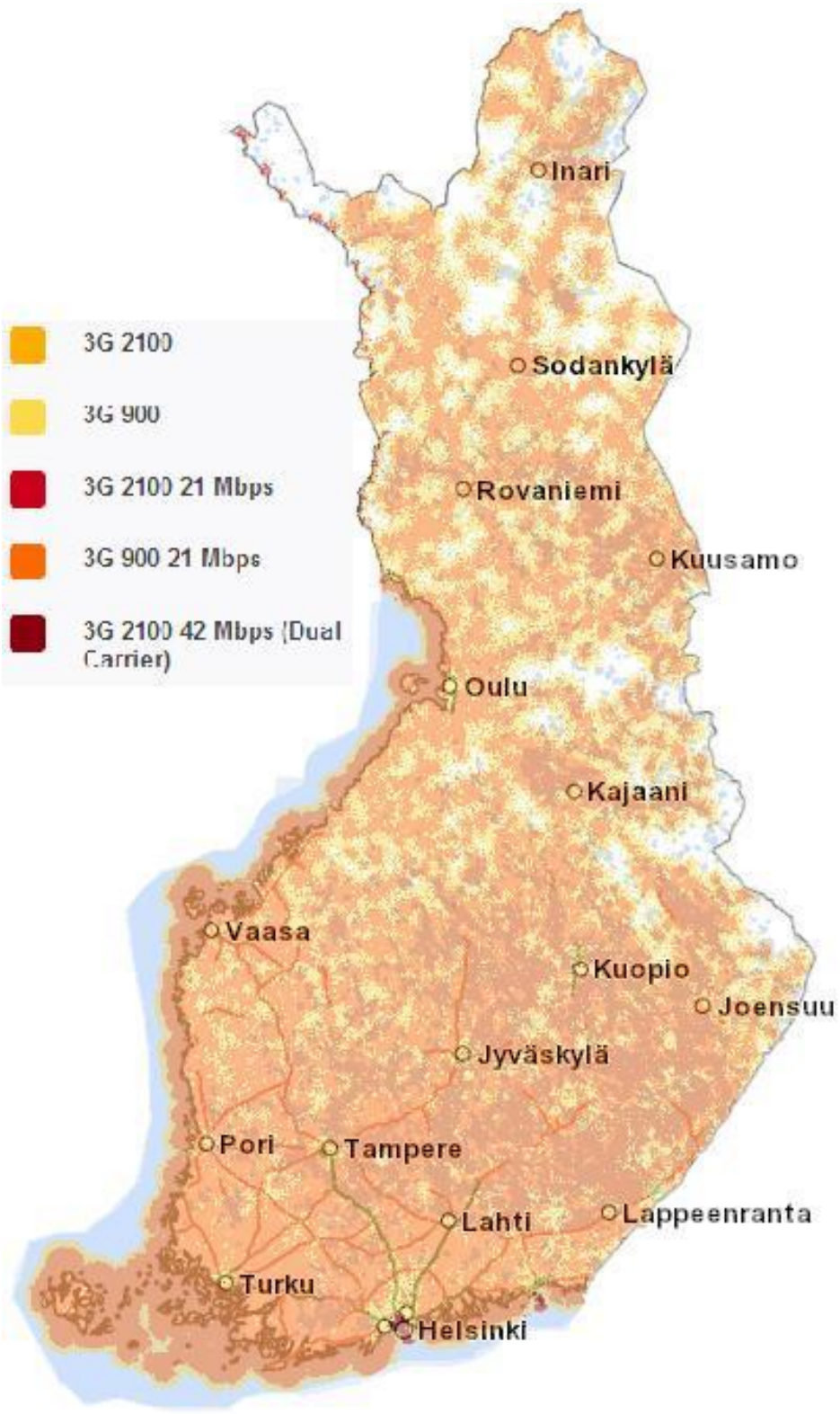
Elisa 2G-verkon (GSM ja Edge) kuuluvuus Suomessa 15.1.2014. [21]



Elisa 3g verkon kuuluvuus. [21]



Soneran 2g verkon kuuluvuus. [38]



Soneran 3g verkon kuuluvuus. [38]