Nea Räisänen

AJONEUVOJEN LANGATTOMISSA VERKOISSA (VANET:SSA) TOIMIVIEN TURVALLISUUSSOVELLUSTEN TIETOTURVALLISUUS

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2017

TIIVISTELMÄ

Räisänen, Nea
Ajoneuvojen langattomissa verkoissa (VANET:ssa) toimivien turvallisuussovellusten tietoturvallisuus
Jyväskylä: Jyväskylän yliopisto, 2017, 30 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaajat: Kovanen, Tiina; Moilanen, Panu

Tieliikenteessä ilmenevien ongelmien, kuten onnettomuuksien ja ruuhkien ratkaisuissa on alettu hyödyntää tieto- ja viestintäteknologiaa. Tällaisia ratkaisuja kutsutaan älykkäiksi liikennejärjestelmiksi. Älykkäiden liikennejärjestelmien avulla voidaan lisätä tärkeän ja hyödyllisen tiedon vaihtoa tiellä liikkujien kesken. Tässä tiedonvaihdossa ajoneuvojen langattomat verkot eli VANET nähdään keskeisenä teknologiana, sillä niiden avulla ajoneuvot voivat automaattisesti kommunikoida keskenään sekä tieinfrastruktuurin kanssa. VANET mahdollistaa useita liikenteen turvallisuutta parantavia sovelluksia, eli turvallisuussovelluksia, mutta muiden langattomien verkkojen tavoin myös VANET sekä sen avulla toimivat turvallisuussovellukset ovat alttiita erilaisille tietoturvauhkille. Ennen kuin VANET ja turvallisuussovellukset voidaan ottaa laajamittaiseen käyttöön tieliikenteessä, on ratkaistava niihin liittyvät tietoturvallisuusuhkat. Tässä tutkielmassa luodaankin katsaus näihin VANET:iin kohdistuviin uhkiin sekä siihen, mitä nämä uhkat merkitsevät tietoturvallisuussovellusten kontekstissa. Aiheen tutkiminen on tärkeää, sillä väärinkäytön kohdistuessa turvallisuussovelluksiin nämä sovellukset voivat ehkäisyn sijaan alkaa aiheuttaa liikenneonnettomuuksia ja niistä johtuvia liikennekuolemia. Tämä tutkielma toteutetaan kirjallisuuskatsauksena, jonka aineistona käytetään informaatioteknologia-alan artikkeleita, konferenssijulkaisuja ja projektiraportteja. Tutkielman tuloksena löytyi useita VANET:iin ja samalla myös turvallisuussovelluksiin kohdistuvia uhkia.

Asiasanat: älyliikenne, VANET, turvallisuussovellus, tietoturvallisuus, hyökkäykset

ABSTRACT

Räisänen, Nea
Information security of safety applications in vehicular ad hoc networks (VANETs)
Jyväskylä: University of Jyväskylä, 2017, 30 p.
Information system science, Bachelor's thesis
Supervisors: Kovanen, Tiina; Moilanen, Panu

Information and communications technology is currently used in solving problems related to road traffic, such as accidents and road congestion. These solutions are called intelligent transportation systems. Intelligent transportation systems can be used to exchange useful and important traffic information between road users. Vehicular ad hoc network (VANET) is considered an essential technology that enables information exchange between road users because VANET enables communication between vehicles and between vehicles and infrastructure. VANET also enables various applications that can enhance road safety, also called safety applications. Because VANET is a wireless medium, it is also, along with the safety applications that use VANET, vulnerable to various security attacks. Before VANET and safety applications can be widely deployed, their security threats must be solved. This study peeks at these security threats and what these threats imply in safety applications context. Studying this subject is important because misusing safety applications could result in traffic accidents and loss of lives. As a result of this study, various security threats concerning VANET and safety applications are identified.

Keywords: intelligent transportation system, VANET, safety application, information security, attacks

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Kulkuneuvojen suuri määrä sekä niiden lisääntyminen tieliikenteessä ruuhkauttavat liikenneinfrastruktuuria ja lisäävät onnettomuusriskiä, kuljetusten viivästelyä ja liikennepäästöjä. Tästä syystä on alettu kehittää tieto- ja viestintäteknologiaa hyödyntäviä ratkaisuja, jotka voivat parantaa liikenteen turvallisuutta, tehokkuutta ja ympäristöystävällisyyttä. Tällaisia ratkaisuja kutsutaan älykkäiksi liikennejärjestelmiksi. (Figueiredo, Jesus, Machado, Ferreira, & Martins de Carvalho, 2001.)

Älykkäitä liikennejärjestelmiä hyödyntämällä voidaan lisätä tieliikenteessä ajoneuvojen sekä infrastruktuurin välistä automaattista tiedonvaihtoa. Lisääntyvän tiedonvaihdon avulla voidaan tarjota kuljettajille liikenteen tilasta ajankohtaista tietoa, esimerkiksi varoituksia lähestyvistä ruuhkista tai tietöistä, jonka pohjalta kuljettaja voi tehdä matkaansa koskevia ratkaisuja, kuten valita vaihtoehtoisen reitin. Automaattinen tiedonvaihto liikenteessä mahdollistaa myös ennakkovaroitukset uhkaavista tilanteista, kuten edellä sattuneesta onnettomuudesta, jolloin kuljettajat voivat saada enemmän aikaa reagoida tilanteeseen välttääkseen onnettomuuden. (Figueiredo ym., 2001.)

Suomen liikenne- ja viestintäministeriö julkaisi vuonna 2009 kansallisen älyliikenteen strategian. Päivitetty versio julkaistiin vuonna 2013. Yksi Suomen liikenteen älystrategian (2013) tavoitteista ja painopistealueista on turvallisuus, jota voidaan parantaa reagoivilla ja ennakoivilla turvajärjestelmillä. Näiden järjestelmien avulla voidaan lieventää jo tapahtuneiden liikenneonnettomuuksien seurauksia sekä ehkäistä onnettomuuksia kokonaan.

Onnettomuuksien ehkäisytoimiin Suomen älyliikennestrategiassa (2013) luetaan yhteistoiminnalliset järjestelmät, jotka perustuvat ajoneuvojen keskinäiseen sekä ajoneuvojen ja liikenneinfrastruktuurin väliseen automaattiseen tiedonvaihtoon. Tämän toteuttamisessa VANET voi olla mahdollistava teknologia.

Jakaakseen informaatiota ajoneuvot muodostavat tilapäisen verkon, joka tunnetaan nimellä VANET (engl. vehicular ad hoc network). Tällainen verkko mahdollistaa automaattisen tiedonvaihdon ajoneuvolta ajoneuvolle (engl. vehicle-to-vehicle, V2V) sekä ajoneuvolta infrastruktuurille, tarkemmin tienvarsien

kiinteille linkkiasemille (engl. vehicle-to-infrastructure, V2I) (Zeadally, Hunt, Chen, Irwin, & Hassan, 2012).

VANET mahdollistaa useita sovelluksia, myös tässä tutkielmassa käsiteltävät turvallisuussovellukset (Zeadally ym., 2012). Näiden sovellusten avulla ajoneuvot voivat muun muassa lähettää ja vastaanottaa varoituksia edellä sattuneesta onnettomuudesta seuraaville kuljettajille, jotta he voivat välttää onnettomuuden.

Suomessa tapahtui vuonna 2016 tammi-marraskuun aikana 4341 henkilövahinkoon johtanutta tieliikenneonnettomuutta, joissa kuoli 220 ja loukkaantui 5384 ihmistä. Onnettomuudet jakautuivat muun muassa risteäviin, vastakkaisiin ja samoihin ajosuuntiin. (Tilastokeskus, 2016.) VANET:n mahdollistamia turvallisuussovelluksia voitaisiin hyödyntää ehkäisemään näitä liikenneonnettomuuksia, sillä ne voivat tarjota kuljettajille enemmän aikaa reagoida ympäröivän liikenteen tapahtumiin (Chen, Jin & Regan, 2010).

Suomen älyliikenteen strategiassa mainittujen yhteistoiminnallisten järjestelmien käyttöönottamiseksi tarvitaan kuitenkin turvallinen keino tiedon välitykseen. Tiedonvaihto liikkujien välillä parantaa liikenneturvallisuutta vain, jos liikkujien saamat viestit ovat luotettavia ja ajantasaisia, eikä niitä ole manipuloitu millään tavoin.

Tämä tutkielma toteutetaan kirjallisuuskatsauksena, jonka lähdeaineisto koostuu pääosin informaatioteknologian alan artikkeleista, konferenssijulkaisuista, kirjallisuudesta sekä projektiraporteista. Tutkielman tavoitteena on selvittää, millaisia sovelluksia voidaan hyödyntää liikenneonnettomuuksien ehkäisyssä, miten sovellukset pääpiirteittäin toimivat ja millaisia tietoturvauhkia niihin kohdistuu. Aiheen tutkiminen on tärkeää, sillä turvallisuussovellukset voivat vähentää merkitsevästi liikenneonnettomuuksia ja -kuolemia. Samalla myös itse sovellusten ja niiden käyttämän langattoman teknologian tietoturvallisuuden tutkiminen on tärkeää. Mikäli sovellusten välinen tiedonvaihto ei ole luotettava, seuraukset voivat olla vakavat, esimerkiksi liikenneonnettomuudet. Näin myöskään Suomen älyliikennestrategian turvallisuustavoitteet eivät voi täyttyä.

Luvussa 2 esitellään älyliikenteen määritelmä sekä sen kannalta keskeinen teknologia eli VANET. Annetaan myös esimerkkejä visioiduista, VANET:n avulla toimivista turvallisuussovelluksista ja niiden toimintaperiaatteesta. Luvussa 3 määritellään tietoturvallisuuden käsite sekä millaisia tietoturvallisuusvaatimuksia VANET:n turvallisuusviesteille tarkoitetun järjestelmän tulee täyttää voidakseen toimia toivotulla tavalla. Luvussa 4 yhdistetään lukujen 2 ja 3 käsitellyt asiat sekä annetaan esimerkkejä hyökkäyksistä, jotka vaarantavat luvussa 3 määriteltyjen vaatimusten täyttymisen. Lopuksi luvussa 5 on tutkielman yhteenveto.

2 ÄLYLIIKENNE JA KOMMUNIKOIVAT AJONEUVOT

Tässä luvussa esitellään ensimmäiseksi älyliikenteen ja älykkäiden liikennejärjestelmien määritelmät. Näiden määritelmien pohjalta edetään älyliikenteen toteuttamisen sekä tämän tutkielman aiheen kannalta keskeisen teknologian, ajoneuvojen muodostamien verkkojen eli VANET:n käsittelyyn. VANET:sta esitellään sen määritelmä, siihen liittyvät standardit ja sen perustoimintaperiaate. Lopuksi vastataan seuraaviin tämän tutkielman tutkimuskysymyksiin: millaisia sovelluksia voidaan hyödyntää liikenneonnettomuuksien ehkäisyssä ja miten sovellukset pääpiirteittäin toimivat? Eli luvun lopuksi käydään läpi, millä tavoin VANET:ia voidaan hyödyntää liikenteen turvallisuuden parantamisessa.

2.1 Älyliikenne ja älykkäät liikennejärjestelmät

Järjestelmiä tai palveluita, jotka soveltavat tieto- ja viestintäteknologiaa liikenteen ongelmien, kuten ruuhkautumisen ratkaisemiseksi, kutsutaan älykkäiksi liikennejärjestelmiksi (Figueiredo ym., 2001; Kulmala, 2010). Milesin ja Chenin (2004) Giannoutakisin ja Lin (2012) mukaan älykkäät liikennejärjestelmät ovat järjestelmiä, teknologioita ja palveluita, joilla pyritään turvallisempiin ja tehokkaampiin kuljetuspalveluihin lisäämällä järjestelmien tuottavuutta ja turvallisuutta, vähentämällä matkustusaikoja ja kustannuksia sekä säästämällä energiaa. Tällaisiin järjestelmiin lukeutuu esimerkiksi ajoneuvojen sisäiset informaatiojärjestelmät ja kuljettajan apujärjestelmät kuten navigointi sekä kolarivaroitusjärjestelmät.

Suomen ensimmäisessä liikenne- ja viestintäministeriön kansallisessa älyliikenteen strategiassa (2009) älyliikenne ja älykäs liikennejärjestelmä määritellään erikseen. Strategiassa älyliikenteellä tarkoitetaan tieto- ja viestintäteknologian hyödyntämistä liikennejärjestelmässä, kaikissa liikennemuodoissa sekä henkilö- että tavaraliikenteessä. Älykäs liikennejärjestelmä puolestaan määritellään strategiassa monien toimijoiden ja toimenpiteiden tulokseksi. Se tarkoittaa

palveluita, jotka ”tukevat liikenteen seurantaa, hallintaa ja ohjausta sekä tarjoavat informaatiota kuljettajille, liikkujille ja liikennejärjestelmän operoijille”.

Suomen liikenne- ja viestintäministeriö julkaisi vuonna 2013 päivitetyn älyliikenteen strategian. Tässä versiossa älykkään liikennejärjestelmän perusajatukseksi kuvaillaan tieto-ja viestintäteknologian hyödyntämistä liikennejärjestelmän toimivuuden parantamiseksi.

Älyliikenne ja älykkäät liikennejärjestelmät ovat siis termeinä lähes toisiaan vastaavia ja niitä käytetäänkin ainakin Suomen älyliikenteen strategiassa (2009) päällekkäin. Strategian määritelmän pohjalta älyliikenne voidaan ajatella yleistermiksi kuvaamaan tieto- ja viestintäteknologiaa hyödyntävää liikennejärjestelmää. Älykäs liikennejärjestelmä puolestaan voidaan strategian sekä muiden edellä mainittujen lähteiden määritelmien pohjalta ajatella konkreettiseksi älyliikenteen toteutukseksi. Tällainen toteutus voi olla esimerkiksi palvelu, jonka avulla liikenteen eri käyttäjät voivat käyttää liikennettä tehokkaammin ja ”älykkäämmin”.

Älyliikenteen yksi merkittävimpiä mahdollistajia on ajoneuvojen tiedonvaihto ympäristönsä tilasta toistensa sekä tieinfrastruktuurin kanssa. Tiedonvaihtoa voidaan toteuttaa esimerkiksi matkapuhelinsovelluksilla, joita on jo kuluttajille saatavilla sovelluskaupoista, esimerkiksi HAAS Alert (HAAS Alert, 2017). Lisäksi Liikennevirastolla ja Trafilla on käytössä NordicWay Coop -kokeilu huhtikuun 2017 loppuun asti Etelä-Suomessa (NordicWay Coop, 2017). Tässä liikenneturvallisuuskokeilussa autoilijat välittävät tietoa Android-puhelimeen ladattavan Coop-sovelluksen avulla liikenneturvallisuutta heikentävistä tekijöistä, kuten onnettomuuksista tai sääolosuhteista (NordicWay Coop). Tällaisten sovellusten välityksellä kuljettajat voivat siis vastaanottaa ja tehdä ilmoituksia liikenteen tilasta, kuten varoituksia tiellä sattuneesta onnettomuudesta. Näiden sovellusten mahdollistama liikennetiedon vaihto edellyttää kuitenkin kuljettajia itse lähettämään ilmoituksia kohtaamistaan esteistä liikenteessä. Näin ollen ilmoitusten lähetys on kuljettajien muistin ja vapaaehtoisuuden varassa. Lisäksi matkapuhelinsovelluksen käyttö voi viedä kuljettajien huomiota pois liikenteestä aiheuttaen näin onnettomuusriskin.

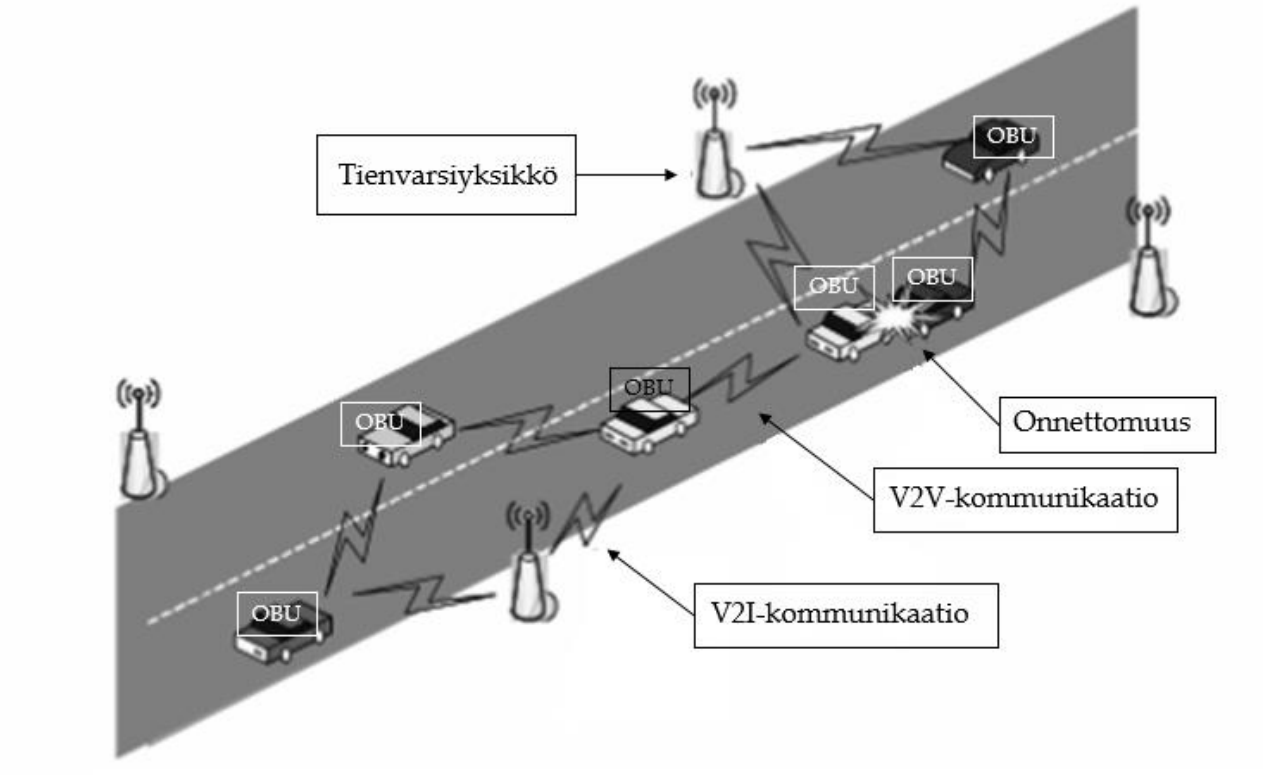
Ajoneuvojen tiedonvaihdosta on kuitenkin mahdollista tehdä automaattista, jolloin ajoneuvot voivat keskustella keskenään reaaliajassa ilman kuljettajien osallisuutta. Tällaisessa automaattisessa tiedonvaihdossa ajoneuvojen langaton tilapäisverkko eli VANET (vehicular ad hoc network) on keskeinen teknologia (Zeadally ym., 2012).

2.2 VANET:n toimintaperiaate

VANET tarkoittaa yleistä, itsestään järjestäytyvää langatonta verkkoa, jonka solmuina toimivat liikkuvat ajoneuvot ja jonka muodostamiseen ei tarvita kiinteää tukiasemaa. VANET:lle ominaista on ajoneuvojen liikkeistä johtuva suuri nopeus ja tieinfrastruktuurin rakenteesta johtuva solmujen rajallinen liikkuvuus.

VANET mahdollistaa suoran kommunikaation ajoneuvojen ja ajoneuvojen ja infrastruktuurin välillä, jolloin ajoneuvot voivat välittää toisilleen esimerkiksi turvallisuuteen liittyviä viestejä. (Harri, Filali & Bonnet, 2009; Hartenstein & Laberteaux, 2008.)

VANET:n toimintaa voidaan havainnollistaa yksinkertaisen kuvion avulla (KUVIO 1). VANET :ssa ajoneuvot voivat kommunikoida keskenään (engl. vehicle-to-vehicle, V2V) ja tieinfrastruktuurin kanssa (engl. vehicle-to-infrastructure, V2I) tielle asetettujen linkkiasemien, eli tienvarsiyksiköiden (engl. road side unit, RSU) avulla (Sichitiu & Kihl, 2008) (KUVIO 1). Jatkossa tässä tutkielmassa ajoneuvojen väliseen kommunikaatioon viitataan englanninkielisellä lyhenteellä V2V ja ajoneuvojen ja tieinfrastruktuurin väliseen kommunikaatioon lyhenteellä V2I, sillä aiheen käsittely näiden lyhenteiden avulla on havainnollisempaa ja koska näille lyhenteille ei toistaiseksi löydy vakiintunutta suomenkielistä vastinetta.



KUVIO 1 Esimerkki VANET:n toiminnasta (muokattu: Qian & Moayeri, 2008, 2795).

Kommunikaatio on mahdollista ajoneuvojen ja tienvarsiyksiköiden välillä, kun ajoneuvot on varustettu jollain radiorajapinnalla tai kulkuvälineyksiköllä (engl. OnBoard Unit, OBU) (KUVIO 1), joka mahdollistaa lyhyen kantaman langattomien tilapäisverkkojen muodostamisen (Stampoulis & Chai, 2007, Zeadallyn ym., 2012 mukaan). OBU tarjoaa sovelluksille ajoympäristön, sijainti-, turvallisuus- ja tiedonvaihtotoiminnot sekä rajapinnat muihin ajoneuvoihin ja tienvarsiyksiköihin (Karagiannis ym., 2011). Ajoneuvojen tulee olla varustettu myös yksityiskohtaisen sijaintitiedon vastaanottavalla laitteella, kuten GPS :llä. Kiin-

teät tienvarsiyksiköt ovat yhteydessä runkoverkkoon, jolloin ne voivat helpottaa ajoneuvojen välistä sekä ajoneuvojen ja infrastruktuurin välistä tiedonvaihtoa. (Zeadally ym., 2012.) Tienvarsiyksikköjä voidaan sijoittaa esimerkiksi teiden varsille, liikennevaloihin tai risteysalueille (Qian & Moayeri, 2008).

VANET :ssa peruskommunikaatiotyyppi perustuu yhden hypyn monilähetykseen (Hartenstein & Laberteaux, 2008). Yhden hypyn monilähetyksessä ajoneuvo lähettää viestin kaikille sen lähetyskantaman alueella oleville ajoneuvoille (Chen ym., 2010). VANET:ssa voidaan joissakin sovelluksissa hyödyntää myös multihop -lähetystapaa, jossa viestin vastaanottaneet ajoneuvot voivat välittää sen eteenpäin (Sichitiu & Kihl, 2008). Tällä tavalla kuljettajat voivat tehdä järkeviä ajoaan koskevia päätöksiä hyvissä ajoin.

Ajoneuvojen lähettämät viestit voidaan jakaa kahteen tyyppiin: rutiiniviesteihin ja tapahtumaviesteihin. Rutiiniviestit ovat ajoneuvojen säännöllisesti lähettämiä tilaviestejä (engl. status message) (Jiang, Taliwal, Meier, Holfelder & Herrtwich, 2006; Hartenstein & Laberteaux, 2008), joten ne voivat lisätä kuljettajien tietoisuutta liikenteestä. Ne ovat merkityksellisiä vain muutaman sekunnin ajan niin, että vastaanottaja voi ennustaa lähettäjän liikkeet tämän ajan aikana (Jiang ym., 2006). Tapahtumaviestin puolestaan laukaisee muutokset ajoneuvon käyttäytymisessä. Tällaiset muutokset, esimerkiksi äkkijarrutus, rikkovat rutiiniviesteistä seuraavaa jatkuvuutta. (Jiang ym., 2006.) Ajoneuvot voivat lähettää tapahtumaviestin eteenpäin läheisille ajoneuvoille, jotka myöskin ovat vaaravyöhykkeellä (Cheng ym., 2011).

Älyliikenteen kannalta VANET on merkittävä, sillä se mahdollistaa monia liikenteen toimintaa ja turvallisuutta parantavia sovelluksia. VANET:n avulla ajoneuvot voivat välittää toisilleen esimerkiksi peräänajon välttämiseen tai liikenteen sujuvuuteen liittyviä viestejä. (Harri ym., 2009.) VANET mahdollistaa myös sovellukset, jotka tarjoavat lisämukavuutta kuljettajille ja matkustajille, kuten Internet-yhteys (Cheng, Shan & Zhuang, 2011). Tässä tutkielmassa keskitytään kuitenkin pelkästään VANET :n liikenteen turvallisuutta parantaviin sovelluksiin, lyhyemmin turvallisuussovelluksiin.

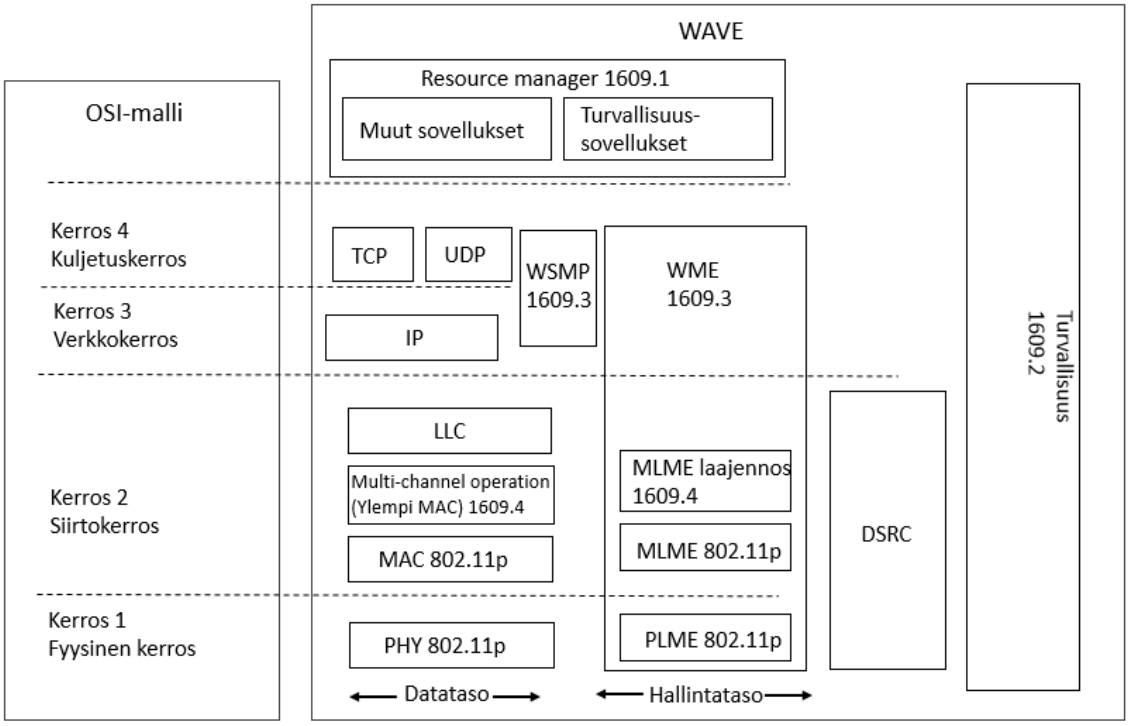
2.3 VANET:iin liittyvät standardit

Standardit yksinkertaistavat tuotekehitystä ja niiden avulla voidaan taata tuotteiden välinen yhdistettävyys sekä yhteistoimivuus myös eri merkkien ja mallien välillä. VANET:iin liittyvät standardit ovat DSRC (Dedicated Short Range Communications) ja IEEE 802.11p WAVE (Wireless Access in Vehicular Environment). Tässä luvussa havainnollistetaan näitä standardipinoja kuvion (KUVIO 2) avulla, sillä kuvio osoittaa hyvin VANET:n standardien sijoittumisen suhteessa tunnettuun OSI-viitemalliin. Kuvio (KUVIO 2) osoittaa myös sen, mitä osia eri standardit käsittävät.

DSRC on lyhyen ja keskipitkän kantaman radioteknologia, joka tukee V2V- ja V2I -kommunikaatiota liikenneturvallisuuden ja liikenteen sujuvuuden parantamiseksi. DSRC:llä tähdätään korkeaan tiedonsiirtoon ja pieneen viivee-

seen. Euroopassa on varattu 20 MHz:n alue 5,8 GHz:n taajuusalueella ja Yhdysvalloissa 75 MHz:n alue 5,9 GHz:n taajuusalueella DSRC:tä hyödyntäville sovelluksille. (Zeadally ym., 2012.) DSRC-kaista on jaettu kanaviin, joista yksi on niin sanottu kontrollikanava, joka on omistettu vain turvallisuuteen liittyvään tiedonvaihtoon (Jiang ym., 2006).

IEEE 802.11p WAVE:n standardointiprosessi sai alkunsa DSRC-kaistan varaamisesta USA:ssa. DSRC:n fyysinen kerros pohjautui käytännössä langattomien lähiverkkojen IEEE 802.11a-standardiin ja MAC-kerros (engl. medium access control) langattomien lähiverkkojen 802.11-standardiin (KUVIO 2). Tämä oli kuitenkin riittämätön ja liian hitaan tiedonvaihdon aiheuttava ratkaisu haastaviin ja muuttuviin liikennetilanteisiin. Vuonna 2004 IEEE 802.11 -standardin työryhmä alkoikin työstää muutosta standardiin 802.11 liittääkseen siihen myös ajoneuvojen ympäristöt. Työryhmä muutti DSRC:n nimen IEEE 802.11p WAVE:ksi. (Zeadally ym., 2012; Uzcategui, De Sucre & Acosta-Marum, 2009.)



KUVIO 2 WAVE-standardit suhteessa OSI-viitemalliin (Uzcátegui ym., 2009; Booysen, Zeadally & Van Rooyen, 2011).

IEEE 802.11p WAVE, kuten myös 802.11 josta se on johdettu, kattaa OSI-viitemallista vain MAC-kerroksen ja fyysisen (PHY) kerroksen (KUVIO 2). IEEE 802.11p -standardi siis määrittelee fyysiselle kerrokselle ja MAC-kerrokselle sellaiset ominaisuudet, joiden avulla IEEE 802.11 voisi toimia ajoneuvojen nopeasti muuttuvassa ympäristössä (Karagiannis ym., 2011). IEEE 802.11p toimii useiden hallintaprotokollien alla, joita ovat IEEE standardit 1609.1-4 (KUVIO 2). Nämä vastaavat resurssien hallinnasta, turvallisuudesta, verkkopalveluista ja kanavan valinnasta. (Zeadally ym., 2012; Toor ym., 2008.) IEEE 1609.3 selittää

myös, miten perinteiset, mutta eivät WAVE:lle ominaiset kuvassa (KUVIO 2) näkyvät protokollat TCP, UDP, IP ja LLC sisällytetään WAVE-järjestelmiin (Uzcátegui ym., 2009). WAVE-standardeissa esitellään myös kaksi elementtiä, joita on hankala sijoittaa OSI-mallin kerroksille: 1609.1-standardissa määritelty resource manager-protokolla ja 1609.2-standardissa määritelty turvallisuusprotokolla (KUVIO 2).

Sisällyttämällä DSRC langattomien lähiverkkojen standardiin IEEE 802.11, WAVE:sta voi tulla maailmanlaajuinen standardi (Zeadally ym., 2012) ja näin ollen myös ensisijainen tiedonvälitysteknologia VANET:ssa. WAVE:n sovitettavuus ajoneuvojen ympäristöihin tekee siitä lupaavan teknologian käytettäväksi liikenteen turvallisuutta parantavissa sovelluksissa. Koska WAVE tukee myös Internet protokollaa (IP, KUVIO 2), mahdollistaa se myös erilaiset Internet-sovellukset käytettäväksi VANET:ssa.

2.4 VANET:n turvallisuussovellukset

Tässä tutkielmassa käsitteellä turvallisuussovellus tarkoitetaan sovelluksia, jotka tarjoavat kuljettajille sellaista informaatiota, jonka avulla he voivat välttää onnettomuuden. Kyky välttää onnettomuuksia voidaan saavuttaa jakamalla tietoa ajoneuvojen sekä tienvarsiyksiköiden kesken. Tätä jaettua tietoa, kuten ajoneuvon sijainti-, nopeus- ja etäisyystietoa sekä risteyksen etäisyystietoa käytetään ennustamaan törmäyksiä. Lisäksi tiedonvaihtoa voidaan käyttää paikantamaan vaarallisia kohtia tiessä, kuten liukkaita mutkia ja kuoppia. (Karagiannis ym., 2011.) Turvallisuussovelluksille yhteistä on siis niiden mahdollisuus estää hengenvaarallisia liikenneonnettomuuksia, sillä ajoneuvojen lähettämät viestit ja varoitukset näiden sovellusten kautta antavat kuljettajille enemmän aikaa reagoida tuleviin tapahtumiin (Raya & Hubaux, 2007).

Monet projektit, standardisointiorganisaatiot ja yhtymät eri puolilla maailmaa, muun muassa Euroopassa ja Yhdysvalloissa, ovat työskennelleet ajoneuvojen kommunikaatiojärjestelmien suunnittelun ja kehityksen parissa. Näiden töiden myötä syntyi alun perin runsaasti erilaisia sovelluksia. Sovelluksille myös määriteltiin niiden toimintaa koskevia vaatimuksia, esimerkiksi kommunikaatiotapa (V2V tai V2I) sekä viiveen sietokyky. (Karagiannis ym., 2011.) Tässä tutkielmassa ei käsitellä jokaista projektia eikä turvallisuussovellusta. Sen sijaan tuodaan muutaman turvallisuussovelluksia käsitelleen projektin avulla esille turvallisuussovellusten monipuolisuus ja sovitettavuus moniin tieliikenteen tilanteisiin, joissa ajoneuvojen törmäys tai muu vaaratilanne on mahdollinen.

Esimerkiksi Yhdysvalloissa VSC-yhtymä (Vehicle Safety Communications Consortium) eritteli ja kuvaili 34 turvallisuussovellusta. Yhtymän projektissa kunkin sovelluksen potentiaalista turvallisuushyötyä arvioitiin, mikä johti kahdeksan korkean potentiaalisen hyödyn turvallisuussovelluksen valintaan ja näiden lähempään tarkasteluun vaatimusten määrittelyä varten. Näitä sovelluksia ovat liikennemerkin rikkomus -varoitus, stop-risteysavustaja (engl. stop

sign movement assistant), vasemmalle kääntymisen avustaja, mutkanopeusvaroitus, elektroninen hätäjarrutusvalo, ennakoiva törmäyksen tunnistaminen, yhteistoiminnallinen kolarivaroitus ja kaistanvaihdon varoitus.

VSC-projektia seurasi kolmivuotinen (2006-2009) VSC-A -projekti (Vehicle Safety Communications–Applications), jossa kehitettiin ja testattiin kommunikaatioon perustuvia, DSRC:hen pohjautuvia V2V-turvallisuusjärjestelmiä. Tätä projektia varten valittiin Yhdysvaltojen liikenneministeriön kolaritietokannasta seitsemän merkittävintä kolaritilannetta, jotka toimivat pohjana projektissa käsiteltävien turvallisuussovellusten valinnalle. Nämä turvallisuussovellukset olivat elektroninen hätäjarrutusvalo, törmäysvaroitus (engl. forward collision warning), kuolleen kulman ja kaistan vaihdon varoitus, ohituskielto -varoitus, risteysavustaja ja hallinnan menetyksen varoitus.

Euroopassa CVIS (Cooperative Vehicle-Infrastructure Systems) -projekti kehitti ja testasi myös useita turvallisuussovelluksia. Näiden sovellusten tarkoitus oli lisätä kuljettajien tietoisuutta heitä ympäröivästä liikenneympäristöstä varoittamalla tien tapahtumista, nopeusrajoituksista, tie- ja sääolosuhteista ja väärään suuntaan ajavista kuljettajista (CVIS-projekti).

Turvallisuussovellukset voisivat siis muun muassa varoittaa autoilijoita kauempana edellä tapahtuneesta onnettomuudesta, jotta lisäonnettomuuksilta, kuten ketjukolareilta, voitaisiin välttyä. Tarpeeksi varhaisessa vaiheessa vastaanotetut varoitukset sen sijaan voisivat estää onnettomuuksia ylipäätään tapahtumasta. Joidenkin tutkimusten mukaan 60 prosenttia onnettomuuksista voitaisiin välttää, mikäli kuljettaja saisi varoituksen puoli sekuntia aikaisemmin ennen törmäyshetkeä. Kun ajoneuvojen nopeudet ovat korkeat, esimerkiksi moottoriteillä, ajoneuvoille jää hyvin vähän aikaa reagoida edellä ajavaan ajoneuvoon. Onnettomuuden sattuessa lähestyvät ajoneuvot usein törmäävät, ennen kuin ehtivät pysähtyä. (Toor, Muhlethaler, Laouiti & La Fortelle, 2008.)

Tärkeä vaatimus turvallisuussovelluksille onkin pystyä vaihtamaan viestejä välittömästi ja tehokkaasti (Toor ym., 2008). Turvallisuussovellukset siis vaativat, että viestit saavuttavat ajoneuvot tiettyyn aikarajaan mennessä. Sovelluksen toiminnasta kuitenkin riippuu, kuinka herkkä sovellus on viiveelle. Toisaalta sovelluksen toiminnasta riippuen viiveen sietokyky voi kasvaa lähteen ja vastaanottajan etäisyyden kasvaessa. (Willke, Tientrakool & Maxemchuk, 2009.)

Tieliikenteessä on siis lukuisia tilanteita, joissa törmäys ajoneuvojen välillä tai muu onnettomuus voi tapahtua. Näitä ovat esimerkiksi risteysalueet, ohitustilanteet, esteet tiellä, kaistan vaihdot ja kaistalle liittymiset (Karagiannis ym., 2011), mikä on nähtävissä myös edellä mainituissa turvallisuussovelluksissa. Lisäksi riski törmäykseen kasvaa ajoneuvon käytöksen muuttuessa nopeasti, esimerkiksi äkkijarrutus ajaessa jonossa, jossa ajoneuvojen väliset turvavälit ovat nopeuteen nähden liian lyhyet. Turvallisuussovellusten toiminnassa on siis kyse myös ihmishengistä tieliikenteessä. Siksi on tärkeää, että ne toimivat oikein ja luotettavasti ja että ne ovat vastustuskykyisiä mahdolliselle väärinkäytölle.

3 TURVALLISUUSSOVELLUSTEN TIETOTURVALLISUUS

Koska VANET mahdollistaa turvallisuuskriittisen tiedon vaihdon ajoneuvojen välillä, on tietoturvallisuus otettava huomioon ennen järjestelmän käyttöönottoa. Ilman tietoturvallisuuden huomioimista VANET :n turvallisuusviestit ovat alttiita muokkaamiselle, hylkäämiselle tai viivästymiselle joko tahallisesta teosta tai järjestelmän toimintahäiriöstä johtuen. Tällä puolestaan voi olla vakavia seurauksia liikenteessä, esimerkiksi liikennekuolemat. (Sun, Zhang, Zhang & Fang, 2010.)

Tässä luvussa määritellään tässä tutkielmassa käytettävä tietoturvallisuuden käsite. Esitellään myös keskeisiä tietoturvallisuusvaatimuksia, jotka VANET:n turvallisuussovellusten tulisi täyttää voidakseen toimia tarkoituksenmukaisesti ja vaaratilanteita aiheuttamatta.

3.1 Tietoturvallisuuden käsite

Von Solms ja Van Niekerk kirjoittavat (2013), että kansainvälinen standardi ISO/IEC 27002 (2005) määrittelee tietoturvallisuuden tiedon luottamuksellisuuden, eheyden ja saatavuuden säilyttämiseksi. Standardin mukaan tietoa voi olla monessa muodossa, kuten paperille tulostettuna ja elektronisena. Suomen kyberturvallisuusstrategiassa (2013) tietoturvallisuudella tarkoitetaan "järjestelyjä, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus". Whitman ja Mattord (2009) Von Solmsin ja Van Niekerkin (2013) mukaan määrittelevät tietoturvallisuuden tiedon sekä tuota tietoa käyttävien, tallentavien ja lähettävien järjestelmien ja laitteiden suojelemiseksi.

Von Solms ja Van Niekerk (2013) huomauttavat, että tietoturvallisuus ei ole tuote tai teknologia, vaan prosessi. Tietoturvallisuus myös määritellään usein turvallisen tiedon ominaisuuksien suhteen. Näitä ominaisuuksia ovat useimmiten luottamuksellisuus, eheys ja saatavuus, mutta ominaisuuksia voi olla enemmänkin.

Tietoturvallisuutta käsiteltäessä usein käytetään myös termiä kyberturvallisuus vastaavana terminä. Näiden kahden termin välillä on kylläkin yhtymäkohtia, mutta täysin toisiaan vastaavia ne eivät ole.

Von Solmsin ja Van Niekerkin (2013) mukaan kyberturvallisuus on tietoturvallisuutta laajempi käsite, mistä syystä se voidaankin nähdä tietoturvallisuuden laajennoksena. Toisin kuin tietoturvallisuudessa, kyberturvallisuudessa on kyse muunkin kuin vain henkilön tai organisaation tiedon tai tietojärjestelmän suojelemisesta. Kyberturvallisuus tarkoittaa myös kybermaailman resursseja käyttävien toimijoiden, kuten henkilöiden ja yhteiskuntien, suojelemista, kun nämä toimijat altistuvat riskeille haavoittuvaisen tieto- ja viestintäteknologian käytön seurauksena. (Von Solms & Van Niekerk, 2013.) Saman suuntaisesti kyberturvallisuus määritellään myös Suomen kyberturvallisuusstrategiassa (2013). Kyberturvallisuuden sanotaan strategiassa käsittävän toimenpiteet, jotka kohdistuvat yhteiskunnan elintärkeisiin toimintoihin ja kriittiseen infrastruktuuriin. Näillä toimenpiteillä pyritään ennakoivasti hallitsemaan ja sietämään kyberuhkia sekä niiden vaikutuksia, "jotka voivat aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle".

Kyberturvallisuudessa on siis mukana myös kybertoimintaympäristön toimijoiden, kuten ihmisten ja yhteiskuntien turvallisuus, toisin kuin tietoturvallisuudessa, joka käsittää vain tiedon ja sitä käyttävien järjestelmien turvallisuuden. Yksi merkittävä ero kyberturvallisuuden ja tietoturvallisuuden välillä myös on, että sekä ihmisiä että yhteiskuntaa laajassa mittakaavassa voidaan vahingoittaa kyberturvallisuushyökkäyksillä, kun taas tietoturvallisuudessa haitta on yleensä epäsuoraa (Von Solms & Van Niekerk, 2013).

Professori Jarno Limnéll on puolestaan ehdottanut, tulisiko kyber -etuliite jättää pois kyberturvallisuudesta puhuessa, sillä digitaalisesta maailmasta on tullut erottamaton osa turvallisuutta. Hänen näkemyksensä mukaan tulisi jatkossa siirtyä kontrolli- ja teknologiakeskeisestä kyberturvallisuudesta yhä enemmän ihmiskeskeisen turvallisuuden korostamiseen.

Edellä esiteltyjen määritelmien perusteella tultiin siihen johtopäätökseen, että termi kyberturvallisuus sekä etuliite "kyber" ulottuvat merkityksessään tämän tutkielman laajuuden ulkopuolelle, sillä tässä tutkielmassa ei käsitellä hyökkäyksiä ajoneuvojen fyysistä turvallisuutta kohtaan. Tässä tutkielmassa aiheen käsittelyn selkeyden vuoksi käytetään kuitenkin termiä tietoturvallisuus korostamaan VANET:n eli ajoneuvojen välisten verkkojen, sitä käyttävien turvallisuussovellusten ja elektronisessa muodossa olevan tiedon turvallisuutta.

3.2 Tietoturvallisuusvaatimukset VANET:n turvallisuussovelluksille

Jotta järjestelmä, eli tämän tutkielman tapauksessa VANET:n turvallisuussovellus, voisi olla vastustuskykyinen uhille ja hyökkäyksille, tulee sen täyttää tietyt tietoturvallisuusvaatimukset. VANET:iin sekä sen avulla toimiviin turvalli-

suussovelluksiin liittyvät tietoturvallisuusvaatimukset vaihtelevat kuitenkin hieman eri lähteiden välillä. Tämä johtunee siitä, että VANET sekä sen pohjalla toimivat turvallisuussovellukset ovat vielä varsin tuoreita ilmiöitä, jolloin myös niihin liittyvät tietoturvallisuusvaatimukset eivät ole vielä vakiintuneita. Sovelluksen tietoturvallisuusvaatimukset riippuvat myös sovelluksen käyttämästä tiedonvaihtotyypistä (Hamida, Noura & Znaidi, 2015).

Raya ja Hubaux (2007) keskittyvät tutkimuksessaan turvallisuussovellusten turvallisuuteen. Heidän mukaansa turvallisuusviesteille tarkoitetun järjestelmän tulisi täyttää seuraavat vaatimukset: saatavuus, todennus, kiistämättömyys, datan johdonmukaisuuden varmistaminen, yksityisyys ja reaaliajan rajoitteet.

Saatavuudella taataan ajoneuvojen verkon toimivuus ja hyödyllisen tiedon saatavuus mihin aikaan tahansa (Mejri, Ben-Othman & Hamdi, 2014). Saatavuus käsittää VANET:ssa toimivien turvallisuussovellusten palvelujen saatavuuden vaihtoehtoisinkin keinoin myös silloin, kun jokin hyökkäys (Raya & Hubaux, 2007) tai muu toimintahäiriö on kaatanut verkon.

Todennus (engl. authentication) on yksi keskeisimmistä vaatimuksista mille tahansa järjestelmälle (Engoulou, Bellaïche, Pierre & Quintero, 2014). Turvallisuusviestien lähettäjät tulee pystyä todentamaan, sillä ajoneuvojen reaktiot turvallisuusviesteihin tulee perustua aitoihin viesteihin. Todennuksella varmistetaan, että viesti vastaanotetaan luotettavalta lähettäjältä (Raya & Hubaux, 2007.) Todennuksen tarkoituksena on siis suojella aitoja verkon solmuja (VANET:n tapauksessa ajoneuvoja sekä tienvarsiyksikköjä) ulkopuolisilta tai sisäpuolisilta hyökkääjiltä, jotka yrittävät soluttautua verkkoon käyttämällä väärennettyä identiteettiä (Mejri ym., 2014).

Kiistämättömyydellä tarkoitetaan sitä, että viestin lähettäjä ei voi kiistää lähettäneensä viestin (Papadimitratos ym., 2008). Kiistämättömyys on todiste vastaanottajalle, että lähettäjä on vastuussa luomistaan viesteistä (Engoulou ym., 2014). Kiistämättömyys on esimerkiksi onnettomuuksien yhteydessä tärkeä turvallisuusvaatimus. Kun kuljettaja ei pysty kiistämään lähettämiään viestejä, pystytään selvittämään ennen onnettomuutta lähetettyjen viestien järjestys ja sisältö, mikä on onnettomuuden tutkinnan kannalta tärkeää (Raya & Hubaux, 2007).

Datan johdonmukaisuuden varmistamista voidaan kutsua myös uskottavuudeksi. Vaikka lähettäjä olisi aito, itse turvallisuusviesti voi olla valheellinen. Uskottavuus-vaatimuksella tarkoitetaankin turvallisuusviestien johdonmukaisuutta muiden samankaltaisten, lähes samaan aikaan ja samassa paikassa luotujen turvallisuusviestien kanssa. (Raya & Hubaux, 2007.) Huomautettakoon, että Raya ja Hubaux (2007) käyttävät artikkelissaan termejä datan johdonmukaisuuden varmistaminen ja uskottavuus, mutta muissa lähteissä datan johdonmukaisuuden vaatimus tunnetaan terminä eheys (engl. integrity) (Mejri ym., 2014; Engoulou, ym., 2014; Hamida ym., 2015).

Yksityisyys on perusihmisoikeus ja Suomessakin on säädetty lukuisia yksityisyyttä suojelevia lakeja. Jo tästä syystä yksityisyys tulee ottaa huomioon VANET:n turvallisuussovelluksia kehitettäessä. Kuljettajien yksityisyys luva-

tonta tarkkailua vastaan tulee taata (Raya & Hubaux, 2007). Kuljettajien ja ajoneuvojen identiteettien ei pitäisi olla helposti tunnistettavissa liikenteessä vaihdetuista viesteistä ja kuljettajan oikeutta hallita pääsyä henkilökohtaisiin tietoihinsa tulisi vahvistaa (Hamida ym., 2015).

Reaaliajan rajoitteet tulee ottaa huomioon suunniteltaessa turvallista järjestelmää turvallisuusviestien vaihtoon. Monet kaavaillut turvallisuussovellukset asettavat tiukkoja aikarajoja viestien lähetykselle (Raya, Papadimitratos & Hubaux, 2006) VANET:ssa, sillä viiveet tekevät joistakin turvallisuusviesteistä tarpeettomia tai aiheuttavat vakavia seurauksia (Engoulou ym., 2014). Reaaliajan rajoite voidaankin nähdä sisältyvän edellä mainittuun saatavuusvaatimukseen. VANET ei täytä saatavuuden vaatimuksia, mikäli sen välityksellä turvallisuusviestit eivät ehdi ajoissa perille kuljettajille, jotta nämä voisivat tehdä viestien pohjalta turvallisuutensa kannalta merkittäviä päätöksiä liikenteessä.

Tietoturvaa käsiteltäessä usein nousee esille saatavuuden lisäksi myös luottamuksellisuus. Koska turvallisuusviestit eivät sisällä luottamuksellista (salausta vaativaa) tietoa, tätä vaatimusta ei tarvita (Raya & Hubaux, 2007) eikä siihen liittyviä uhkia käsitellä tässä tutkielmassa.

4 VANET:IIN KOHDISTUVIA HYÖKKÄYSTYYPPEJÄ

Tässä luvussa vastataan tutkielman toiseen tutkimuskysymykseen eli siihen, millaisia tietoturvauhkia kohdistuu turvallisuussovelluksiin. Tämä voidaan selvittää tutkimalla VANET:iin kohdistuvia hyökkäyksiä. Tässä luvussa tuodaankin ensimmäiseksi esille VANET:n sekä turvallisuussovellusten välinen yhteys, jonka vuoksi on tärkeää tutkia VANET:iin kohdistuvia hyökkäyksiä. Hyökkäyksiä lähestytään tässä luvussa sen kautta, minkä tietoturvavaatimuksen täyttymisen tietty hyökkäys vaarantaa. Hyökkäysten vaikuttavuutta tietoturvavaatimuksia kohtaan havainnollistetaan aluksi taulukon avulla luvussa 4.2. Lopuksi esitellään esimerkkihyökkäys kutakin luvussa 3.2 esiteltyä tietoturvavaatimusta kohtaan ja hyökkäyksen merkittävyys turvallisuussovellusten kontekstissa.

4.1 Hyökkäysten merkitys VANET:ssa

Kuten luvussa 2 todettiin, älykkäiden liikennejärjestelmien tärkeä komponentti on VANET, joka mahdollistaa tiedonvaihdon ajoneuvojen välillä (Cunha ym., 2016). Turvallisuussovellukset ovat keskeinen ajovoima VANET:lle (Qian & Moayeri, 2008), eli VANET:ia kehitetään pääosin juurikin turvallisuussovellusten käytön mahdollistamiseksi (De Fuentes, González-Tablas & Ribagorda, 2011).

Turvallisuussovelluksille keskeinen vaatimus on kyky kerätä informaatiota ajoneuvon sensoreilta, muilta ajoneuvoilta tai molemmilta prosessoidakseen ja levittääkseen informaatiota turvallisuusviestien muodossa muille ajoneuvoille tai infrastruktuurille sovelluksen toiminnasta riippuen (Al-Sultan, Al-Doori, Al-Bayatti & Zedan, 2014). VANET siis mahdollistaa sen, että nämä turvallisuussovellukset pystyvät levittämään informaatiota muille ajoneuvoille tai tienvarsiyksiköille. Näin ollen turvallisuussovellukset käyttävät VANET:ia levittääkseen informaatiota, sillä VANET:ia kehitetään ensisijaisesti turvallisuus-

sovellusten mahdollistamiseksi. VANET:n ja turvallisuussovellusten välillä on siis tiivis yhteys.

Ajoneuvojen verkoissa käytetyllä langattomalla teknologialla on kuitenkin epäkohtia. Nämä epäkohdat jättävät verkon haavoittuvaksi erilaisille hyökkäyksille, jotka kohdentuvat tämän tyyppiseen tiedonsiirtoteknologiaan. Kun otetaan huomioon ajoneuvojen verkkojen arkkitehtuuri, joka käsittää melkein seitsemän kerrosta OSI-mallin mukaan, hyökkäyksiä ja haavoittuvuuksia liittyy joka kerrokseen aina fyysiseltä kerrokselta sovelluskerrokselle. Kuten mikä tahansa muukin tiedonvaihtoa ja dataa prosessoiva järjestelmä, VANET on altis erilaisille uhkille ja hyökkäyksille. (Mejri ym. 2014.)

Koska turvallisuussovellusten toiminnassa on myös kyse ihmishengistä (Qian & Moayeri, 2008) ja koska turvallisuussovellukset levittävät turvallisuuskriittistä informaatiota VANET:n avulla, on tärkeää suojata VANET väärinkäytöltä (Qian & Moayeri, 2008). VANET:iin kohdistuvat hyökkäykset vaikuttavat siis myös turvallisuussovellusten toimintaan, mistä syystä on tärkeää tutkia, millaisille hyökkäyksille ja uhkille VANET on altis.

4.2 Hyökkäystyyppien esittely

Koska VANET ja sen tietoturvallisuus ovat tuoreita tutkimuksen kohteita, VANET:iin liittyvien hyökkäysten luokittelu ei ole vakiintunutta, mikä näkyy lähteissä lievinä ristiriitaisuuksina. Lähteiden perusteella näyttää siltä, että hyökkäysten vaikuttavuus tiettyihin vaatimuksiin on jokseenkin jopa tulkinnanvaraista. Esimerkiksi Mejrin ym. (2014) artikkelin luokittelussa monilähetyksen peukalointi luokitellaan saatavuuteen vaikuttaviin hyökkäyksiin. Hamidan ym. (2015) taulukossa (TAULUKKO 1) monilähetyksen peukalointi koskettaa sen sijaan yksinomaan eheyttä. Engouloun ym. (2014) artikkelissa palvelunestohyökkäyksen sanotaan vaikuttavan saatavuuden ohella myös eheyteen, kun taas Hamidan ym. (2015) luokittelussa kyseinen hyökkäys vaikuttaa vain saatavuuteen. Tähän mennessä julkaistut artikkelit hyökkäysten luokittelusta VANET:ssa voidaankin nähdä alustavina ja suuntaa antavina. On myös mahdollista, että hyökkäyksiä ilmenee tulevaisuudessa lisää, kun VANET lopulta otetaan käyttöön (Engoulou ym., 2014).

Tähän tutkielmaan valittiin havainnollistavaksi esimerkiksi Hamidan ym. (2015) taulukko (TAULUKKO 1), sillä se joistakin eroavaisuuksistaan huolimatta sisältää myös runsaasti yhtäläisyyksiä muihin hyökkäysten vaikuttavuutta käsitteleviin lähteisiin. Muissa lähteissä ei myöskään löytynyt vastaavanlaista taulukkoa, johon olisi merkitty yhden hyökkäyksen vaikuttavuus useampaankin kuin yhteen vaatimukseen.

Taulukosta (TAULUKKO 1) luottamuksellisuusvaatimus on rajattu pois, sillä kuten luvussa 3.2 todettiin, turvallisuussovellusten lähettämät turvallisuusviestit eivät sisällä salaamista vaativaa tietoa, joten luottamuksellisuutta ei tarvita niiden tapauksessa (Raya & Hubaux, 2007). Näin ollen siihen kohdistuvia hyökkäyksiä ei myöskään käsitellä tässä tutkielmassa.

Kuten taulukosta (TAULUKKO 1) nähdään, yksi hyökkäys voi vaarantaa useamman kuin yhden tietoturvallisuusvaatimuksen. Aiheen käsittelyn selkeyttämiseksi ei tarkastella jokaista hyökkäystä yksitellen. Sen sijaan tarkastellaan hyökkäyksiä tietoturvallisuusvaatimusten kautta siten, että esitellään kullekin vaatimukselle esimerkkihyökkäys, joka vaarantaa kyseisen vaatimuksen toteutumisen turvallisuussovelluksissa.

TAULUKKO 1 Hyökkäykset ja murretut tietoturvallisuusvaatimukset (Hamida ym., 2015).

Murrettu tietoturvallisuusvaatimus / **Hyökkäys**	**Saatavuus**	**Todennus**	**Kiistämättömyys**	**Eheys**	**Yksityisyys**
Palvelunestohyökkäys	✓				
Häirintä (jamming attack)	✓				
Sybil	✓	✓			
Palvelunestohyökkäyksen variantit (mm. madonreikä, haittaohjelmat)	✓	✓	✓	✓	✓
Tapahtumien jäljitettävyyden menetys			✓		
Illuusio		✓		✓	
Toisto		✓		✓	
Avaimen ja/ tai sertifikaatin toisto		✓			
GPS:n huijaus / sijainnin väärentäminen		✓			✓
Viestin peukalointi	✓		✓	✓	
Monilähetyksen (broadcast) peukalointi				✓	
Solmun imitointi		✓	✓	✓	
Raaka voima (brute force)					
Salakuuntelu					
Liikenteen analyysi					✓
Jäljitys / sosiaalinen manipulointi (social engineering)					✓
Ajoitushyökkäys	✓				
Man-in-the-middle		✓	✓	✓	

Hyökkäysten ohella tulisi ymmärtää myös, millaiset hyökkääjät tähtäisivät järjestelmään ja millaisin motiivein (Khan Pathan, 2010, 232). Hyökkääjien ja heidän motiiviensa tarkastelu jää kuitenkin tämän tutkielman laajuuden ulkopuolelle.

Seuraavaksi käydään läpi VANET:iin kohdistuvia, jo tunnistettuja hyökkäyksiä. Lähestytään hyökkäyksiä luvussa 3.2 esitettyjen tietoturvallisuusvaatimuksien sekä niihin vaikuttavien hyökkäyksien kautta (TAULUKKO 1).

4.3 Hyökkäyksiä saatavuutta kohtaan

Palvelunestohyökkäys on esimerkki hyökkäyksestä saatavuutta kohtaan (TAULUKKO 1). VANET:ssa palvelunestohyökkäyksessä hyökkääjä kuormittaa tiedonvaihtokanavaa esimerkiksi suurella määrällä turhia viestejä, minkä seurauksena verkko kaatuu (Raya & Hubaux, 2007; Laurendeau & Barbeau, 2006) ja ajoneuvot lakkaavat lähettämästä ja vastaanottamasta turvallisuuskriittistä informaatiota (Samara, Al-Salihy, & Sures, 2010). Samalla saatavuus ja reaaliajan vaatimukset eivät täyty.

Turvallisuussovellukset asettavat tiukat aikarajat viestien lähetykselle ja vastaanottamiselle (Raya ym., 2006) eli ne ovat hyvin herkkiä viiveelle. Esimerkiksi yhteistoiminnallisessa törmäysvaroitusjärjestelmässä vain muutaman sekunnin viive voi tehdä varoitusviestit turhiksi (Parno & Perrig, 2005). Tämä puolestaan voi aiheuttaa onnettomuuksia, jos kuljettajat vastaanottavat varoitusviestin liian myöhään ehtiäkseen reagoimaan, esimerkiksi jarruttamaan ajoissa. Reaaliajan vaatimusten tavoittaminen tekeekin VANET:sta alttiin palvelunestohyökkäyksille (Parno & Perrig, 2005). Alttius palvelunestohyökkäyksille johtuu myös siitä, että VANET:ssa voi olla suuri määrä osallistuvia solmuja, eli ajoneuvoja ja tienvarsiyksikköjä (Faezipour, Nourani, Saeed & Addepalli, 2012) ja koska VANET:ssa käytetty langaton teknologia on luonteeltaan avoin (Hasbullah & Soomro, 2010).

4.4 Hyökkäyksiä todennusta kohtaan

Koska VANET:ssa kaikki ajoneuvot voivat lähettää ja vastaanottaa viestejä (ETSI, 2010), tarvitaan todennusta, jotta voidaan varmistua lähettäjän luotettavuudesta ja suojella verkkoa hyökkääjiltä, jotka yrittävät soluttautua verkkoon väärillä identiteeteillä, kuten luvussa 3.2 todettiin. Haavoittuvuus todennusvaiheessa voi altistaa koko verkon hyökkääjille, sillä väärennettyjen identiteettien käyttö mahdollistaa monia hyökkäyksiä (Hamida ym., 2015), esimerkiksi Sybil-hyökkäyksen (Parno & Perrig, 2005).

Sybil-hyökkäyksessä haitallinen ajoneuvo imitoi monta muuta ajoneuvoa häiritäkseen VANET :n sovellusten normaalia toimintaa (Kumar & Maheshwari, 2014). Esittämällä useaa ajoneuvoa samanaikaisesti on mahdollista suorittaa monia muita hyökkäyksiä VANET:ia kohtaan. Nämä väärennetyt identiteetit luovat myös illuusion ylimääräisistä ajoneuvoista tiellä ja väärentävät muiden ajoneuvojen sijaintia verkossa (RoselinMary, Maheshwariv & Thamaraiselvan, 2013). Illuusion lisäksi Sybil-hyökkäyksessä hyökkääjällä on mahdollista syöttää väärennettyä tietoa VANET:iin esittämiensä olemattomien ajoneuvojen kautta (Xiao, Yu, & Gao, 2006).

Sybil-hyökkäys on haitallinen esimerkiksi sellaisissa turvallisuussovelluksissa, joissa ajoneuvo jarruttaessaan voimakkaasti lähettää varoitusviestejä seu-

raaville ajoneuvoille, jotka puolestaan välittävät viestit edelleen eteenpäin niitä seuraaville ajoneuvoille. Sybil-hyökkäyksessä lukuisat väärennetyt ajoneuvot voivat puuttua tähän viestin edelleenvälitykseen, mikä voi johtaa mittaviin ketjukolareihin esimerkiksi moottoritiellä ja potentiaalisesti myös liikennekuolemiin. (Xiao ym., 2006.)

4.5 Hyökkäyksiä kiistämättömyyttä kohtaan

Kiistämättömyys riippuu todennuksesta. Kiistämättömyys luo kuitenkin vankan todisteen, kun järjestelmä voi tunnistaa haitalliset ajoneuvot, jotka eivät pysty kiistämään haitallisia toimiaan verkossa. (Hamida ym., 2015.) Voidaan siis ajatella, että haavoittuvuudet todennuksessa altistavat VANET:n myös kiistämättömyyteen kohdistuviin hyökkäyksiin.

Esimerkki hyökkäyksestä kiistämättömyyttä kohtaan on imitointi. Tässä hyökkäyksessä hyökkääjä, eli haitallinen ajoneuvo, anastaa toisen ajoneuvon identiteetin, ennen kuin alkaa suorittaa muita haitallisia toimia. Kun viranomaiset lopulta yrittävät jäljittää syyllistä esimerkiksi sattuneeseen onnettomuuteen, he saattavat pidättää viattoman henkilön, mikäli verkko sisältää erheellistä tietoa. (Enguolou ym., 2014.)

4.6 Hyökkäyksiä eheyttä kohtaan

Johtuen VANET:ssa käytetyn langattoman teknologian avoimesta luonteesta VANET on altis myös väärän tiedon levitykselle (Hasbullah & Soomro, 2010), eli hyökkäyksille eheyttä kohtaan. Toisaalta voidaan luoda eheysmekanismeja, jotka auttavat suojelemaan informaatiota haitallista muokkausta, poistamista tai lisäämistä vastaan (Mejri ym., 2014). Haavoittuvuudet eheyden varmistamisessa antavat kuitenkin haitalliselle ajoneuvolle mahdollisuuden suorittaa turvallisuusviestien eheyttä rikkovia hyökkäyksiä. Tällaiset hyökkäykset koskevat pääosin V2V-kommunikaatiota niiden heikkouden vuoksi (Mejri ym., 2014).

Esimerkiksi haitallinen ajoneuvo voi lähettää väärennettyjä turvallisuusviestejä tiettyä tarkoitusta varten muille ajoneuvoille. Tällainen viesti voi olla muun muassa väärennetty liikenneruuhkasta varoittava viesti, jotta haitallinen ajoneuvo itse voi saada paremmat tieolosuhteet. (Lin, Sun, Ho & Shen, 2007.) Tämä puolestaan voi aiheuttaa ruuhkia muualla, kun ihmiset valitsevat vaihtoehtoisia reittejä.

4.7 Hyökkäyksiä yksityisyyttä kohtaan

Langattoman tiedonvaihdon avoimen luonteen vuoksi hyökkääjä voi helposti salakuunnella verkon liikennettä VANET:ssa (Lin ym., 2007; Cencioni & Di Pietro, 2008; Wiedersheim, Ma, Kargl & Papadimitratos, 2010), mitä edesauttaa VANET:n toteutukseen kaavailtu 802.11-pohjainen radioteknologia (Cencioni & Di Pietro, 2008). Lisäksi monet visioidut VANET:n sovellukset, myös turvallisuussovellukset, luottavat sijainti- ja aikatietoon. Tämä vaatii kaikkia ajoneuvoja toistuvasti lähettämään aikaleimatun sijaintinsa avoimesti läheisille ajoneuvoille. (Wiedersheim ym., 2010.) Ajoneuvojen lähettämät turvallisuusviestit tarjoavat siis runsaasti tietoa niiden lähettäjästä (Cencioni & Di Pietro, 2008). Näin ollen VANET ja turvallisuussovellukset ovat alttiita yksityisyyttä loukkaaville hyökkäyksille.

Yksi vakavimmista uhkista yksityisyydelle VANET:ssa on liikenteen analyysi -hyökkäys (Isaac, Zeadally & Camara, 2010). Liikenteen analyysi -hyökkäyksessä hyökkääjä kuuntelee verkkoa ja kerää siitä informaatiota tietyn ajan, minkä jälkeen hyökkääjä yrittää hyödyntää kerättyä informaatiota omiin tarkoituksiinsa (Mejri ym., 2014). Hyökkääjä voi esimerkiksi jäljittää ajoneuvon sen fyysisen sijainnin ja liikkumiskaavan suhteen (Lin ym., 2007). Turvallisuussovellusten toiminnalle keskeistä sijaintitietoa voidaan myös väärinkäyttää. Kerätystä sijaintitiedosta hyökkääjä voi luoda ajoneuvoista ja niiden kuljettajista sijaintiprofiileja. Kun hyökkääjällä on hallussaan tällaisia sijaintiprofiileja, voi helposti murtaa kuljettajien yksityisyyden, sillä kuljettajan ja hänen ajoneuvonsa välillä on vahva korrelaatio (useimmilla ajoneuvoilla on vain muutama käyttäjä). (Wiedersheim ym., 2010.)

5 YHTEENVETO

Tässä tutkielmassa käytiin läpi älyliikenteen sekä älykkäiden liikennejärjestelmien käsitteet sekä todettiin, että varsinkin automaattisen tiedonvaihdon lisääminen tiellä liikkujien kesken voi parantaa muun muassa liikenneturvallisuutta. Automaattisen tiedonvaihdon mahdollistajaksi tieliikenteessä esiteltiin ajoneuvojen langattomat verkot eli VANET, jonka perustoimintaperiaate ja standardit tuotiin esille. Käytiin läpi esimerkkejä VANET:n mahdollistamista turvallisuussovelluksista, joiden lähettämien viestien avulla kuljettajat voivat saada lisää reagointiaikaa liikenteen tapahtumiin ja näin muun muassa välttää onnettomuuksia. Seuraavaksi määriteltiin tietoturvallisuuden käsite sekä millaiset tietoturvallisuusvaatimukset turvallisuusviesteille tarkoitetun järjestelmän VANET:ssa tulisi täyttää voidakseen toimia tarkoituksenmukaisella tavalla. Lopuksi tuotiin esille VANET:iin liittyviä tietoturvauhkia, jotka vaikuttavat myös turvallisuussovellusten toimintaan.

VANET:n avulla on mahdollista toteuttaa Suomen älyliikenteen strategian turvallisuustavoitteet, sillä VANET mahdollistaa strategiassa mainitut yhteistoiminnalliset järjestelmät. Näiden järjestelmien sanotaan olevan keskeisessä roolissa liikenneonnettomuuksien ehkäisyssä, sillä niiden avulla ajoneuvot voivat vaihtaa keskenään sekä liikenneinfrastruktuurin kanssa tärkeää liikennetietoa. Tällaiset järjestelmät, eli turvallisuussovellukset, ovat sovitettavissa lukuisiin eri liikenteen tilanteisiin, joissa ajoneuvojen välinen törmäys on mahdollinen, esimerkiksi risteysalueet ja kaistanvaihdot.

Tutkielman tuloksista käy kuitenkin ilmi, että VANET:iin, samoin kuin muihinkin langattomiin verkkoihin, kohdistuu lukuisia hyökkäyksiä. Nämä hyökkäykset vaarantavat samalla VANET:n avulla toimivien turvallisuussovellusten toiminnan, mikä koskettaa lopulta myös ihmishenkiä tieliikenteessä. Väärin toimivat turvallisuussovellukset voivat kääntyä toimimaan tarkoitustaan vastaan ja alkaa aiheuttaa liikenneonnettomuuksia. Esimerkiksi jos hyökkäyksen seurauksena katoaa edellä sattuneesta onnettomuudesta varoittavia turvallisuusviestejä niiden lähetyksen aikana, seurauksena voi olla ketjukolari. Samalla kuljettajien luottamus järjestelmään voi kärsiä. Turvallisuussovellusten toiminnalla ei ole juurikaan pohjaa, mikäli niiden käyttäjät varoituksen saades-

saan eivät usko varoituksen paikkansapitävyyteen. Turvallisuussovellusten kyky parantaa liikenneturvallisuutta ja ehkäistä onnettomuuksia jää hyödyntämättä, mikäli niiden toimintaan ei luoteta. Jo tästäkin syystä VANET:n ja sen pohjalla toimivien turvallisuussovellusten tietoturvallisuus tulisi rakentaa mahdollisimman vastustuskykyiseksi erilaisille uhkille, mukaan lukien tässäkin tutkielmassa esitellyille hyökkäyksille.

Tämän tutkielman tulokset voidaankin nähdä suuntaa antavana listana uhkista, jotka tulee ottaa huomioon ennen VANET:n sekä turvallisuussovellusten laajamittaista käyttöönottoa. On tärkeää olla tietoinen uhkista jo suunniteltaessa VANET:n ja turvallisuussovellusten kaltaisia järjestelmiä. Pelkkien haavoittuvuuksien ja niihin kohdistuvien hyökkäysten kartoitus ei kuitenkaan riitä, vaan tarvitaan myös ymmärrystä hyökkääjistä sekä heidän mahdollisista motiiveistaan. Koska VANET on hyvin tuore ilmiö, kaikkia mahdollisia siihen kohdistuvia uhkia ei välttämättä ole vielä edes tunnistettu, vaan niitä voi ilmetä tulevaisuudessa lisää. Tarvitaan siis runsaasti lisää tutkimusta aiheesta.

Koska kandidaatin tutkielma ei ole luonteeltaan kovin laaja tutkimus, jää aiheen käsittely väistämättä hyvin rajalliseksi. Tässä tutkielmassa ei esimerkiksi käsitelty hyökkääjien ominaisuuksia, ajoneuvon fyysistä turvallisuutta eikä VANET:n ja turvallisuussovellusten teknisempiä näkökulmia ja ratkaisuja. Tietoturvallisen VANET:n suunnittelun kannalta ne ovat kuitenkin tärkeitä huomioon otettavia asioita. Myöskin mahdolliset ratkaisut esiteltyihin tietoturvauhkiin jäivät käsittelyn ulkopuolelle tässä tutkielmassa. Tutkielma antoikin yleisellä tasolla silmäyksen laajasta aiheesta. Tämän tutkielman myötä voisinkin jatkaa aiheen käsittelyä myöhemmin pro gradu -tutkielmassa. Voisin esimerkiksi tutkia, millaisilla turvallisuusprotokollilla tässä tutkielmassa esitellyt tietoturvallisuusvaatimukset voivat täyttyä. Voisin myös tutkia ratkaisuja tässä tutkielmassa löytyneisiin tietoturvallisuusuhkiin. VANET:n mahdollistamien turvallisuussovellusten hyödyt vaikuttavat kuitenkin niin merkittäviltä, että niiden käyttöönotto voisi olla erityisesti liikenneturvallisuuden kannalta kannattavaa, mutta vain mikäli tietoturvanäkökulmat otetaan jo varhaisessa vaiheessa huomioon. Tietoturvan huomioimisella voidaan varmistaa, että uusi järjestelmä ei muutu vain uudeksi rikollisten keinoksi hyötyä taloudellisesti, vahingoittaa ihmisiä tai suorittaa muita haitallisia toimia.

LÄHTEET

Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H. & Zedan, H. (2014). A comprehensive survey on vehicular ad hoc network. *Journal of Network and Computer Applications, 37*, 380-392.

Booysen, M. J., Zeadally, S. & van Rooyen, G. J. (2011). Survey of media access control protocols for vehicular ad hoc networks. *IET Communications, 5*(11), 1619-1631. doi:10.1049/iet-com.2011.0085.

Cencioni, P. & Di Pietro, R. (2008). A mechanism to enforce privacy in vehicle-to-infrastructure communication. *Computer Communications, 31*(12), 2790-2802.

Chen, R., Jin, W. & Regan, A. (2010). Broadcasting safety information in vehicular networks: Issues and approaches. *IEEE Network, 24*(1).

Cheng, H. T., Shan, H. & Zhuang, W. (2011). Infotainment and road safety service support in vehicular networking: From a communication perspective. *Mechanical Systems and Signal Processing, 25*(6), 2020-2038. doi://dx.doi.org/10.1016/j.ymssp.2010.11.009

Cunha, F., Villas, L., Boukerche, A., Maia, G., Viana, A., Mini, R. A. & Loureiro, A. A. (2016). Data communication in VANETs: Protocols, applications and challenges. *Ad Hoc Networks, 44*, 90-103.

CVIS D2.2, "Use cases and system requirements". (2006). IST CVIS Project, CVIS IST-4-027293-IP deliverable D2.2 version 1.0.

Engoulou, R. G., Bellache, M., Pierre, S. & Quintero, A. (2014). VANET security surveys. *Computer Communications, 44*, 1-13. doi:10.1016/j.comcom.2014.02.020.

ETSI, Intelligent transport systems (its), security, threat, vulnerability and risk analysis (tvra). (2010). Technical Report ETSI TR 102 893 V1.1.1.

Faezipour, M., Nourani, M., Saeed, A. & Addepalli, S. (2012). Progress and challenges in intelligent vehicle area networks. *Communications of the ACM, 55*(2), 90-100.

Figueiredo, L., Jesus, I., Machado, J. A. T., Ferreira, J. R. & Martins de Carvalho, J. L. (2001). *Towards the development of intelligent transportation systems* doi:10.1109/ITSC.2001.948835.

Fuentes, J. M. d., Gonzlez-Tablas, A. I. & Ribagorda, A. (2010). Overview of security issues in vehicular ad-hoc networks.

Giannoutakis, K. N. & Li, F. (2012). Making a business case for intelligent transport systems: A holistic business model framework. *Transport Reviews, 32*(6), 781-804. doi:10.1080/01441647.2012.740096.

HAAS Alert. (19.3.2017). Haettu osoitteesta https://www.haasalert.com/

Hafeez, K. A., Zhao, L., Ma, B. & Mark, J. W. (2013). Performance analysis and enhancement of the DSRC for VANET's safety applications. *IEEE Transactions on Vehicular Technology, 62*(7), 3069-3083. doi:10.1109/TVT.2013.2251374.

Hamida, E. B., Noura, H. & Znaidi, W. (2015). Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures. *Electronics, 4*(3), 380-423.

Harri, J., Filali, F. & Bonnet, C. (2009). Mobility models for vehicular ad hoc networks: A survey and taxonomy. *IEEE Communications Surveys & Tutorials, 11*(4), 19-41. doi:10.1109/SURV.2009.090403.

Hartenstein H. & Laberteaux, L. P. (2008). A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine, 46*(6), 164-171. doi:10.1109/MCOM.2008.4539481.

Hasbullah, H., Soomro, I. A. & Ab Manan, J. -. (2010). Denial of service (DOS) attack and its possible solutions in VANET. *World Academy of Science, Engineering and Technology, 65*, 411-415.

Isaac, J. T., Zeadally, S. & Cmara, J. S. (2010). Security attacks and solutions for vehicular ad hoc networks. *IET Communications, 4*(7), 894-903. doi:10.1049/iet-com.2009.0191.

ISO/IEC 27002: Code of practice for information security management (2005).

Jiang, D., Taliwal, V., Meier, A., Holfelder, W. & Herrtwich, R. (2006). Design of 5.9 ghz dsrc-based vehicular safety communication. *IEEE Wireless Communications, 13*(5), 36-43. doi:10.1109/WC-M.2006.250356.

Kansallinen älyliikenteen strategia (2009). Selvitysmiehen ehdotus. Liikenne- ja viestintäministeriö. Haettu 19.3.2017 osoitteesta http://julkaisut.valtioneuvosto.fi/handle/10024/78225

Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K. & Weil, T. (2011). Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Communications Surveys & Tutorials, 13*(4), 584-616. doi:10.1109/SURV.2011.061411.00019.

Khan Pathan, A. (2010). *Security of self-organizing networks: MANET, WSN, WMN, VANET.* Auerbach Publications.

Kohti uutta liikennepolitiikkaa. Älyä liikenteeseen ja viisautta liikkujille. Toisen sukupolven älystrategia liikenteelle. (2013). Liikenne- ja viestintäministeriö. Haettu 19.3.2017 osoitteesta http://julkaisut.valtioneuvosto.fi/handle/10024/77969

Kulmala, R. (2010). Ex-ante assessment of the safety effects of intelligent transport systems. *Accident Analysis & Prevention, 42*(4), 1359-1369. doi://dx.doi.org/10.1016/j.aap.2010.03.001.

Kumar, P. V., & Maheshwari, M. (2014). Prevention of Sybil attack and priority batch verification in VANETs. Teoksessa *Information Communication and Embedded Systems (ICICES), 2014 International Conference on* (1-5). IEEE.

Laurendeau, C., & Barbeau, M. (2006). Threats to Security in DSRC/WAVE. Teoksessa *International Conference on Ad-Hoc Networks and Wireless* (266-279). Springer Berlin Heidelberg.

Limnéll, J. (20.9.2016). Kyberturvallisuus osana tämän päivän turvallisuutta. Kyber kaikkialla -luentosarja. Jyväskylän yliopiston informaatioteknologian tiedekunta & Keski-Suomen kadettipiiri. Haettu 17.2.2017 osoitteesta https://moniviestin.jyu.fi/ohjelmat/it/panu/kyber/kyber-kaikkialla

Lin, X., Sun, X., Ho, P. & Shen, X. (2007). GSIS: A secure and privacy-preserving protocol for vehicular communications. *IEEE Transactions on Vehicular Technology, 56*(6), 3442-3456.

Mejri, M. N., Ben-Othman, J. & Hamdi, M. (2014). Survey on VANET security challenges and possible cryptographic solutions. *Vehicular Communications, 1*(2), 53-66. doi:10.1016/j.vehcom.2014.05.001.

NordicWay Coop. (19.3.2017). Haettu osoitteesta: http://infotripla.fi/coop/

Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M. . . . Hubaux, J. P. (2008). Secure vehicular communication systems: Design and architecture. *IEEE Communications Magazine, 46*(11), 100-109. doi:10.1109/MCOM.2008.4689252.

Qian, Y., & Moayeri, N. (2008). Design of secure and application-oriented VANETs. Teoksessa *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE* (2794-2799). IEEE.

Raya, M., Papadimitratos, P. & Hubaux, J. (2006). Securing vehicular communications. *IEEE Wireless Communications, 13*(5), 8-15. doi:10.1109/WC-M.2006.250352.

Raya, M. & Hubaux, J. (2007). Securing vehicular ad hoc networks. *Journal of Computer Security, 15*(1), 39-68.

RoselinMary, S., Maheshwari, M., & Thamaraiselvan, M. (2013). Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA). Teoksessa *Information Communication and Embedded Systems (ICICES), 2013 International Conference on* (237-240). IEEE.

Samara, G., Al-Salihy, W. A., & Sures, R. (2010). Security analysis of vehicular ad hoc nerworks (VANET). Teoksessa *Network Applications Protocols and Services (NETAPPS), 2010 Second International Conference on* (55-60). IEEE.

Sichitiu, M. L. & Kihl, M. (2008). Inter-vehicle communication systems: A survey. *IEEE Communications Surveys & Tutorials, 10*(2), 88-105. doi:10.1109/COMST.2008.4564481.

Stampoulis, A. & Chai, Z. (2007). A survey of security in vehicular networks. *Project CPSC, 534*.

Sun, J., Zhang, C., Zhang, Y & Fang, Y. (2010). An identity-based security system for user privacy in vehicular ad hoc networks. *IEEE Transactions on Parallel and Distributed Systems, 21*(9), 1227-1239. doi:10.1109/TPDS.2010.14.

Suomen kyberturvallisuusstrategia (2013), Haettu 1.2.2017 osoitteesta: http://turvallisuuskomitea.fi/index.php/fi/component/k2/14-suomen-kyberturvallisuusstrategia.

Suomen virallinen tilasto (SVT): Tieliikenneonnettomuustilasto [verkkojulkaisu]. ISSN=1798-758X. Marraskuu 2016, Liitekuvio 1. Tieliikenteessä kuolleet onnettomuustyypin mukaan, tammi - marraskuussa 2016. Helsinki: Tilastokeskus [viitattu: 17.2.2017]. Saantitapa: http://www.stat.fi/til/ton/2016/11/ton_2016_11_2016-12-19_kuv_001_fi.html.

Toor, Y., Muhlethaler, P., Laouiti, A. & La Fortelle, A. D. (2008). Vehicle ad hoc networks: Applications and related technical issues. *IEEE Communications Surveys & Tutorials, 10*(3), 74-88. doi:10.1109/COMST.2008.4625806.

Uzcategui, R. A., De Sucre, A. J. & Acosta-Marum, G. (2009). Wave: A tutorial. *IEEE Communications Magazine, 47*(5), 126-133. doi:10.1109/MCOM.2009.4939288.

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97-102.

VSC, "Final Report". (2006). US DOT, Vehicle Safety Communications Project DOT HS 810 591.

VSC-A, "Final Report". (2009). US DOT, Vehicle Safety Communications Applications (VSC-A) Project DOT HS 810 073.

Whitman, M. E. & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

Wiedersheim, B., Ma, Z., Kargl, F., & Papadimitratos, P. (2010). Privacy in inter-vehicular networks: Why simple pseudonym change is not enough. Teoksessa *Wireless On-demand Network Systems and Services (WONS), 2010 Seventh International Conference on* (176-183). IEEE.

Willke, T. L., Tientrakool, P. & Maxemchuk. N. F. (2009). A survey of inter-vehicle communication protocols and their applications. *IEEE Communications Surveys & Tutorials, 11*(2), 3-20. doi:10.1109/SURV.2009.090202.

Xiao, B., Yu, B., & Gao, C. (2006). Detection and localization of sybil nodes in VANETs. Teoksessa *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks* (1-8). ACM.

Zeadally, S., Hunt, R., Chen, Y., Irwin, A. & Hassan, A. (2012). Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommunication Systems, 50*(4), 217-241.