



TAMPEREEN TEKNILLINEN YLIOPISTO  
TAMPERE UNIVERSITY OF TECHNOLOGY

**HARRI MYLLYSUO**

**ÄLYKKÄIDEN KULJETUSJÄRJESTELMIEN TIETOTURVAMEKA-  
NISMIT AUTONOMISTEN AJONEUVOJEN VERKKOYMPÄRIS-  
TÖSSÄ**

Diplomityö

Tarkastajat: professori Tarmo Lipping,  
yliopisto-opettaja Matti Monnonen

Tarkastajat ja aihe hyväksytty  
Talouden ja rakentamisen tiedekunnan  
koulutusvaradekaanin päätöksellä  
29. toukokuuta 2017

## TIIVISTELMÄ

**HARRI MYLLYSUO:** Älykkäiden kuljetusjärjestelmien tietoturvamekanismit autonomisten ajoneuvojen verkkoympäristössä

Tampereen teknillinen yliopisto

Diplomityö, 50 sivua, 2 liitesivua

Lokakuu 2017

Johtamisen ja tietotekniikan diplomi-insinöörin tutkinto-ohjelma

Pääaine: Verkkoympäristön hallinta ja tietoturva

Tarkastajat: professori Tarmo Lipping ja yliopisto-opettaja Matti Monnonen

Avainsanat: tietoturva, älyliikenne, autonominen, ajoneuvo, älykkäät kuljetusjärjestelmät, ITS-G5

Älykkäisiin kuljetusjärjestelmiin kuuluu tieliikenteen osalta sellaisia komponentteja, joilla parannetaan merkittävästi liikenneturvallisuutta. Eräs parannuksen mahdollistava tekijä on ajoneuvojen verkottuminen ja sitä kautta saatu tieto kaikkien ajoneuvojen olinpaikasta.

Verkottumisen mahdollistamiseksi on kehitetty oma viitearkkitehtuuri ajoneuvokäyttöön. Viitearkkitehtuurin myötä on mahdollista kytkeytyä myös osaksi maailmanlaajuista internetverkkoa. Tämän seurauksena nousevat esille tietoturvakysymykset, sillä verkkolaitteiden määrä kasvaa nopeasti.

Tämä diplomityö keskittyy tietoturvamekanismeihin, joita on kehitetty autonomisten ajoneuvojen verkkoympäristöä varten. Esille nostetaan myös muutamia epäkohtia ja puutteita. Tietoturvaan liittyen tarkastellaan muutamia tehtyjä testauksia ja tutkimuksia sekä tutustutaan ajoneuvojen väliseen kommunikaatioon simulointiympäristössä.

Älykkäiden kuljetusjärjestelmien tietoturvamekanismit autonomisten ajoneuvojen verkkoympäristössä on laaja kokonaisuus. Niihin liittyen tämä diplomityö keskittyy pääosin Euroopan alueella toimiviin ratkaisuihin. Aihealueen laajuudesta huolimatta tämä diplomityö onnistuu osoittamaan kehityskohteita esimerkiksi matkapuhelinverkkoihin perustuvan ajoneuvokommunikaation yksityisyysasioista. Älykkäiden kuljetusjärjestelmien tietoturvastandardeissa ei myöskään määritellä millään tasolla fyysistä tietoturvaa.

## ABSTRACT

**HARRI MYLLYSUO:** Information Security Mechanisms of Intelligent Transport Systems in Network Environment of Autonomous Vehicles

Tampere University of Technology

Master of Science Thesis, 50 pages, 2 Appendix pages

October 2017

Master's Degree Programme in Management and Information Technology

Major: Network Management and Information Security

Examiners: Professor Tarmo Lipping and University Teacher Matti Monnonen

Keywords: information security, intelligent transport systems, autonomous, vehicles, ITS, V2X, ITS-G5

Intelligent transport systems contain components that intend to improve road safety significantly. One factor to make this possible is the networking of vehicles and in consequence of that the cooperative awareness.

A specific reference and communication architecture has been developed to make networking of vehicles possible. This architecture also means that vehicles will be connected to the global internet. This will raise questions about information security because the amount of network devices is growing rapidly.

This thesis focuses on security mechanisms that have been developed for the network environment of autonomous vehicles. Some faults and flaws are shown. Some research and testing of vehicles' security is discussed. Also, vehicles' communication in simulation environment is explored.

Information security mechanisms of intelligent transport systems in network environment of autonomous vehicles is a large subject area. This thesis focuses on security mechanisms used in the European area. Despite the complexity and the extent of the subject area this thesis succeeds in showing targets for development e.g. in the privacy concerns of a cellular vehicle communication. Also, the intelligent transport systems' standards of information security do not define the physical security at all.

## ALKUSANAT

Tämä diplomityö on saanut alkunsa pitkän prosessin aikana. Sen alkujuuret vievät aina edelliseen koulutukseeni saakka Tampereen ammattikorkeakouluun vuosiin 2005–2009, joista viimeisenä valmistuin auto- ja työkonetekniikan insinööriksi. Koulutuksen jälkeinen työelämä vierähti niin autojen katsastuksessa kuin työkoneiden tuotesuunnittelussa. Lisäksi ainainen kiinnostus tietotekniikkaa kohtaan sekä jatkuvasti lisääntyvä tietotekniikan määrä työelämässä ja muuallakin ajoivat päätökseen hakeutua tietotekniikan diplomi-insinöörikoulutukseen. Jo silloisessa työelämässä oli havaittavissa, että tietotekniikka lisääntyy huimaa vauhtia myös autojen ja työkoneiden saralla. Tämä ajatus mielessä lähdin opiskelemaan DI-tutkintoa Tampereen teknilliseen yliopistoon.

Opiskelun ohella mietin sopivaa diplomityön aihetta. Pääajatuksena oli, että sen tulisi yhdistää jollakin tavalla tietotekniikka ja ajoneuvot. Viimeaikaiset keskustelut robottiautoista ja autonomisista autoista sekä työelämässä havaitut itsestään kulkevat työkoneet toivat kipinää diplomityön ajatteluun. Näiden pohjalta lähdin työstämään ajatusta, josko aihe voisi liittyä autonomisiin ajoneuvoihin.

Toinen viime aikoina paljon puhuttu aihe on tietoturva ja sen kasvava tarve, kun nettiyhdytystä lisätään niin jääkaappeihin, leivänpaahtimiin kuin koripalloihinkin. Näinpä on nettiyhteys saavuttanut myös autot. Lisäksi DI-koulutuksessani oli mahdollista sisällyttää tietoturvaan liittyviä kursseja aina pääaineeksi saakka. Näistä sain ajatuksen lisämausteeseen diplomityössäni, eli autonomisten ajoneuvojen verkkoympäristön tietoturvaan, jota ei ole liiaksi käsitelty varsinkaan suomen kielellä. Pisteenä i:n päälle oli silmiin osunut uutisointi Tampereella järjestettävästä robottiautojen testauksesta.

Tästä alkoi varsinainen diplomityön valmistelu tiedonhaulla ja kyselyillä niin VTT Oy:ltä kuin Tieto Oyj:ltä. Näiltä yrityksiltä sainkin merkittäviä taustatietoja ja apuja työni aineistoksi, joista iso kiitos heille. Iso kiitos kuuluu myös TTY:n Porin kampuksen niille henkilöille, jotka olivat työtäni ohjaamassa. Lisäksi kiitos työnantajalleni (Sampo Rosenlew Oy) mahdollisuudesta opintovapaaseen tämän projektin loppuunsaattamiseksi. Kiitokset myös ideoista, tuesta ja sparraamisesta Vaisto Solutions Oy:n Sami Dahlmanille. Kiitokset myös perheelleni. Lopuksi vielä haluan esittää isot erityiskiitokset tuesta ja ymmärryksestä vaimolleni hänen omalla äidinkielellään (japaniksi).

この論文を理解し、支えてくれたことに深く感謝します。

Porissa, 20.10.2017

Harri Myllysuu

# SISÄLLYSLUETTELO

1.	JOHDANTO .....	1
2.	ÄLYKKÄÄT KULJETUSJÄRJESTELMÄT .....	3
	2.1 Älykkäiden kuljetusjärjestelmien historiaa .....	3
	2.2 ITS-järjestelmien nykytila .....	4
	2.3 ITS-järjestelmien tulevaisuus .....	6
3.	STANDARDIT JA VIRANOMAISMAÄRITELMÄT .....	7
	3.1 Viranomaisten määritelmät .....	7
	3.2 Standardien taustaa .....	8
	3.3 ITS-aseman viitearkkitehtuuri .....	9
	3.3.1 Pääsykerros (Access) .....	10
	3.3.2 Tiedonsiirtokerros (Networking & Transport) .....	12
	3.3.3 Palvelukerros (Facilities) .....	13
	3.3.4 Sovelluskerros (Applications) .....	13
	3.3.5 Hallintakerros (Management) .....	15
	3.3.6 Tietoturvakeros (Security) .....	16
	3.4 Kommunikointi ITS-ympäristössä .....	17
4.	AUTONOMISTEN AJONEUVOJEN VERKKOYMPÄRISTÖ .....	19
	4.1 Vehicle-to-Everything (V2X) -kommunikointi .....	19
	4.2 Cellular V2X (C-V2X) -kommunikointi .....	20
	4.3 Tampere UrbanAutoTest .....	21
5.	ITS-YMPÄRISTÖN TIETOTURVAMEKANISMIT .....	23
	5.1 Tietoturva-arkkitehtuuri .....	23
	5.2 Tietoturvan hallinta .....	26
	5.2.1 Luottamuksen ja yksityisyyden hallinta .....	26
	5.2.2 Pääsynvalvonta .....	27
	5.2.3 Identiteetin hallinta .....	27
	5.2.4 Luottamuksellisuus .....	28
	5.3 Tietoturvapalvelut .....	28
	5.3.1 ITS-aseman tietoturvapalvelut .....	29
	5.3.2 Tietoturvan hallinnan tietoturvapalvelut .....	29
	5.4 Uhka-, haavoittuvuus- ja riskianalyysi .....	31
	5.5 Yhteiset toimintamallit .....	33
	5.6 C-V2X-kommunikaation tietoturva .....	34
	5.7 Yhteenveto tietoturvamekanismeista .....	35
6.	V2X-KOMMUNIKAATION JA -TIETOTURVAN TESTAUS .....	36
	6.1 Yleistä testauksesta .....	36
	6.2 V2X-kommunikaation simulointiympäristö .....	37
	6.2.1 VeINS-simulointiympäristön sovellukset .....	37
	6.2.2 VeINS-simulointiympäristön asennus .....	38
	6.2.3 V2X-kommunikaation simulointi .....	39

6.3 Tietoturvan testauksista.....	42
7. YHTEENVETO .....	44
LÄHTEET.....	47

LIITE A: VERKKOKOMPONENTIT NED-KIELELLÄ

LIITE B: KOMMUNIKOINNIN LÄHDEKODI C++-KIELELLÄ

## KUVALUETTELO

<i>Kuva 1.</i>	<i>Liikenteen automaation eri tasot [10].</i>	<i>5</i>
<i>Kuva 2.</i>	<i>OSI- ja TCP/IP-viitemallit.</i>	<i>9</i>
<i>Kuva 3.</i>	<i>ITS-järjestelmään kytketyn laitteen viitearkkitehtuuri.</i>	<i>10</i>
<i>Kuva 4.</i>	<i>Pääsykerroksen yleiskuvaus.</i>	<i>11</i>
<i>Kuva 5.</i>	<i>Tiedonsiirtokerroksen yleiskuvaus.</i>	<i>12</i>
<i>Kuva 6.</i>	<i>Palvelukerroksen yleiskuvaus.</i>	<i>13</i>
<i>Kuva 7.</i>	<i>Sovelluserroksen yleiskuvaus.</i>	<i>14</i>
<i>Kuva 8.</i>	<i>Hallintakerroksen yleiskuvaus.</i>	<i>15</i>
<i>Kuva 9.</i>	<i>Tietoturveysikön yleiskuvaus.</i>	<i>16</i>
<i>Kuva 10.</i>	<i>ITS-kommunikoinnin havaintoesimerkki [22].</i>	<i>17</i>
<i>Kuva 11.</i>	<i>ITS-alijärjestelmät [22].</i>	<i>18</i>
<i>Kuva 12.</i>	<i>V2X-ympäristön havaintoesimerkki [11].</i>	<i>19</i>
<i>Kuva 13.</i>	<i>Tampereen testausympäristön rataprofiili [13].</i>	<i>22</i>
<i>Kuva 14.</i>	<i>Periaatekuva ITS-tietoturva-arkkitehtuurista.</i>	<i>24</i>
<i>Kuva 15.</i>	<i>ITS-tietoturvan viitemalli [28].</i>	<i>25</i>
<i>Kuva 16.</i>	<i>ITS-kommunikaation tietoturvapalvelut kerroksittain.</i>	<i>31</i>
<i>Kuva 17.</i>	<i>Esimerkki peruskommunikaation graafisesta verkkoympäristöstä.</i>	<i>39</i>
<i>Kuva 18.</i>	<i>Peruskommunikoinnin esimerkkisimulaatio.</i>	<i>40</i>
<i>Kuva 19.</i>	<i>Peruskommunikoinnin simulaation tapahtumat graafisessa muodossa.</i>	<i>41</i>
<i>Kuva 20.</i>	<i>VeINS-projektin mukainen simulointiympäristö.</i>	<i>41</i>

## LYHENTEET JA MERKINNÄT

BSA	engl. Basic Set of Applications, perussovellusten ryhmä, jota käytetään ajoneuvojen verkkoympäristössä
CAM	engl. Cooperative Awareness Message, sanoma, jolla ilmoitetaan kaikkien yhdistettyjen laitteiden olinpaikkatiedot
DENM	engl. Decentralized Environmental Notification Message, sanoma, jolla ilmoitetaan ympäristön tapahtumista
ETSI	engl. European Telecommunications Standards Institute, Euroopan tietoliikenteen standardisointi-instituutti
IEEE	engl. Institute of Electrical and Electronics Engineers, kansainvälinen järjestö, joka tuottaa mm. standardeja
IP	engl. Internet Protocol, verkkokerroksen protokolla, jolla hoidetaan tietoliikennepakettien reititys
ITS	engl. Intelligent Transport Systems, älykkäät kuljetusjärjestelmät, älyliikenne
LLC	engl. Logical Link Control, loogisen siirtoyhteyden ohjauksen alikerros
LTE	engl. Long Term Evolution for UMTS, neljännen sukupolven (4G) matkapuhelinteknologia
MAC	engl. Medium Access Control, tiedonsiirtokanavan saantimenettelyn alikerros
OSI	engl. Open Systems Interconnection, tietoliikenteen protokollakerrosten viitemalli
PKI	engl. Public Key Infrastructure, salausavainten vaihtoon käytettävä julkisen avaimen järjestelmä
SAE	engl. Society of Automotive Engineers, yhdysvaltalainen autoalan standardisointijärjestö
TCP	engl. Transmission Control Protocol, tietokoneiden välille yhteyksien luomiseen käytettävä protokolla, jonka avulla lähetys onnistuu luotettavasti
TTY	Tampereen teknillinen yliopisto
UDP	engl. User Datagram Protocol, yhteydetön protokolla, jonka avulla tiedostojen siirto onnistuu
UMTS	engl. Universal Mobile Telecommunications Systems, kolmannen sukupolven (3G) matkapuhelinteknologia
URL	engl. Uniform Resource Locator, verkkosivun osoite
V2X	engl. Vehicle-to-Everything, verkotetut ajoneuvot, jotka ovat yhteydessä kaiken ulkopuolisen kanssa
WAVE	engl. Wireless Access in Vehicular Environment, langaton kommunikointitekniikka ajoneuvoympäristössä
WLAN	engl. Wireless Local Area Network, langaton lähiverkkotekniikka

# 1. JOHDANTO

Älykkäät kuljetusjärjestelmät eli älyliikenne on nykyään iso aihealue, kun puhutaan esimerkiksi teollisesta internetistä. Nämä järjestelmät kokonaisuutena sisältävät niin tie-, raide-, laiva- kuin lentoliikenteenkin kehitysmalleja, mutta tässä diplomityössä keskitytään tieliikenteen osa-alueeseen. Sen järjestelmät sisältävät monia teknologisia kehitysmalleja, joilla parannetaan liikenneturvallisuutta merkittävästi. Tämän seurauksena kehitysaskeleet ovat tulleet siihen pisteeseen, että autoista ja ajoneuvoista on kehitetty ja kehitetään automaattisia ja autonomisia. Automaattinen auto kykenee tekemään esimerkiksi hätäjarrituksen itsenäisesti, kun taas autonominen auto kykenee itsenäiseen päätöksentekoon ennestään tuntemattomassa ympäristössä, toisin sanoen ilman kuljettajaa.

Ajoneuvoja varten on kehitetty verkkoympäristö, jotta ne voivat kommunikoida keskenään sekä kaikkien muiden asemien kanssa. Tämä ominaisuus tarvitaan, sillä kuljettaja ei aina ole tekemässä päätöksiä ajamisen suhteen. Se tarvitaan myös siksi, jotta kaikkien ajoneuvojen ja muiden asemien tarkat olinpaikat tiedetään. Tämän tiedon avulla voidaan esimerkiksi estää liikenneonnettomuuksia ja ajoneuvojen yhteentörmäyksiä sekä saadaan liikenne tehokkaammaksi. Verkotettujen ajoneuvojen ympäristö tarkoittaa myös sitä, että kaikki ajoneuvot ovat tavalla tai toisella kytkeytyneet maailmanlaajuiseen internetverkkoon.

Jotta ajoneuvot voisivat toimia ja kommunikoida verkkoympäristössä, tarvitaan niille oma viite- ja kommunikointiarkkitehtuuri, jota käytetään kaikissa tähän verkkoon kytkeytyissä laitteissa. Kyseistä arkkitehtuuria tarkastellaan tässä diplomityössä painottuen Euroopan alueella käytettävään malliin. Arkkitehtuuri takaa sen, että kaikki ajoneuvoverkon laitteet on mahdollista kytkeä verkkoon ja siten ne kytkeytyvät osaksi globaalia internetverkkoa. Tämän seurauksena nousevat esille tietoturvakysymykset, sillä verkkoon kytkeytyneiden laitteiden määrä kasvaa jatkuvasti. Siksi viitearkkitehtuuriin on sisällytetty oma osa tietoturva-asioita varten.

Verkotettujen ajoneuvojen tietoturva-asioiden tarkastelu tässä vaiheessa on tärkeää siksi, että niihin liittyen – ja yleensäkin – tietoturvanmääritelmät kehitetään jälkijunassa. Tässä diplomityössä tarkastellaan kaikkia niitä tietoturvan määritelmiä, joita on jo kehitetty ja julkaistu ajoneuvoympäristöön liittyen. Niihin kuuluu niin viranomaisten tekemiä määritelmiä kuin eri organisaatioiden tekemiä standardeja. Standardeissa määritellään muiden muassa tietoturvan hallinta, tietoturvapalvelut sekä uhka-, haavoittuvuus- ja riskianalyysi.

Tässä diplomityössä tutustutaan ajoneuvojen väliseen kommunikointiin. Se perustuu joko langattomaan lähiverkkotekniikkaan tai uudempaan matkapuhelinverkkoja hyödyntävään

verkkoteknologiaan. Tampereelle on rakennettu näitä molempia verkkoteknologioita hyödyntävä testausympäristö, johon myös tutustutaan.

Ajoneuvojen väliseen kommunikointiin tutustutaan myös simulointiympäristön kautta, jossa on mahdollista toteuttaa haluamansa tai tarvitsemansa kaltainen kommunikointiympäristö. Sen lisäksi esitetään pohdintoja erilaisista simulointiympäristöistä. Näitä tarkastellaan siksi, että ajoneuvokommunikaation tietoturva on usein testattu erityisesti simulointiympäristöissä. Tällaisia testauksia käsitellään muutamia. Niistä huomataan, että erilaisia ominaisuuksia ja asetuksia on jätetty huomioimatta eri testeissä, jolloin niiden tulokset eivät ole vertailukelpoisia keskenään.

Tämän diplomityön tutkimuksissa huomataan, että simulointiympäristöissä ei ole otettu huomioon tietoturvan testaukseen liittyviä moduuleita. Niitä on itse mahdollista ohjelmoida avoimeen lähdekoodiin perustuvassa simulointiympäristössä, mutta ohjelmointi on rajattu tämän diplomityön aihealueen ulkopuolelle.

Lisäksi tätä työtä varten tehdyissä tutkimuksissa huomataan, että ajoneuvojen oikeassa kommunikointiympäristössä ei ole suoritettu tietoturvaan liittyviä tutkimuksia ja testauksia. Testauksia ei myöskään ollut mahdollista päästä suorittamaan itse.

Tämän diplomityön rakenne on seuraava. Toisessa luvussa tutustutaan lähemmin älykkäisiin kuljetusjärjestelmiin sekä niiden historian ja nykytilan kautta tulevaisuudennäkymiin. Kolmas luku käsittelee niin viranomaisten määritelmiä kuin myös useiden eri standardointijärjestöjen määrittelemiä standardeja, joihin älykkäät kuljetusjärjestelmät pitkälti pohjautuvat. Neljännessä luvussa tarkastellaan autonomisten ajoneuvojen verkkoympäristöä, joka kuuluu pienempänä osana älykkäisiin kuljetusjärjestelmiin, sekä sitä varten rakennettua UrbanAutoTest-testausympäristöä Tampereella. Viides luku keskittyy kokonaan tietoturvamekanismeihin, joita käytetään älykkäissä kuljetusjärjestelmissä. Sen jälkeen kuudennessa luvussa tarkastellaan ajoneuvojen välistä kommunikaatiota sekä sen tietoturvan testauksia. Lopulta seitsemännessä luvussa on yhteenveto koko työstä.

## 2. ÄLYKKÄÄT KULJETUSJÄRJESTELMÄT

*Intelligent Transport Systems* (ITS) eli älykkäät kuljetusjärjestelmät, jota voidaan suomeksi kutsua myös termeillä älyliikenne tai liikennetelematiikka, on määritelty esimerkiksi Euroopan unionin direktiivissä 2010/40/EU [18]. Sen mukaan ITS-järjestelmissä tieto- ja viestintäteknikat yhdistyvät liikenteen ja kuljetuksen osa-alueisiin. Tähän kokonaisuuteen kuuluvat niin infrastruktuuri, ajoneuvot, käyttäjät, liikenteen ohjaus kuin myös liikkuvuus ja sen hallinta. Kokonaisuuteen kuuluvat myös yhtymäkohdat muihin kuljetusten muotoihin, kuten esimerkiksi raide-, laiva- ja lentoliikenteeseen. Käytännössä erilaisia ITS-järjestelmiä voidaan jo nykyään havaita esimerkiksi monissa autoissa, kun niihin on ajan myötä hiipinyt turvallista ajoa edistäviä järjestelmiä. Samoja järjestelmiä käytetään edelleen hyväksi moderneissakin ITS-järjestelmissä. Seuraavissa luvuissa kuvataan eräitä ITS-järjestelmien kehitysaskelia liittyen tieliikenteeseen.

### 2.1 Älykkäiden kuljetusjärjestelmien historiaa

New Yorkin maailmannäyttelyssä vuonna 1939, johon Suomikin osallistui Alvar ja Aino Aallon suunnitteleman osaston myötä, oli esillä Futurama-näyttely [8]. Siinä esiteltiin, miltä maailma mahtaisi näyttää 1960-luvulla kaikkine automaattisine katuvalaistuksineen, monikaistaisine valtateineen ja automatisoituine autoineen. Tällaisia esityksiä ja niiden suunnitelmia voidaan kutsua ITS-järjestelmien ensimmäisiksi kehitysaskeliksi.

ITS-järjestelmien kehitysaskleet voidaan Tokuyaman kirjoittaman artikkelin [15] mukaan karkeasti jakaa kolmeen eri vaiheeseen. Artikkelin mukaan ensimmäisessä vaiheessa on aloitettu ITS-järjestelmien tutkimukset 1960- ja 1970-luvuilla. Nämä aikaisen vaiheen tutkimukset ovat aloittaneet *Comprehensive Automobile Control System* (CACS) -projekti [9] Japanissa, *the Electronic Route Guidance System* (ERGS) -projekti Yhdysvalloissa sekä vastaavanlainen projekti Saksassa. ERGS-projektin yhteydessä 1960-luvulla Yhdysvaltojen itäosiin asennettiin muutamille risteysalueille tienvarsiyksiköitä, joihin autot olivat radioviestintäyhteydessä [8]. Tokuyaman mukaan kaikilla näillä projekteilla oli yhteinen painotus reittiopastuksessa sekä ne perustuivat keskusprosessointijärjestelmiin, joissa olivat valtavat keskustietokoneet ja tietoliikennejärjestelmät. Kuitenkaan näiden projektien tuloksena ei saatu aikaiseksi käytännön sovelluksia.

Toinen vaihe ajoittuu Tokuyaman mukaan aikajaksolle 1980–1995, jolloin teknologiset parannukset, kuten esimerkiksi massamuistit, auttoivat kehittämään ITS-järjestelmiä. Alkoi myös tulla enemmän uusia tutkimus- ja kehitystyön tuloksia, joita pystyttiin hyödyntämään järkevästi ITS-järjestelmien kehityksessä. Tokuyama mainitsee, että toisen vaiheen aikana alkoi jälleen uusia projekteja. Japanissa alkoi vuonna 1984 *Road/Automobile*

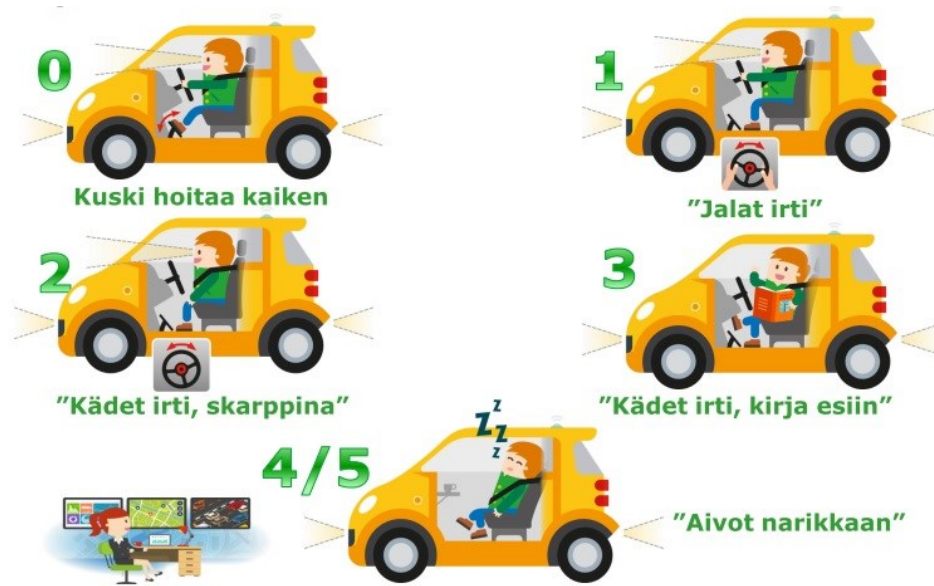
*Communication System (RACS)* -projekti, joka muodosti pohjan nykyisille autojen navigointijärjestelmille. Euroopassa oli meneillään kaksi projektia samaan aikaan: *the Program for a European Traffic System with Higher Efficiency and Unprecedented Safety (PROMETHEUS)* -projekti oli pääosin autovalmistajien perustama, kun *the Dedicated Road Infrastructure for Vehicle Safety in Europe (DRIVE)* -projekti oli Euroopan Yhteisön aloittama. Myös Yhdysvalloissa *U.S. Intelligent Vehicle-Highway Systems (IVHS)* -projekti oli edistymässä.

Tokuyaman mukaan ITS-järjestelmien kehityksen kolmas vaihe sisältää erilaisia suuntauksia. Niissä aiempien projektien tuloksia alettiin nähdä käytännön sovelluksina. Alettiin ymmärtää koko ITS-järjestelmien potentiaali, ja mitä niillä voitaisiin saavuttaa. ITS-järjestelmät alkoivat tulla tunnetuksi ja sen myötä ne saivat paikkansa tietotekniikan maailmassa ja hierarkiassa. Tutkimustöiden jatkuessa ja teknologioiden edelleen kehittyessä alettiin nähdä sovelluksia, joita on käytössä vielä nykyäänkin.

## 2.2 ITS-järjestelmien nykytila

Tällä hetkellä useisiin ajoneuvoihin on saatavissa lukuisia erilaisia turvallista ajoa tukevia lisävarusteita kuten esimerkiksi mukautuva vakionopeussäädin, automaattinen hätäjarrutusjärjestelmä, kaistavahti, kuljettajan vireystilaa valvova järjestelmä ja niin edelleen. Samaan aikaan testataan ilman kuljettajaa toimivia autoja, joiden kehityksen edelläkävijöitä ovat olleet esimerkiksi Bosch, Google ja Tesla. Bosch on käynyt joitain yhteistyöneuvotteluja Japanin hallituksen kanssa, jotta autonomiset autot olisivat käytössä Tokion olympialaisissa vuonna 2020 [17]. Bosch on myös maailman suurimpana autonomien valmistajana monien eri automerkkien kanssa kehittämässä itseajavia autoja, kuten Daimlerin kanssa yhteistyönä toteutettu uusi Mercedes-Benz E -sarja. Google on kehittänyt itseajavan auton, jonka konsepti tunnetaan nykyään nimellä Waymo, ja tehnyt sillä testejä muun liikenteen seassa jo vuodesta 2009 alkaen [40]. Tesla puolestaan on esitellyt Model S -mallissaan autopilot-toiminnon, jonka päällekytkemisen jälkeen auto pystyy osittain ajamaan ilman kuljettajaa [43]. Audi esitteli Frankfurtin autonäyttelyssä 11.9.2017 oman Audi Aicon -konseptiautonsa. Siinä ei ole lainkaan ohjauspyörää eikä polkimia.

Älykkäiden kuljetusjärjestelmien ja älyliikenteen yhteydessä puhutaan nykyään usein automaattisista ja autonomisista ajoneuvoista. Näillä termeillä on selkeä merkitysero [6]. Automaattiajoneuvo tarkoittaa sellaista ajoneuvoa, joka kykenee selviytymään liikenteessä osittain ilman kuljettajan toimenpiteitä, kuten esimerkiksi hätäjarrutuksen tekeminen automaattisesti. Autonominen ajoneuvo puolestaan tarkoittaa sellaista ajoneuvoa, joka kykenee itsenäiseen päätöksentekoon ilman kuljettajaa ennalta määrittelemättömässä ympäristössä omien järjestelmiensä avulla ja ilman toimivaa yhteyttä toisiin ajoneuvoihin tai infrastruktuuriin. Yhdysvaltalainen autoalan standardointijärjestö *Society of Automotive Engineers (SAE) International* on määritellyt eri automaatiotasot kuvaamaan ajoneuvojen automaatiota [14]. Suomessa Liikenteen turvallisuusvirasto Trafi on tehnyt



**Kuva 1.** Liikenteen automaation eri tasot [10].

samasta asiasta selkokielisen kuvauksen (Kuva 1) [10]. Käytännössä siis autonominen auto on automaatiotasolla 5.

Nykyään ITS-järjestelmiin liittyen kehitetään runsaasti erilaisia sovelluksia. Pääosin ne voidaan jakaa automaation tarpeisiin sekä ajoneuvojen verkotuksen tarpeisiin [8]. Automaatiosovelluksilla kehitetään ajoneuvojen kykyä toimia erilaisissa tilanteissa itsenäisesti, kuten esimerkiksi jo edellä mainittu hätäjarrutus tai parkkiruutuun pysäköinti ilman kuljettajan toimenpiteitä. Näiden sovellusten toiminta perustuu pääosin erilaisiin antureihin ja kameroihin, joita ajoneuvoihin on asennettu. Esimerkiksi kaistavahdin toiminta perustuu kameraan, joka seuraa tien reunaviivaa.

Verkotetut ajoneuvot käyttävät langatonta verkkoyhteyttä, jonka avulla ne voivat olla yhteydessä toisiinsa (*Vehicle-to-Vehicle*, V2V) sekä tukiasemiin, jotka on kiinteästi asennettu tienvarsiyksiköihin (*Vehicle-to-Infrastructure*, V2I). Näihin yhteyksiin liittyen käytetään ja kehitetään sovelluksia, joiden avulla saadaan reaaliaikaista tietoa jokaisen ajoneuvon ja tienkäyttäjän olinpaikasta, kulkusuunnasta, kulkunopeudesta ja niin edelleen. Kaikilla näillä toimenpiteillä on tarkoituksena parantaa liikenneturvallisuutta merkittävästi tulevaisuuden tarpeita varten [8].

Jo nykyään voidaan havaita, että verkotettujen ajoneuvojen kehityksen yhteydessä on tietoturva jäänyt hieman taka-alalle. Tämä voidaan havaita siitä, että tietoturvasta on alettu puhua vasta reilusti myöhemmin. Kuitenkin se on erittäin tärkeä osa-alue, sillä ajoneuvojen verkotuksen myötä laitteiden määrä verkossa moninkertaistuu, jolloin on isompi pinta toteuttaa jokin hyökkäys. Toisaalta myös yksityisyysasiat pitää muistaa, sillä henkilökohtaisia tietoja ei saa saada selville ajoneuvon tietoja tutkimalla.

## 2.3 ITS-järjestelmien tulevaisuus

Jotta voidaan puhua tulevaisuudesta, täytyy ottaa huomioon muutama fakta menneisyydestä. Yhdistyneiden kansakuntien (YK) mukaan koko maailman väestöstä 10 prosenttia on asunut kaupunkialueilla noin vuosisata sitten ja 30 prosenttia 1950-luvulla [48]. Maailman sivilisaatio on saavuttanut eräänlaisen maamerkin vuonna 2008, kun väestöstä puolet on asunut kaupunkialueilla. Ennuste on, että kaupunkialueilla asuu noin 66 prosenttia koko maailman väestöstä vuonna 2050. Kun otetaan huomioon vielä YK:n ennuste, jonka mukaan maailman väestö on 9,7 miljardia vuonna 2050, saadaan kaupunkialueille runsaasti asukkaita. Tästä seuraa myös se, että liikennejärjestelmiä on kehitettävä koko ajan tulevaisuutta ajatellen.

Tällä hetkellä tulevaisuuden liikennejärjestelmien kehitykseen vastataan infrastruktuurien rakentamisella sekä eri standardeihin, säädös- ja lakikysymyksiin keskittymällä [6]. Tärkeässä osassa ovat myös innovointi- ja kokeilutoiminta, joiden ansiosta on lisätty poikkitieteellistä kanssakäymistä. Näillä toimenpiteillä pystytään kehittämään älyliikenteen kokonaisuutta.

Älyliikenteestä voi varmasti tehdä tulevaisuuden visioita niin paljon kuin vain mielikuvitus antaa periksi. Jotkut realistisimmista visioista ovat kuitenkin sellaisia, joita on jo jollain tasolla testattu tai ollaan testaamassa. Onnistuneiden testien jälkeen järjestelmiin voidaan aina lisätä joitain uusia ominaisuuksia. Tällaisia visioita tulevaisuuden älyliikenteestä on esimerkiksi raskaan kaluston automaattinen jonoajo (*platooning*), jossa useampi kuorma-auto voi ajaa jonossa vain noin metrin päässä toisistaan. Ensimmäisessä autossa on koko ohjelmistopaketti autonomiseen ajamiseen ja perässä olevat autot vain seuraavat ensimmäistä. Tulevaisuudessa käsitys auton omistamisesta muuttuu, sillä käyttöön tulee jaettuja autoja. Kun tulee tarve matkustaa autolla jonnekin, se tilataan älypuhelimien sovelluksella ja auto on käytettävissä matkan ajan. Tällöin autosta siis puhutaan palveluna, ei omistamisena. Tulevaisuudessa voitaneen puhua myös kokonaisista älykaupungeista, joissa samaan järjestelmään yhdistyvät niin liikenne, terveydenhuolto, julkiset palvelut kuin myös energian jakelu.

Jotta älyliikenne voisi toimia moitteettomasti, pitäisi kaikkien ajoneuvojen olla autonomisia, sillä ohjelmallisen älyn ja ihmisälyn toimintatavat voivat poiketa toisistaan merkittävästi tietyissä tilanteissa. Täysautonomisuuteen luonnollisesti kuluu vielä paljon aikaa, koska osa ihmisistä haluaa ajaa itse autoaan. Useat autovalmistajat ovat ennustaneet, että automaattiautot tulevat tuotantoon ja liikenteeseen ainakin osittain vuoteen 2025 mennessä. Joidenkin arvioiden mukaan täysin autonomiset autot ovat käytössä kaikkialla vuonna 2070.

## 3. STANDARDIT JA VIRANOMAISMÄÄRITELMÄT

Koko älykkäiden kuljetusjärjestelmien kenttä pohjautuu erittäin vahvasti viranomaistahojen tekemiin määritelmiin sekä useiden eri organisaatioiden kehittämiin standardeihin, kuten usein teknologian alalla on. Tässä luvussa käydään läpi määritelmiä ja standardeja, joiden pohjalta määräytyy ITS-järjestelmiin kytkettyjen laitteiden viitearkkitehtuuri, tiedonsiirto, tietoturva sekä käytettävissä olevat palvelut ja toiminnot. Aluksi kuvataan yleisesti eri viranomaistahojen tekemiä määritelmiä sekä tärkeimpiä standardeja liittyen ITS-järjestelmiin.

### 3.1 Viranomaisten määritelmät

Euroopan Unionin direktiivi [18], jossa älykkäät liikennejärjestelmät määritellään, on Euroopan komission ehdotuksen perusteella asetettu. Euroopan komission mukaan ITS-järjestelmät kasvattavat liikenneturvallisuutta, liikenteen tehokkuutta ja joustavuutta sekä käyvät Euroopan kasvavien pakokaasupäästöjen ja ruuhkien kimppuun [5]. Tämä onnistuu hyödyntämällä erilaisia tieto- ja viestintäteknikoita kaikissa kuljetusten muodoissa. Euroopan komissio työskentelee teollisuuden, viranomaisten ja muiden eri tahojen kanssa löytääkseen yhteisiä ratkaisuja ITS-järjestelmien kehittämiseen. Komission mukaan liikenteen digitalisaatio ottaa isoja harppauksia eteenpäin tulevina vuosina, joten sen tarkoitus on tukea ITS-järjestelmien kehittämistä ja myös ITS-järjestelmien seuraavan sukupolven kehittämistä. Seuraavasta sukupolvesta käytetään nimitystä C-ITS (*Cooperative ITS*), joka tähtää liikenteen automaatioon.

C-ITS-järjestelmät sallivat tehokkaan tiedonvaihdon langattomien verkkojen välityksellä, jotta ajoneuvot voivat olla yhteydessä toisiinsa, tieinfrastruktuuriin sekä muihin tienkäyttäjiin. Jo nykyäänkin ajoneuvot ovat verkottuneita, ainakin osittain, mutta lähitulevaisuudessa ne kykenevät olemaan suoraan vuorovaikutuksessa toistensa ja tieinfrastruktuurin kanssa [4]. Tämä vuorovaikutuksessa oleminen toimii perustana C-ITS-järjestelmille, joiden ansiosta voidaan odottaa merkittävää parannusta niin liikenneturvallisuuteen, liikenteen tehokkuuteen kuin ajomukavuuteenkin. Tätä kehitystyötä varten Euroopan komissio on 30.11.2016 ottanut käyttöön eurooppalaisen strategian C-ITS-järjestelmille. Sen tehtävänä on helpottaa C-ITS-järjestelmien investointeja ja kehitystyötä Euroopan Unionin alueella, jotta voidaan saada aikaiseksi runsaasti C-ITS-palveluita vuoteen 2019 mennessä ja sen jälkeen.

Ajoneuvojen verkottumisen myötä kaikki ajoneuvot tulevat tavalla tai toisella olemaan osana globaalia internetverkkoa, joka puolestaan nostaa tietoturvakysymykset ajankoh-

taisiksi. Tämän seurauksena C-ITS-strategia on tällä hetkellä saavuttanut toisen vaiheensa, jossa tietoturvaan liittyvä varmennepolitiikka (*Certificate Policy*) [3] on hyväksytty 14.6.2017. Sen avulla ohjataan yleistä tietoturvaa sekä varmennepolitiikkaa.

Suomessa Liikenne- ja viestintäministeriö on julkaissut Liikenteen automaation ja robotiikan kehittämistoimenpiteiden tiekartan 2017-2019 [6], jonka mukaan Suomen tavoitteena on olla liikenteen automaatiokehityksen kärjessä. Tämä toteutetaan varmistamalla automaatiokehitykselle paras mahdollinen säädös- ja toimintaympäristö sekä kehittämällä tarvittavia toimenpiteitä, kuten esimerkiksi kokeilujen toteuttaminen ja tukeminen, 5G-verkkoteknologian käyttöönotto sekä satelliittipaikannuksen laadunparannus.

### 3.2 Standardien taustaa

Kansainvälinen tekniikan alan järjestö *Institute of Electrical and Electronics Engineers* (IEEE) määrittelee monien eri alojen keskeisiä standardeja. Se on määritellyt muiden muassa langattomille lähiverkoille IEEE 802.11 -standardin. Standardiin on tehty vuonna 2010 laajennus IEEE 802.11p, jolla siihen on lisätty langaton järjestelmä ajoneuvoympäristön kommunikaatiota varten, *Wireless Access in Vehicular Environments* (WAVE) [38]. Laajennukseen on lisätty myös määritelmä IEEE 802.11 -yhteensopivien laitteiden keskinäisestä kommunikaatiosta ilman verkon tukiaseman tukea. Tätä kutsutaan *Ad-Hoc*-verkoksi. Saman laajennuksen pohjalta on kehitetty kokonainen IEEE 1609 -standardiperhe, joka on määritelty erityisesti ajoneuvojen välistä langatonta WAVE-ympäristöä varten [39].

Eurooppalainen voittoa tavoittelematon telealan standardisointijärjestö *European Telecommunications Standards Institute* (ETSI) on IEEE 802.11p -standardin pohjalta kehittänyt ITS-G5-standardit [23]. Ne on määritelty nimenomaisesti Euroopan alueella käytettäviksi ja ne pohjautuvat jo olemassa oleviin standardeihin, lähinnä IEEE 802.11 sekä ANSI/IEEE 802.2 -standardeihin [21]. Näistä jälkimmäinen määrittelee loogisen siirtoyhteyden ohjauksen alikerroksen LLC (*Logical Link Control*). ANSI-lyhenne tulee sanoista *American National Standards Institute*, joka on Yhdysvaltalainen standardeja valvova ja kehittävä voittoa tavoittelematon instituutti. Tässä diplomityössä keskitytään ensisijaisesti ETSI-järjestön määrittelemiin eurooppalaisiin ITS-G5-standardeihin<sup>1</sup>.

ETSI EN 302 663 -standardin [21] mukaan ITS-G5-standardien määrittelemät teknologiat tukevat tiedonsiirtoa liikkuvien asemien välillä käyttäen *Ad-Hoc*-yhteystapaa. Määritellyt teknologiat toimivat taajuuskaistalla 5,9 GHz, joka on jaettu eri taajuusalueisiin käyttötarkoituksen mukaan:

- ITS-G5A: turvallisuuteen liittyvien teknologioiden taajuusalue 5,875–5,905 GHz,

---

<sup>1</sup> ITS-järjestelmien standardeja kehitetään muutamien standardisointiorganisaatioiden yhteistyönä. Näitä ovat yllä mainittujen lisäksi mm. ISO (*International Organization for Standardization*) ja CEN (*Commission Européen de Normalisation*), joiden ITS-standardeja ovat esim. ISO TC 204 ja CEN TC 278.

- ITS-G5B: muiden kuin turvallisuuteen liittyvien teknologioiden taajuusalue 5,855–5,875 GHz,
- ITS-G5C: verkkoliikenteelle varattu taajuusalue 5,470–5,725 GHz,
- ITS-G5D: tulevaisuuden teknologioille varattu taajuusalue 5,905–5,925 GHz.

Näillä taajuusalueilla toimivien ITS-asemien yleiseen viitearkkitehtuuriin tutustutaan seuraavassa luvussa.

### 3.3 ITS-aseman viitearkkitehtuuri

Usein tietoliikenteen materiaaleissa käytetään eri tiedonsiirtoprotokollien yhdistelmän kuvaamiseen OSI (*Open Systems Interconnection*) -viitemallia, jossa yhdistelmä kuvataan seitsemässä kerroksessa:

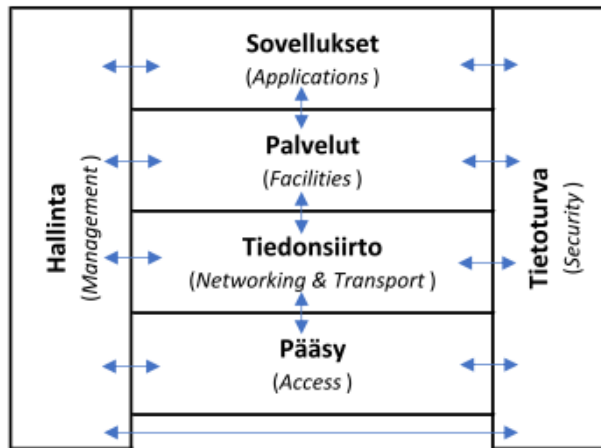
1. Fyysinen kerros (*Physical Layer*).
2. Siirtoyhteyserros (*Data Link Layer*).
3. Verkkokerros (*Network Layer*).
4. Kuljetuserros (*Transport Layer*).
5. Istunterros (*Session Layer*).
6. Esitystapakerros (*Presentation Layer*).
7. Sovelluserros (*Application Layer*).

Siirtoyhteyserros (DLL) on jaettu kahteen alikerrokseen: tiedonsiirtokanavan saantime-  
nettelyn alikerros MAC (*Medium Access Control*) ja loogisen siirtoyhteyden ohjauksen  
alikerros LLC. Toinen, nykyään ehkäpä enemmän käytössä oleva kuvaus on TCP/IP  
(*Transmission Control Protocol / Internet Protocol*) -viitemalli, jossa erona edelliseen on  
se, että kerrokset 1 ja 2 on yhdistetty peruserrokseksi sekä kerrokset 5–7 on yhdistetty  
sovelluserrokseksi. Kuva 2 havainnollistaa OSI- ja TCP/IP-viitemallit.

OSI	TCP/IP
Sovelluserros ( <i>Application Layer</i> )	Sovelluserros ( <i>Application Layer</i> )
Esitystapakerros ( <i>Presentation Layer</i> )	
Istunterros ( <i>Session Layer</i> )	
Kuljetuserros ( <i>Transport Layer</i> )	Kuljetuserros ( <i>Transport Layer</i> )
Verkkokerros ( <i>Network Layer</i> )	Verkkokerros ( <i>Internet Layer</i> )
Siirtoyhteyserros ( <i>Data Link Layer</i> )	Peruserros ( <i>Link Layer</i> )
Fyysinen kerros ( <i>Physical Layer</i> )	

**Kuva 2.** OSI- ja TCP/IP-viitemallit.

ITS-järjestelmiin liittyneitä asemia varten on standardissa ETSI EN 302 665 [22] määritelty oma viitearkkitehtuuri. Kuva 3, joka perustuu standardiin [22], esittää yksinkertaistetun mallin viitearkkitehtuurista, joka on sama kaikille ITS-järjestelmään liittyneille asemissa. Siitä voidaan havaita pääsykerros (*Access*), tiedonsiirtokerros (*Networking & Transport*), palvelukerros (*Facilities*) sekä ylimpänä sovelluskerros (*Applications*). Näitä reunustavat hallintakerros (*Management*) ja tietoturvakkerros (*Security*). Siniset nuolet ilmaisevat kaksisuuntaisia tiedonvaihtokanavia, joiden kautta kerrokset vaihtavat informaatiota keskenään.



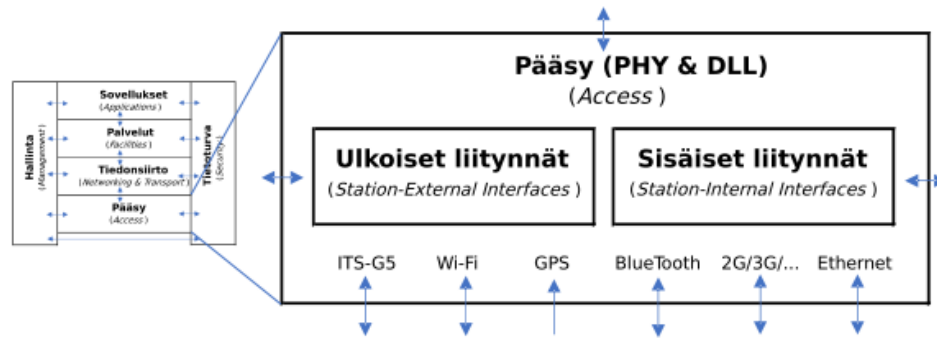
**Kuva 3.** ITS-järjestelmään kytketyn laitteen viitearkkitehtuuri.

Kuten ITS-aseman viitearkkitehtuurista voidaan huomata, se muistuttaa hieman OSI-viitemallia ja vielä enemmän TCP/IP-viitemallia. Tämä johtuu standardin [22] määrittelemästä viitearkkitehtuurista, jossa pääsykerros vastaa OSI-mallin fyysistä kerrosta ja siirtoyhteyserrosta (TCP/IP-peruskerros), tiedonsiirtokerros verkko- ja kuljetuskerroksia sekä palvelukerros istunto-, esitystapa- ja sovelluskerroksia (TCP/IP-sovelluskerros). Reunoilla olevat hallinta- ja tietoturvakkerrokset vastaavat sekä kommunikation hallintaa että tietoturvapalveluista, jotka ovat yhteiset kaikille kerroksille. Ylin sovelluskerros sisältää ITS-spesifisiä sovelluksia ja palveluita.

Seuraavissa luvuissa kuvataan tarkemmin ITS-viitearkkitehtuurin eri kerrosten sisältöä ja toimintoja.

### 3.3.1 Pääsykerros (Access)

ITS-aseman viitearkkitehtuurin alin pääsykerros vastaa TCP/IP-mallin alinta kerrosta. Kuva 4, joka perustuu standardiin [22], esittää yksityiskohtat pääsykerroksen toimintoista ja viestintäkanavista. Havainnollistamisen helpottamiseksi kuvan vasempaan reu-



**Kuva 4.** Pääsykerroksen yleiskuvaus.

naan on jätetty pienikokoinen viitearkkitehtuurin kuvaus. Viestintää varten olevia loogisia kanavia ovat muun muassa Ethernet-, BlueTooth-, GPS- sekä ITS-G5-kanavat. Pääsykerros sisältää lisäksi liitännät niin aseman ulkoisille kuin sisäisillekin yhteyksille.

Pääsykerroksen tarkoituksena on ottaa vastaan tiedonsiirtopaketteja, jotka on lähetetty tiettyyn fyysiseen osoitteeseen (esimerkiksi MAC-osoite). ITS-ympäristössä varsinkin ajoneuvojen kohdalla paketteja otetaan vastaan käyttäen yleensä sellaisia langattoman tekniikan loogisia kanavia kuin WiFi, 2G, 3G, 4G ja 5G.

Standardi ETSI ES 202 663 [23] määrittelee pääsykerroksen vielä tarkemmin siten, että siihen kuuluu OSI-mallin mukaiset fyysinen kerros (PHY) sekä DLL-kerroksen MAC-alikerros. Siinä on määritelty pääsyteknologioita PHY- ja MAC-kerroksille, joita kutsutaan yhteisnimityksellä ITS-G5-teknologiat. Standardi määrittelee myös, että ITS-G5A-taajuusalueen teknologioiden tulisi toimia verkon tukiaseman tuen ulkopuolella. Standardin mukaan pääsykerroksella toteutetaan myös ruuhkanhallintaa, jossa MAC-alikerroksella toimii esimerkiksi siirtotielle pääsymekanismi *Carrier Sense Multiple Access (CSMA)*. PHY- ja MAC-kerrokset tukevat myös ylempien kerrosten ruuhkanhallintaa, sillä ITS-G5-teknologioihin kuuluu useammalle kerrokselle jaettu hajautettu ruuhkanhallinta *Distributed Congestion Control (DCC)*.<sup>2</sup>

Loogisten kanavien yhteyspisteiden lisäksi pääsykerros sisältää yhteyspisteet ympäröiville viitearkkitehtuurin kerroksille. Näitä ovat hallinta-, tiedonsiirto- sekä tietoturvakerrokset. Aivan kuten TCP/IP-viitemallin mukaisessa tapauksessa, pääsykerros ottaa vastaan bittejä jotakin fyysistä mediaa pitkin ja siirtää ne tiedonsiirtokerrokselle eteenpäin lähetettäväksi.

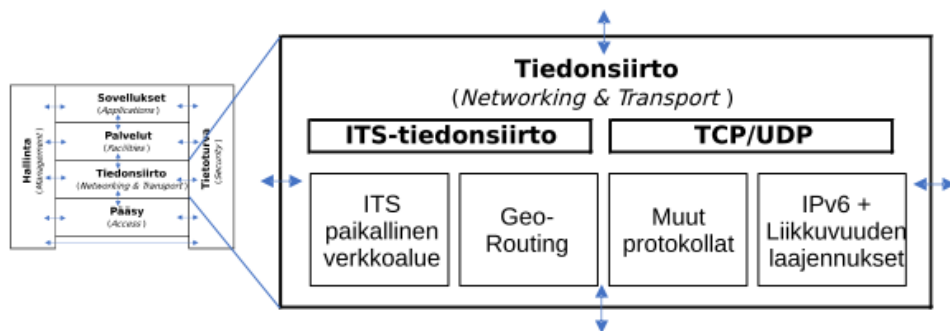
<sup>2</sup> ITS-järjestelmien pääsykerroksen ruuhkanhallintamekanismit on määritelty standardissa ETSI TS 102 687.

### 3.3.2 Tiedonsiirtokerros (*Networking & Transport*)

Tiedonsiirtokerros vastaa TCP/IP-viitemallin verkko- ja kuljetuskerroksia. Tämän kerroksen tehtävänä on kuljettaa tietoliikennepaketteja verkon yli lähettävän aseman ja vastaanottavan aseman välillä. Verkkokerrosta vastaavia tehtäviä varten on ITS-ympäristöön määritetty GeoNetworking-protokolla [22]. Tämän lisäksi käytetään myös IPv6 (IP versio 6) -protokollaa eri menetelmin, kuten esimerkiksi GeoNetworking-protokollan päällä tai liikkuvuuden tuella varustettuna. Verkkokerroksella käytössä on myös CALM FAST -protokolla.<sup>3</sup>

Kuljetuskerrosta vastaavia tehtäviä hoitavat tutut TCP- ja UDP (*User Datagram Protocol*) -protokollat. Näiden lisäksi käytössä on myös joitakin ITS-spesifisiä kuljetusprotokollia. Kuva 5, joka perustuu standardiin [22], esittää yleiskuvauksen tiedonsiirtokerroksesta. Sen yläosasta voidaan havaita kuljetuskerrosta vastaavat protokollat ITS-tiedonsiirto ja TCP/UDP. Alaosasta voidaan havaita verkkokerrosta vastaavia protokollia, joista GeoRouting-elementti sisältää GeoNetworking-protokollan.

Myös tiedonsiirtokerroksella toimii DCC-ruuhkanhallintajärjestelmiä. Verkkokerrososuudella toimivat järjestelmät ovat *Transmit Power Control* (TPC) ja *Transmit Rate Control* (TRC). Muuten tiedonsiirtokerroksen tehtävät vastaavat TCP/IP-viitemallin verkko- ja kuljetuskerroksien tehtäviä. Se käsittelee pääsykerrokselta saatuja tietoliikennepaketteja ja lähettää ne vastaanottavan aseman tiettyyn porttiin käyttäen joko ITS-spesifisiä, TCP- tai UDP-kuljetusprotokollia. Vastaavasti se myös vastaanottaa sille lähetettyjä paketteja tietyn portinumeron kautta.



**Kuva 5.** Tiedonsiirtokerroksen yleiskuvaus.

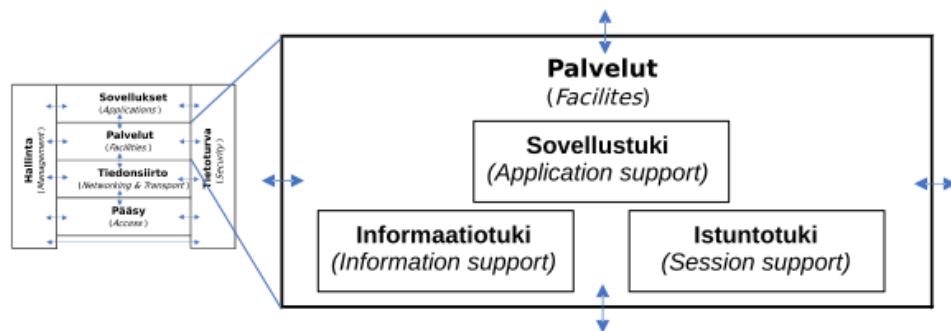
<sup>3</sup> GeoNetworking-protokolla on määritelty standardissa ETSI TS 102 636 (kaikki osat), IPv6-protokollan eri menetelmiä standardeissa ISO/IEC 21210 ja ETSI TS 102 636-6-1 sekä CALM FAST -protokolla standardissa ISO/IEC 29281.

### 3.3.3 Palvelukerros (*Facilities*)

Palvelukerros sisältää sovellusten käyttämät protokollat, joilla toimitetaan käyttäjille palveluita tai vaihdetaan sovellusten sisältämää dataa käyttäen alempia tiedonsiirtoprotokollia. Periaate on sama kuin esimerkiksi TCP/IP-viitemallin sovelluskerroksella. Palvelukerroksella toimivista sovelluksista ja palveluista useimmat ovat ITS-ympäristöä varten kehitettyjä. Niitä on lukuisia ja ne on yleisesti määritelty ETSI EN 302 665 -standardissa [22]. Palvelukerroksen yläpuolella toimiva ITS-spesifinen sovelluskerros sisältää useita eri sovelluksia, joiden viestintätuki sijaitsee palvelukerroksella. Palvelukerros sisältää siis sanomahallinnon tuen yleiselle tiedonvaihdolle ITS-laitteiden sovellusten välillä [22].

Tiedonvaihtoon käytettäviä standardissa määriteltyjä sanomia ovat esimerkiksi ympäristön tapahtumasanomat, joita käytetään muiden muassa ruuhkatilanteista ilmoittamiseen, sekä sanomat kaikkien ITS-laitteiden olinpaikasta. Yleisimmät sanomat ja niiden sovellusympäristöt kuvataan tarkemmin Sovelluskerrosluvussa. Kaikille näille sovelluksille ja sanomille yleinen sanomahallinnon tuki sijaitsee palvelukerroksella. Kuva 6, joka perustuu standardiin [22], esittää palvelukerroksen yleiskuvauksen, jossa palvelut sisältävät tuen niin informaatiolle, istunnolle kuin sovelluksillekin. Näiden lisäksi siinä on yhteyspisteet ympäröiville kerroksille.

Muita palvelukerroksen sisältämiä tukipalveluita ovat esimerkiksi yleinen *Human-Machine Interface* (HMI) -tuki. Tämä on käyttöliittymä, jonka avulla kone pystyy esittämään informaatiota ihmiselle. Toinen esimerkki tukipalvelusta on osoitetuki, joka tukee alempien kerrosten osoitteenmuodostusta. Kuten jo aiemmin mainittiin, kaikki nämä palvelut on kuvattu standardissa ETSI EN 302 665 [22].



**Kuva 6.** Palvelukerroksen yleiskuvaus.

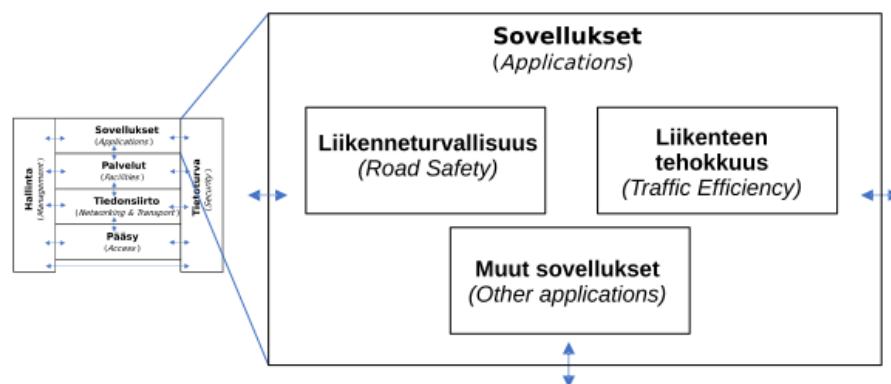
### 3.3.4 Sovelluskerros (*Applications*)

Standardissa ETSI TR 102 638 [24] määritellään ITS-ympäristössä käytettävät perussovellukset, *Basic Set of Applications* (BSA). Nämä BSA-sovellukset on kehitetty pääosin

ajoneuvoympäristöä varten, joka käsittää kommunikoinnin ajoneuvojen välillä sekä ajoneuvojen ja infrastruktuurin välillä. Kuva 7, joka perustuu standardiin [22], esittää yleiskuvauksen sovelluskerroksesta, jossa kahtena tärkeimpänä sovelluksena ovat liikenneturvallisuuden (*Road Safety*) sekä liikenteen tehokkuuden (*Traffic Efficiency*) liittyvät sovellukset. Siitä voidaan myös havaita ympäröivien kerrosten väliset yhteyspisteet, joita siniset nuolet esittävät. Esimerkiksi sovellus- ja palvelukerrosten välinen kaksisuuntainen yhteyspiste on FA-SAP (*Facilities/Applications - Service Access Point*). Tämän pisteen kautta sovelluskerroksen sovellusten tuottamat sanomat siirtyvät palvelukerroksella sijaitsevalle sanomahallinnon tuelle käsiteltäviksi.

**Liikenneturvallisuus** eli *Road Safety* -sovelluspaketin sovellukset liittyvät yleisen liikenneturvallisuuden parantamiseen tiellä. Se sisältää kaksi kuljettajaa avustavaa sovellusta, *Cooperative Awareness (CA)* sekä *Road Hazard Warning (RHW)* [26]. CA-sovellus sisältää neljä elementtiä ajoa avustavaan käyttötarkoitukseen: varoitus hälytysajoneuvosta, ilmoitus hitaasta ajoneuvosta, varoitus risteysalueen onnettomuudesta ja ilmoitus lähestyvistä moottoripyörästä. CA-sovellus pyörittää CA-peruspalvelua (*Cooperative Awareness Basic Service*), joka käsittää yleisen tietoisuuden kaikkien ITS-laitteiden olinpaikasta, kulkusuunnasta, nopeudesta ja muista muuttujista [19]. Tämä yhteistoiminnallinen tietoisuus on toteutettu *Cooperative Awareness Message (CAM)* -sanomilla, joita kaikki ITS-järjestelmään kytketyt laitteet lähettävät tukiasemalle säännöllisesti 0,1–1 sekunnin välein [19].

RHW-sovellus tiedottaa liikenteen ja tien vaaratilanteista kaikille käyttäjille [26]. Standardin mukaan sovellus tiedottaa vaarasta esimerkiksi sijainnin, ajallisen keston, vakuusasteen sekä kehittymisen ajan ja tilan suhteen. Tiedottamisen hoitaa *Decentralized Environmental Notification (DEN)* -peruspalvelu, joka käyttää tiedottamiseen DENM (*DEN Message*) -sanomia [20]. Sanomat on jaettu neljään ryhmään, jotka ovat uusi, päivitettävä, peruttava ja negatiivinen. Viimeisellä vahvistetaan jonkin tilanteen päättymisen.



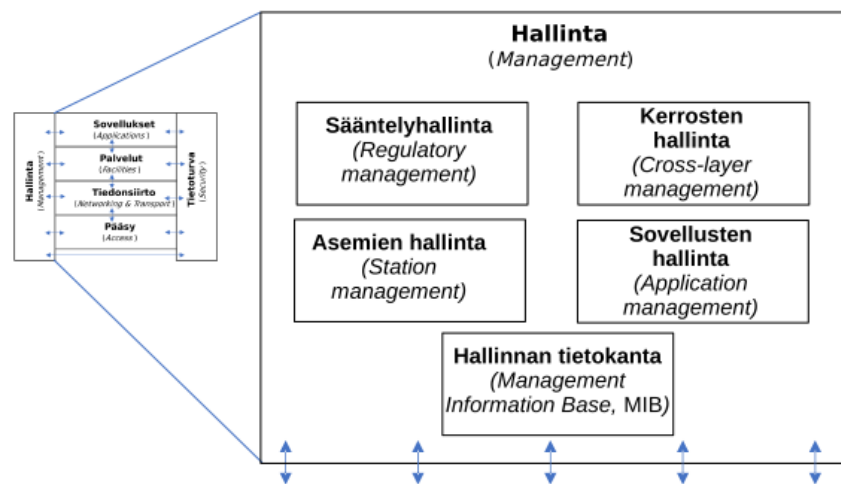
**Kuva 7.** Sovelluskerroksen yleiskuvaus.

**Liikenteen tehokkuus** eli *Traffic Efficiency* -sovelluspaketin sovellukset liittyvät liikenteen tehokkuuden parantamiseen [26]. Perusideana on toimittaa reaaliaikaista liikennetietoa tien käyttäjille. Liikennetiedot on mahdollista saada käyttämällä hyväksi CAM- ja DENM-sanomia, joiden avulla keskusjärjestelmät laskevat ja tuottavat reaaliaikaista liikennedatua. Sovelluspaketin sisältämiä sovelluksia ovat esimerkiksi ajonopeuden hallintaan liittyvät sovellukset sekä yhteistoiminnallinen navigointisovellus, joka ilmoittaa suositeltavia ja nopeimpia ajoreittejä.

**Muut sovellukset** eli *Other Applications* -sovelluspakettiin liittyvät sovellukset ovat esimerkiksi sijainnin perusteella tarjottavat paikalliset palvelut, kuten ajoneuvon huoltopalvelut, tai sopivan pysäköintipaikan etsiminen ja hallinta [26]. Pakettiin liittyy myös erilaisia viihdepalveluja, kuten paikallisen mainonnan vastaanottaminen tai mediapalvelujen lataaminen.

### 3.3.5 Hallintakerros (*Management*)

Standardissa EN 302 665 [22] määritellään ITS-aseman hallintakerroksen toimintaa. Kuva 8, joka perustuu standardiin [22], esittää yleiskuvauksen hallintakerroksesta. Siinä on eritelty joitain elementtejä, kuten aseman hallinta (*Station Management*) ja sovellusten hallinta (*Application management*). *Management Information Base (MIB)*<sup>4</sup> -elementti on kommunikoinnissa käytetty hallinnan tietokanta, johon yleensä ollaan yhteydessä SNMP (*Simple Network Management Protocol*) -protokollan avulla.



**Kuva 8.** Hallintakerroksen yleiskuvaus.

Hallintakerros on koko ITS-aseman pääydin, joka hallitsee kaikkien kerrosten toimintoja. Tämä kerros sisältää hallinnan niin verkotukselle, kommunikaatiolle, ITS-sovelluksille, ITS-asemille kuin kerrosten väliselle tiedonvaihdonkin. Hallintakerros sisältää lisäksi

<sup>4</sup> Standardi ETSI TS 102 732-2 (*Part 2*) määrittelee MIB-tietokannan käytön ITS-ympäristössä.

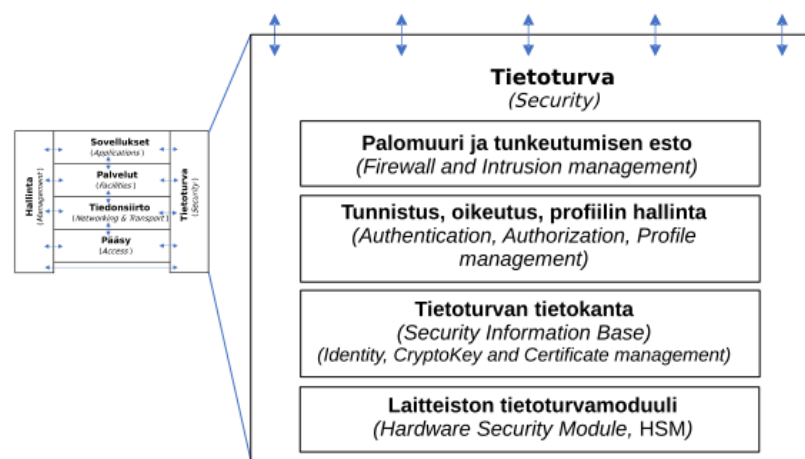
elementit ITS-kommunikoinnin palvelunhallintaan, joka tarkastelee kommunikoinnin toimintaa. Hallintakerros hallitsee myös yleisen ruuhkanhallinnan toimintaa ja sen eri kerroksilla suoritettavia toimintoja.

Standardin [22] mukaan hallintakerroksen tehtäviin kuuluu uusista ITS-palveluista ilmoittaminen asemille. ITS-järjestelmät tukevat kahta mekanismia, *push* ja *pull*, joiden avulla ITS-aseman tulisi tunnistaa palveluiden olemassaolo. *Push*-mekanismista käytetään nimitystä *ITS Service Advertisement*, jolla palveluiden olemassaolo ilmoitetaan.

### 3.3.6 Tietoturvakeros (Security)

Standardin [22] mukaan tietoturvakeros voidaan ajatella olevan osa hallintakerrosta, mutta kuitenkin se esitetään viitearkkitehtuurissa omana yksikkönään. Kuva 9, joka perustuu standardiin [22], esittää yleiskuvauksen tietoturvakerosesta. Se sisältää palomuurin, tunkeutumisen eston ja tunnistuksen hallinnat sekä tietoturvan tietokannan, joka liittyy esimerkiksi sertifikaattien hallintaan. Tietokannan voidaan katsoa kuuluvan osana MIB-tietokantaan. Tietoturvakeros kuuluu myös laitteiston tietoturvamoduuli sekä yhteyspisteet kaikille muille viitearkkitehtuurin kerroksille.

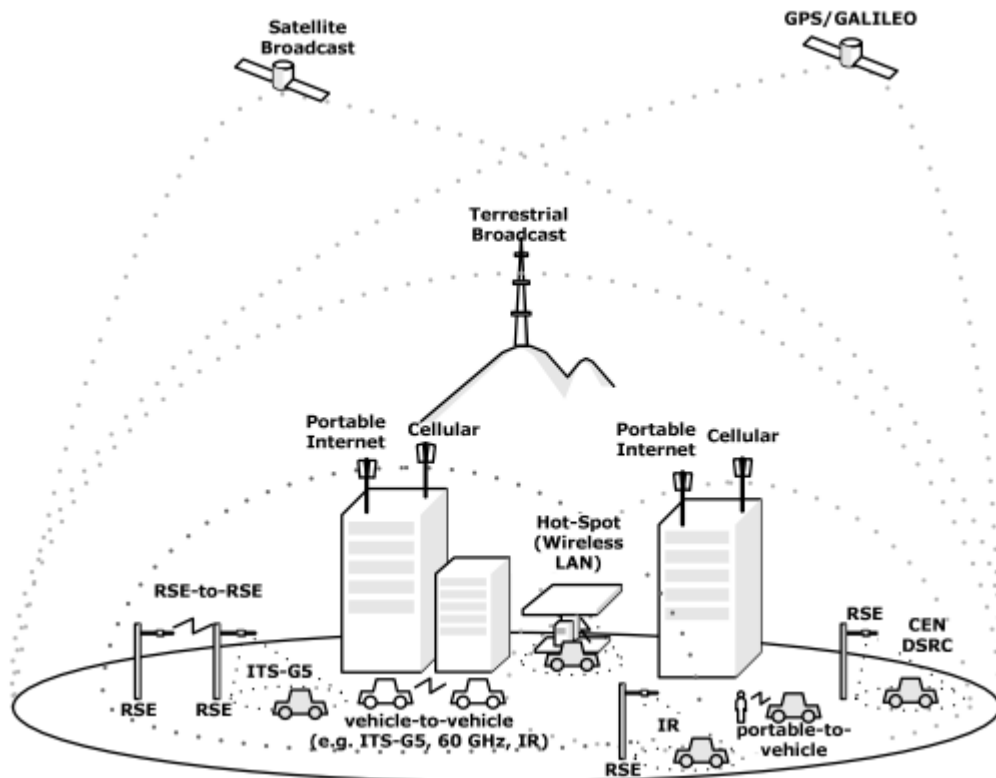
ITS-asemien tietoturvaa ja sen toimintoja kuvataan tarkemmin luvussa 5 ITS-ympäristön tietoturvamekanismit. Kuitenkaan ITS-tietoturvan standardit eivät määrittele tarkemmin esimerkiksi palomuurin toimintaa, tunkeutumisen estojärjestelmiä, laitteiston tietoturvamoduulia tai tietoturvan tietokantaa. Tästä on siis pääteltävä, että näihin kyseisiin elementteihin ei liity mitään ITS-spesifisiä toimintoja, vaan niiden toiminta on täysin vastaavaa kuin millä tahansa laitteistoalustalla. Luku 5 keskittyykin ITS-standardeista löytyviin määritelmiin, jotka pääosin liittyvät tunnistukseen, oikeutukseen ja profiilin hallintaan.



**Kuva 9.** Tietoturvakerosikön yleiskuvaus.

### 3.4 Kommunikointi ITS-ympäristössä

Standardin ETSI EN 302 665 [22] mukaan ITS-kommunikointi on uudentyyppinen kommunikointijärjestelmä, joka on omistettu erityisesti liikenteen ja kuljetusten tarpeisiin. Kuva 10 esittää havaintoesimerkin ITS-järjestelmien kommunikointiympäristöstä, joka perustuu ITS-verkkoalueeseen ja yleiseen verkkoalueeseen. ITS-verkkoalue viittaa kaikkiin niihin laitteisiin ja asemiin, jotka on määritelty ITS-standardeissa. Yleinen verkkoalue viittaa kaikkiin muihin asemiin, joita ympäristössä käytetään.

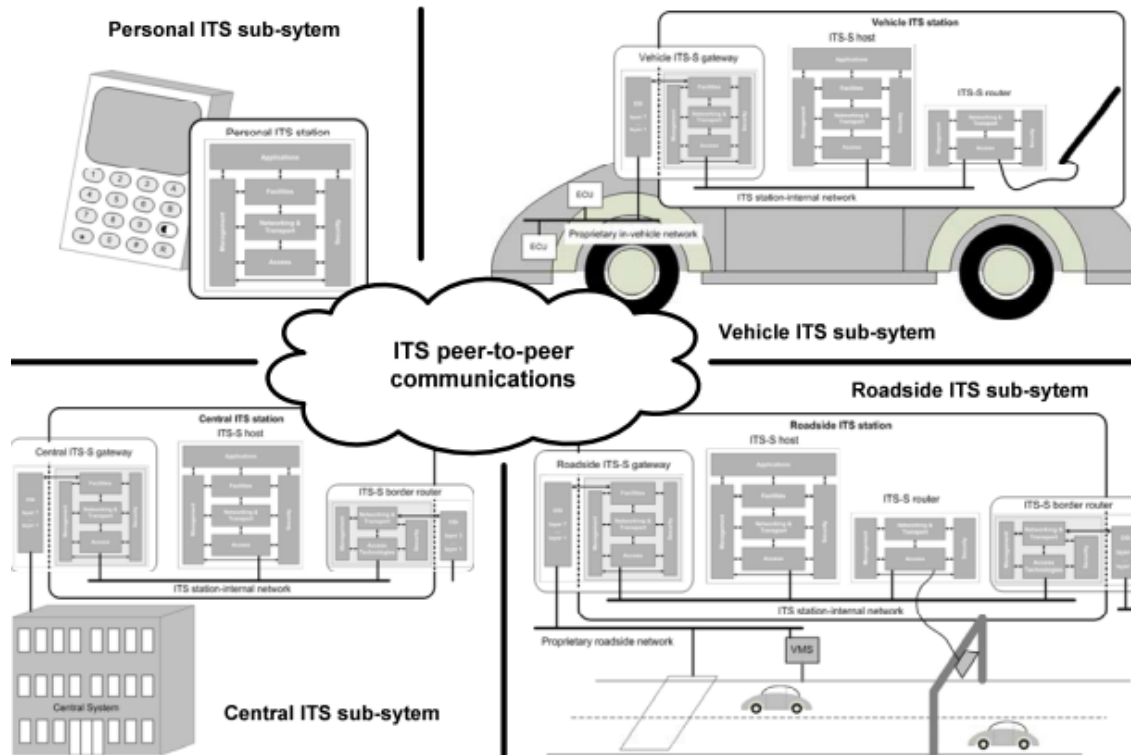


*Kuva 10. ITS-kommunikoinnin havaintoesimerkki [22].*

Kuva 11 esittää ITS-kommunikaatioon osallistuvat asemat. Ne on jaettu neljään alijärjestelmään:

- henkilökohtaiset laitteet (mobiililaitteet),
- keskusalijärjestelmä (osa ITS-keskusjärjestelmää),
- ajoneuvot,
- tienvarsiyksiköt.

Kaikki näihin alijärjestelmiin kuuluvat laitteet sisältävät ITS-viitearkkitehtuurin mukaisen rakenteen eli ne ovat ITS-asemia. Henkilökohtaiset laitteet ovat kädessä pidettäviä laitteita, kuten älypuhelimia, jotka sisältävät ITS-aseman. Keskusalijärjestelmä on määritelty omaksi ITS-asemakseen, joka on oletusyhdyntävä kautta yhteydessä keskusjärjestelmään ja joka sisältää myös reitittimen. Ajoneuvojen alijärjestelmään kuuluvat



**Kuva 11.** ITS-alijärjestelmät [22].

ITS-asetat, jotka ovat henkilöautoissa, kuorma-autoissa ynnä muissa ja jotka sisältävät niin oletusyhdykäytävän kuin reitittimenkin. Tienvarsiyksiköt ovat ITS-asemia, jotka sisältävät oletusyhdykäytävän, isännän ja reitittimen. Ne ovat käytännössä tukiasemia, jotka ovat kiinteästi asennettu mastoihin tai muihin kiinteisiin alustoihin.

ITS-aseman oletusyhdykäytävä yhdistää eri asemia TCP/IP-viitemallin ylimmällä sovel-luskerroksella eli ITS-viitemallin palvelukerroksella. ITS-aseman reititin puolestaan käyttää kerrosta 3 (tiedonsiirto, TCP/IP-kerrokset 2 ja 3) kahden eri aseman yhdistämi-seen. Keskusalijärjestelmien, ajoneuvojen ja tienvarsiyksiköiden ITS-asetat sisältävät myös erikseen reunareitittimen (*border router*), joka käyttää kerrosta 3 yhteyden ottami-seen sillä erolla, että se ottaa yhteyden ITS-verkkojärjestelmän ulkopuolisiin asemiin.

Tässä luvussa kuvattu ja kommunikoinnin viitearkkitehtuuria ja menetelmiä käytetään myös autonomisten ajoneuvojen verkkoympäristössä, joka on pienempi osakokonaisuus älykkäistä kuljetusjärjestelmistä. Siihen tutustutaan tarkemmin seuraavassa luvussa.

## 4. AUTONOMISTEN AJONEUVOJEN VERKKOYMPÄRISTÖ

Verkkoympäristö, johon autonomiset ajoneuvot ovat kytkettyinä, on pienempi osakokonaisuus ITS-järjestelmästä. Samoin kaikki ITS-standardit ja viranomaismääritelmät ovat voimassa ajoneuvojen ympärille rakennetussa verkossa ja kommunikoinnissa. Tässä luvussa tarkastellaan hieman tarkemmin näitä ajoneuvoja varten määriteltyjä verkkoympäristöjä, ensin peruskommunikointiin keskittyvää *Vehicle-to-Everything* (V2X) -ympäristöä, toiseksi uusia lisäominaisuuksia tuovaa *Cellular V2X* (C-V2X) -ympäristöä sekä viimeiseksi oikeaa V2X-testiympäristöä, joka on rakennettu Tampereelle.

### 4.1 *Vehicle-to-Everything* (V2X) -kommunikointi

V2X-termi on lyhenne sanoista *Vehicle-to-Everything*, joka nimensä mukaisesti tarkoittaa verkkoympäristöä, jossa ajoneuvo on yhteydessä kaiken ulkopuolisen kanssa. Tällaiseen verkkoympäristöön kuuluvat esimerkiksi toiset ajoneuvot, tieinfrastruktuuri kuten liikennemerkkit, liikennevalot ja erikseen rakennetut tukiasemat, sekä jalankulkijat. V2X-termi voidaankin purkaa erillisiksi termeiksi yhteystyyppien mukaan: ajoneuvojen välinen kommunikointi *Vehicle-to-Vehicle* (V2V), ajoneuvojen ja infrastruktuurin välinen kommunikointi *Vehicle-to-Infrastructure* (V2I), ajoneuvojen ja jalankulkijoiden välinen kommunikointi *Vehicle-to-Pedestrian* (V2P), ajoneuvojen ja verkon välinen kommunikointi *Vehicle-to-Network* (V2N) ja niin edelleen. Kuva 12 esittää havainnollistavan esimerkin V2X-ympäristöstä ja eri yhteystyypeistä.



**Kuva 12.** V2X-ympäristön havaintoesimerkki [11].

Qualcommin esityksen [11] mukaan V2X-kommunikoinnilla on paljon erilaisia käyttötilanteita, kuten esimerkiksi varoitukset edessä olevasta törmäysmahdollisuudesta, jonosta, huonon näkyvyyden risteyksestä tai tilannenopeudesta mutkassa. Käyttötilanteita ovat myös mukautuva vakionopeussäädin ja automaattinen jonoajo, pysäköintipaikan ja sähköauton latauspaikan näyttäminen sekä ilmoitus lähestyvistä hälytysajoneuvosta.

Yleisesti ottaen V2X-kommunikointi tuottaa parannetun aktiivisen liikenneturvallisuuden, koska auton reaaliaikainen tietoisuus ympäristöstään on 360° eli joka suuntaan. Liikenteen tehokkuus paranee, kun autot voivat ajaa lähempänä toisiaan. Myös tietoisuus kaikista ympäristön tilanteista kasvaa, jonka ansiosta ajamisesta tulee jouhevampaa. Tämä kaikki johtaa siihen, että V2X-kommunikoinnilta ja -verkolta vaaditaan vieläkin tehokkaampaa käyttöä, jotta esimerkiksi autojen nopeuksia voidaan kasvattaa entisestään, lisätä uusia käyttötilanteita ja kerätä enemmän dataa autoista. Tällä hetkellä on kehitysasteella laajempi V2X-verkko, jota tarkastellaan seuraavaksi.

## 4.2 Cellular V2X (C-V2X) -kommunikointi

Kun matkapuhelinverkkoihin liittyvää GSM-verkkoa (*Global System for Mobile Communications*) eli niin kutsuttua 2G-verkkoa alettiin kehittää eteenpäin, perustettiin projekti nimeltä 3GPP (*Third Generation Partnership Project*). 3GPP-projektin kehitystyön tuloksena saatiin aikaiseksi matkapuhelinverkkojen kolmas sukupolvi eli UMTS (*Universal Mobile Telecommunications Systems*) -verkko, jota kutsutaan myös 3G-verkoksi. Kun projekti kehittää uusia tekniikoita ja kehitysaskelia, se julkaisee *Release*-versioita. Esimerkiksi joulukuussa 2008 se julkaisi *Release 8* -version, jossa olivat tekniikat LTE (*Long Term Evolution for UMTS*) -verkkoa eli neljännen sukupolven (4G) verkkoa varten [16].

3GPP-projekti julkaisi vuonna 2015 *Release 13* -version, jossa alettiin kehittää LTE-tekniikoita V2X-kommunikointia varten [16]. Version 13 myötä projekti alkoi kehittää myös seuraavan sukupolven (5G) matkapuhelinverkkoa. *Release 14* ja *15* -versiot tuovat edelleen lisäominaisuuksia ja -tekniikoita ajoneuvojen väliseen kommunikointiin. Näiden versioiden aikana on lanseerattu uusi nimi (*LTE Advanced Pro*) tekniikalle, jota käytetään ainakin V2X-kommunikointiin. Matkapuhelinverkkojen hyödyntämisen seurauksena V2X-verkkoympäristölle on annettu nimeksi *Cellular Vehicle-to-Everything (C-V2X)*.

C-V2X-kommunikointi perustuu kahteen viestintärajapintaan, PC5 ja Uu [16]. Periaate näillä rajapinnoilla on, että PC5 on käytössä ajoneuvojen väliseen suoraan kommunikointiin ja Uu ajoneuvojen ja verkon väliseen kommunikointiin. 3GPP-projekti sekä ETSI-standardisointijärjestö ovat yhteistyössä tuottaneet vuoden 2017 aikana standardin ETSI TS 123 285 [36] näiden määritelmien selkeyttämiseksi. Siinä määritellään oma arkkitehtuuri ja viitemalli C-V2X-kommunikointia varten sekä esitetään myös määritelmät PC5- ja Uu-rajapinnoille.

C-V2X-kommunikointi tuo jälleen uusia lisäetuja autojen välisiin yhteyksiin. Näitä ovat esimerkiksi autojen välinen ilman verkon tukiasemaa tapahtuva suora kommunikointi, jonka etäisyys voi olla jopa satoja metrejä [11]. Sen ansiosta yhä useampi auto pystyy kommunikoimaan keskenään samaan aikaan reaaliaikaisesti, olivatpa ne sitten verkon tukiaseman kantoalueella tai eivät.

V2X-kommunikoinnin tuomia haasteita ovat esimerkiksi Doppler-ilmiö, kun autojen nopeus on suhteellisen suuri ja ne ajavat vastakkaiseen suuntaan. Tähän haasteeseen C-V2X-kommunikointi vastaa parannetulla signaalinkäsittelyllä [11]. Toinen esimerkki V2X-kommunikoinnin haasteesta on ajan synkronoinnin lähteen puute, kun auto on verkon tukiaseman kantoalueen ulkopuolella. Tähän C-V2X vastaa parannuksella, jolla hyödynnetään GPS-aikaa eli satelliittia ajan synkronointiin, kun tukiasema ei ole kantomatkan päässä.

Tulevaisuudessa on tavoitteena ottaa käyttöön 5G-verkkoteknologiat. Ensimmäinen vaihe käyttöönotosta tapahtunee vuonna 2020. Teknologiat ollaan ottamassa käyttöön myös C-V2X-ympäristössä, johon saadaan jälleen uusia ominaisuuksia ja parannuksia. Silloin tulee realistisesti mahdolliseksi muiden muassa täysin autonominen ajaminen sekä V2X-pohjainen lisätty todellisuus, jossa esimerkiksi kuorma-auton takana ajettaessa on mahdollista nähdä sen eteen.

Yhteenvetona voidaan todeta, että autonomisten ajoneuvojen verkkoympäristössä on käytössä kaksi eri verkkoteknologiaa. V2X-kommunikointi perustuu IEEE 802.11p -standardin pohjalta määriteltyihin teknologioihin eli ajoneuvokäyttöön tarkoitettuihin langattomiin lähiverkkoteknologioihin. Näitä varten Euroopan alueelle on määritelty ITS-G5-standardit. C-V2X-kommunikointi puolestaan perustuu LTE-teknologioihin eli matkapuhelinverkkoteknologioihin. Suomeen on rakennettu näitä molempia teknologioita hyödyntävä testausympäristö, joka tunnetaan nimellä Tampere UrbanAutoTest.

### 4.3 Tampere UrbanAutoTest

Suomen tieliikennelaki ja -asetukset sallivat autonomisen ajamisen testaamisen jo nyt. Siksi on ollut mahdollista perustaa Tampereelle UrbanAutoTest-projekti [44]. Projektin tietojen [44] mukaan sen päätehtävä on sekä auttaa että helpottaa yrityksiä kehittämään ja testaamaan autonomisen ajamisen toimintoja. Projektissa on mukana joukko yrityksiä, kuten Teknologian tutkimuskeskus VTT Oy, Tieto Oyj, TTS Työtehoseura, Taipale Telematics, HERE, sekä Tampereen kaupunki ja Liikenteen turvallisuusvirasto Trafi. Projektin mukaan se on kehittänyt testausympäristön, joka koostuu sekä suljetun että julkisen tieverkon testiradasta. Julkisen tieverkon testiympäristö sijaitsee Tampereella, jossa testiajoneuvoilla ajetaan normaalin liikenteen seassa. Kuva 13 esittää Tampereen testiympäristön rataprofiilin. Testausympäristöön sisältyy myös testauslaitteita, oikeaksi todistamista ja varmentamista, teknologian tutkimusta ja konsultointipalveluja sekä testausajoneuvoja ja -työkaluja.



**Kuva 13.** Tampereen testausympäristön rataprofiili [13].

Projektin muihin päätehtäviin kuuluu kehittää Tampereelle testiympäristö, joka perustuu olemassa oleviin ja aiempien projektien yhteydessä kehitettyihin testauslaitteisiin [13]. Kehitettävänä on myös toimintakykyinen palvelumalli testauspaikalle.

VTT Oy:n tekemän esityksen [13] mukaan UrbanAutoTest-projekti muokkaa testiajoneuvoja siten, että yritykset voivat testata ja kehittää automaattisen ajamisen toiminnollisuuksia, kuten esimerkiksi sensoreita ja käyttöliittymiä. Esityksen mukaan muokkauksen yhteydessä on kehitetty prototyypisovellus automaattiselle ohjaukselle. Tampereen alueelle on asennettu 2 tienvarsiyksikköä, joiden tukiasemat tukevat ITS-G5-standardien mukaista liikennettä.

Koska kyse on autonomisen ajamisen testistä, on sitä varten rakennettu myös muutama autonominen ajoneuvo. Esimerkkinä voidaan mainita kaksi testiajoneuvoa, Citroen C4 ja Volkswagen Touareg. Citroen C4 -autoon on asennettu testiä varten muiden muassa lasersertukat (toimintasäde 120 metriä), pitkän kantaman tutka (200 metriä), lyhyen kantaman tutka (50 metriä), laitteet ITS-G5- sekä LTE-kommunikaatiota varten sekä paljon muuta laitteistoa. Nämä autot saavat ajaa normaalisti Suomen tieliikenteessä liikenneturvallisuusvirasto Trafín myöntämän koenumerotodistuksen ja sen myötä saatujen koenumero-kilpien perusteella.

Testiympäristöjen myötä autonominen ajaminen tulee aina askeleen lähemmäksi todellisuutta. Siksi onkin tärkeää keskittyä myös tietoturvaan liittyviin asioihin. Seuraavassa luvussa käsitellään tietoturvamekanismeja, joita on kehitetty ITS-ympäristöä varten.

## 5. ITS-YMPÄRISTÖN TIETOTURVAMEKANISMIT

Jotta V2X-kommunikointi voisi tapahtua turvallisesti, tarvitsee se tietoturva- ja kommunikointi-infrastruktuurin, joka varmistaa tietoliikenteen luotettavuuden. Jokaisen tietoliikenneviestin lähteen on oltava luotettu ja viestin sisällön on oltava suojattu ulkopuolisilta häiriöiltä. Tässä luvussa esitellään muutamia tietoturvamekanismeja, joita käytetään ITS-ympäristössä. Luvun loppupuolella tarkastellaan yleistasolla uusia, vielä osittain kehitystasolla olevia C-V2X-kommunikoinnin tietoturvanäkökulmia.

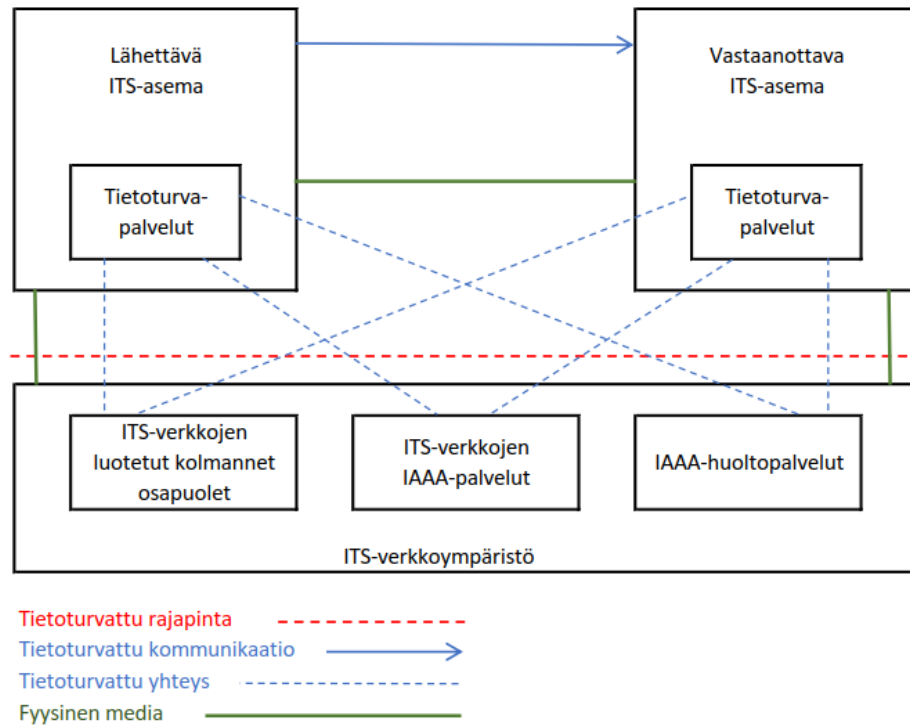
Yleisellä tasolla ajateltuna tietoturvamekanismit voidaan jakaa kolmeen perusalueeseen: fyysiseen, hallinnolliseen ja informaatiolliseen. Fyysinen tietoturva sisältää esimerkiksi lukot, hälyttimet ja vartioinnin, joilla voidaan suojautua luvatonta sisäänpääsyä vastaan. Sosiaalishallinnollinen tietoturva käsittää niin lait, säännöt ja rangaistukset kuin henkilöstön valinnankin. Puolestaan teknishallinnollinen tietoturva käsittää muiden muassa loikit eli tapahtumakirjanpidon, pääsynvalvonnan sekä oikeus- ja nimeämiskäytännöt. Informaatiollinen tietoturva koostuu esimerkiksi tunnistuksesta, sähköisestä allekirjoituksesta sekä salauksesta.

V2X-kommunikaation tietoturvamekanismit perustuvat pohjimmiltaan yleisen tason ajattelumalliin. Sen lisäksi siinä käytetään ITS-ympäristöä varten määriteltyjä tietoturvastandardeja. Ne kuuluvat aiemmin kuvattuihin ITS-G5-standardeihin. Niissä on määritelty tarkemmin esimerkiksi ITS-aseman tietoturva-arkkitehtuuri ja -palvelut.

### 5.1 Tietoturva-arkkitehtuuri

Standardi ETSI TS 102 731 [27] määrittelee perustason käsitteet ja pääpiirteet ITS-ympäristön tietoturvapalveluille ja -arkkitehtuurille. Siinä käytetään eri mekanismeja turvalliseen ja yksityisyyden suojaavaan kommunikaatioon. Ensin tarkastellaan arkkitehtuuria ja myöhemmin tietoturvapalveluita.

Kuva 14, joka perustuu standardiin [27], esittää periaatekaavion ITS-ympäristön kommunikaation tietoturva-arkkitehtuurista. Siinä on havainnollistettu perustilanne, jossa on sekä lähetävä että vastaanottava ITS-asema, joiden sisällä tietoturvapalvelut ovat suojaamassa yhteyttä. Asemat ottavat suojatun yhteyden ITS-verkkoon turvatun rajapinnan kautta. Rajapintaa kuvaa punainen katkoviiva. Rajapinnan sisällä toimivat esimerkiksi kaikki luotetut kolmannet osapuolet ja huoltopalvelut. IAAA (*Identification, Authentication, Authorization, Auditing*) viittaa tunnistukseen, oikeutukseen ja muihin tietoturvapalveluihin ja niihin liittyviin huoltotoimenpiteisiin, kuten kumoamiseen. Tietoturvallinen yhteys kuljetetaan fyysisistä mediaa pitkin, joka esimerkin tapauksessa on esitetty vihreällä värillä.



**Kuva 14.** Periaatekuva ITS-tietoturva-arkkitehtuurista.

Standardi ETSI TS 102 731 [27] määrittelee myös tarkemmin ITS-kommunikaation tietoturva-arkkitehtuurin. Se on jaettu siten, että siihen kuuluu ITS-viranomaisten hierarkia, tietoturvan parametrien hallinta sekä viestintämallit. Viranomaisten hierarkia käsittää valmistajat, joiden tulisi määrittellä kaikille ITS-asemille oktetin mittainen ainutlaatuinen tunniste, joka on voimassa koko toiminnallisen eliniän. Hierarkiaan kuuluvat myös sekä rekisteröintiviranomaiset (*Enrolment Authority*) että oikeutusviranomaiset (*Authorization Authority*). Rekisteröintiviranomainen rekisteröi ITS-aseman käyttämällä hyväksyen valmistajan antamaa tunnistetta. Puolestaan oikeutusviranomainen myöntää ITS-asemalle oikeudet ja valtuudet käyttää eri palveluita.

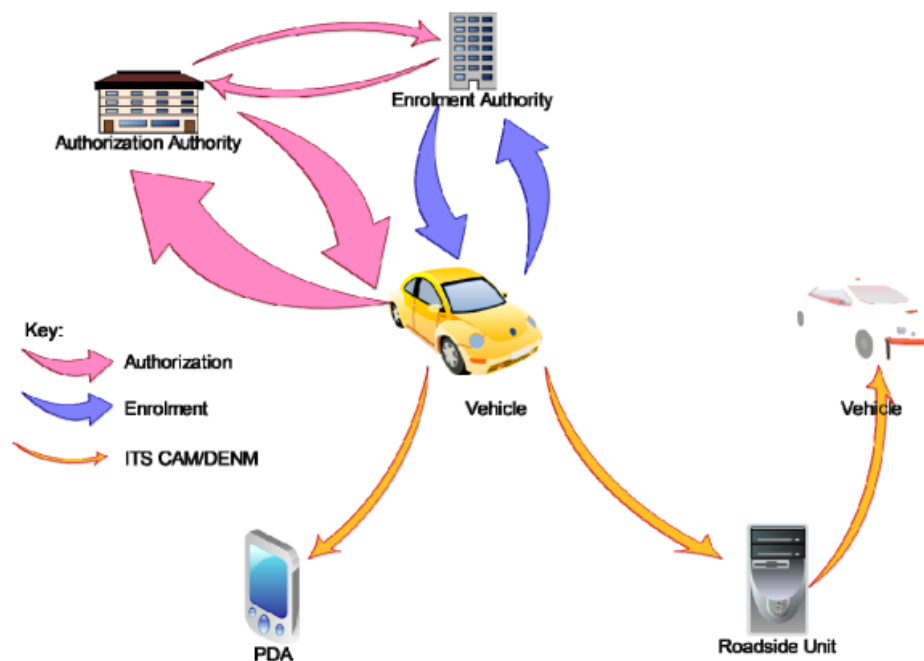
Tietoturvaparametrien hallinta käsittelee standardin [27] mukaan esimerkiksi ITS-asemien tunnistetietoja. Niistä ei saa saada selville mitään henkilöiden yksityisiä ja henkilökohtaisia tietoja. Tämä perustuu niin ihmisoikeuksiin kuin yksityisyydensuojaankin. Jotta ajoneuvon tunnistetiedoista ei minkään linkin kautta saataisi selville henkilön yksityisiä tietoja, on ITS-kommunikaatioon kehitetty erityiset varmennusliput (*Authorization Ticket*). Niiden avulla ajoneuvot voidaan tunnistaa siten, ettei ajoneuvojen alkuperäisiä tunnistetietoja tarvitse käsitellä.

Kommunikaation tietoturva-arkkitehtuurin viimeinen osa käsittää viestintämallit, joilla mahdollistetaan turvattu viestintä. Ensimmäinen malli käsittää julkiset viestit ja sitä käytetään yleislähetystykseen (*broadcast*). Viesteiltä vaaditaan tunnistusta ja eheyttä. Toinen malli käsittää yksityiset viestit, joita lähetetään jollekin tietylle vastaanottajalle (*unicast*).

Näiltä viesteiltä vaaditut ominaisuudet ovat tunnistus, eheys, yksityisyys sekä luotettavuus. Viimeisenä mallina on *Security Association (SA)* eli turvallisuuskäytänteet. Niiden avulla saadaan turvattu yhteys kahden tai useamman ITS-aseman välille pidemmäksi ajaksi. Turvallisuuskäytänteet määrittelevät käytettävät salausalgoritmit, -avaimet sekä muut julkiset ja yksityiset parametrit, joiden avulla niin luotettavuus, tunnistus kuin eheyskin voidaan varmistaa.

Tietoturva-arkkitehtuurin kuvauksen jälkeen voidaan esittää ITS-tietoturvan viitemalli. Se on malli, jossa on kuvattuna kommunikaatioon osallistuvat osapuolet ja niiden välinen turvattu viestiliikenne. Osapuolet ovat rekisteröinti- ja oikeutusviranomaiset, ajoneuvot sekä muut ITS-ympäristön asemat, kuten tienvarsiyksiköt ja henkilökohtaiset mobiililaitteet. Viestiliikenne puolestaan kuljettaa salausavaimilla salattuja viestejä eri osapuolille. Kuva 15 esittää tämän ITS-tietoturvan viitemallin, josta voidaan huomata, että myös CAM- ja DENM-sanomat kuuluvat siihen.

Kuten CAM- ja DENM-sanomat määrittelevistä standardeista [19,20] voidaan todeta, ovat niitä tuottavat sovellukset pakolliset kaikissa ITS-ympäristön laitteissa. Tästä voidaan siis päätellä, että kyseiset sanomat kuuluvat oleellisesti tietoturvan viitemalliin. Näiden sanomien tunnistuksessa sertifikaatit ovat oleellisessa roolissa; saapuvat sanomat hyväksytään vain, jos sertifikaatti on voimassa.



**Kuva 15.** ITS-tietoturvan viitemalli [28].

## 5.2 Tietoturvan hallinta

Standardissa ETSI TS 102 940 [28] on tietoturvan hallinta määritelty ITS-aseman kannalta tarkasteltuna. Se tarvitsee oman turvallisen yhteyden yleisiin kohteisiin, kuten esimerkiksi palveluihin, dataan ja protokolliin. ITS-aseman tietoturva voidaan jakaa ulkoi- siin ja sisäisiin tietoturvavaatimuksiin. Ulkoisten vaatimusten tapauksessa ITS-asema toi- mii yhteyden päätepisteenä, jolloin tietoturvavaatimuksina ovat turvallisuus ja luottamus sekä verkkoon että yhteyden toiseen päätepisteeseen. Sisäisten vaatimusten tapauksessa ITS-aseman ajatellaan olevan prosessointialusta ja sovellusisäntä. Tällöin tietoturvavaa- timuksena on suojata sovelluksia, jaettua dataa, ohjelmistoja sekä laitteistoja. Tällaista linjausta voidaan kutsua ITS-aseman tietoturvan hallinnan peruseräiteeksi.

Jotta ITS-asema saa luotetun yhteyden rekisteröintiviranomaisen palvelimeen, tulee nou- dattaa standardissa [28] määriteltyjä suosituksia yhteyden avaamiseen. Suosituksissa ke- hotetaan säilyttämään kaikki salausavaimien materiaalit muistissa, joka on suojattu tietojen väärentämistä ja muuttamista sekä luvaton lukemista vastaan. Pääsy salausavainma- teriaaleihin tulee sallia vain luvallisille käyttäjille. Avaimet tulee välittää toiselle osapuol- lelle mieluummin salattuna kuin selvätekstinä ja toisen osapuolen tulee olla turvattu pros- essointialusta. Mikään muu sovellus tai moduuli kuin tietoturvamoduuli ei saa muodos- taa suoraa yhteyttä avainmuistiin. Myös tietoturvamoduuli ja sen liityntä avainmuistiin on suojattava väärentämistä, salakuuntelua, manipulaatiota ja muita tietoturvauhkia vas- taan.

### 5.2.1 Luottamuksen ja yksityisyyden hallinta

Tietoturvan hallintaan kuuluu standardin [28] mukaan yhtenä osana myös luottamuksen ja yksityisyyden hallinta. Rekisteröinti- ja oikeutusviranomaiset tuottavat sellaisia palve- luita, jotka tukevat luotetun yhteyden avaamista sekä yksityisyyden suojaamista. Luote- tun yhteyden avaamista tukemaan viranomaistahot toimittavat kaikki tarpeelliset sertifi- kaatit, jotta ITS-asemat voivat käyttää ITS-järjestelmää ja sen palveluita ja sovelluksia. Yksityisyyden suojaamista tukemaan viranomaiset toimittavat pseudonyymit, joita voi- daan käyttää merkityksellisempään tunnistukseen ja joita voidaan vaihtaa toistuvasti, jotta vastaavuuksia ja riippuvuussuhteita voidaan välttää.

Luottamuksen ja yksityisyyden hallinta on määritelty standardissa ETSI TS 102 941 [29], jossa yksityiskohtaisesti ja tarkemmin määritellään luottamus- ja yksityisyysasiat esimer- kiksi valmistajan ja viranomaisten osalta. Siinä myös määritellään tarkemmin salaus- avainten vaihtoon käytettävä julkisen avaimen PKI (*Public Key Infrastructure*) -järjes- telmä.

## 5.2.2 Pääsynvalvonta

Ennen kuin ITS-asema voi käyttää ITS-palveluita ja -sovelluksia täysipainoisesti, täytyy suorittaa pääsynvalvonta (*Access Control*). Sen peruslinjat on määritelty standardissa ETSI TS 102 940 [28] sekä pääsynvalvontamenetelmien tarkat vaatimukset standardissa ETSI TS 102 942 [30]. Viranomaisten myöntämät sertifikaatit voidaan ottaa ITS-aseman käyttöön vasta, kun pääsynvalvontamenetelmät on suoritettu. Menetelmillä suojataan ITS-aseman identiteettiä ja vältetään palveluiden väärinkäyttö. Pääsynvalvontaan kuuluvat sellaiset menetelmät kuin alustus, rekisteröinti ja oikeutus. Osittain näihin termeihin viitattiin jo edellisen luvun Tietoturva-arkkitehtuurin viranomaishierarkiassa, mutta tässä yhteydessä niihin tulee muutamia lisähuomioita.

Alustuksen yhteydessä ITS-asemalle muodostetaan eri valtuustietoja, kuten valmistajan kanssa määriteltävä ainutlaatuinen tunniste. Tämän lisäksi menetelmään kuuluu julkisen ja yksityisen salausavainparin sekä salatun sertifikaatin muodostaminen. Salattu sertifikaatti yhdistää identiteetin ja julkisen salausavaimen ITS-asemaan ja sen profiiliin.

Rekisteröinti suoritetaan dialogina ITS-aseman ja viranomaistahon kanssa. Rekisteröinnissä käytetään hyväksi alustuksen valtuustietoja, joiden avulla voidaan muodostaa rekisteröinnin valtuustiedot. Ne sisältävät esimerkiksi salatun sertifikaatin, joka osoittaa kaikki sovellukset ja palvelut, joita asema on valtuutettu käyttämään. Rekisteröinnin valtuustiedot mahdollistavat aseman pyytää oikeutusta viranomaiselta pseudonyyminä.

Myös oikeutus suoritetaan dialogina ITS-aseman ja viranomaistahon välillä. Oikeutukseen käytetään rekisteröinnin valtuustietoja, joiden avulla muodostetaan oikeutuksen valtuustiedot. Näiden avulla puolestaan muodostetaan yksi tai useampi salattu ja allekirjoitettu sertifikaatti, joilla ITS-asema voi vakuuttaa pseudonyyminä olevansa oikeutettu lähettämään dataa tai viestin toiselle asemalle.

## 5.2.3 Identiteetin hallinta

Standardin ETSI TS 102 940 [28] mukaan identiteetin hallinta on yksi tietoturvan hallinnan osa-alue. Myös standardissa ETSI TS 102 941 [29] määritellään yksityisyyttä liittyen ITS-ympäristöön. Sen mukaan yksityisyyteen liittyy 4 avaintekijää: mahdollisuus esiintyä anonyyminä, mahdollisuus esiintyä pseudonyyminä, mahdollisuus irrottautua yhteydestä sekä mahdollisuus olla havaitsemattomissa. Kuitenkin anonyyminä esiintyminen sekä havaitsemattomissa oleminen ovat sopimattomia ratkaisuja, sillä yhtenä ITS-järjestelmien päävaatimuksena on aseman oleminen havaittavissa, jotta liikenneturvallisuus parane. Puolestaan pseudonyyminä esiintyminen ja yhteydestä irrottautuminen tarjoavat tarkoituksenmukaisen yksityisyydensuojan turvallisuussanomien (CAM- ja DENM-sanomien) lähettäjälle.

Näiden yksityisyyteen liittyvien seikkojen vuoksi oikeutusviranomaisen toimittama ITS-asemalle useita pseudonyymejä ja niihin liittyvät valtuusliput. Yksityisyydensuoja on toteutettu vaihtamalla säännöllisesti aseman pseudonyymiä ja siihen liittyvää sertifiointia. Identiteetin hallinta sisältää valtuutuksien luonnin, varastoinnin, varmentamisen ja kumoamisen.

#### 5.2.4 Luottamuksellisuus

Monet ITS-sovellukset ja -palvelut lähettävät viestejä yleislähetystenä (*broadcast*). Ne on tarkoitettu kaikkien vastaanottajien nähtäväksi ja käsiteltäväksi. Näihin viesteihin ei liity muita luottamuksellisuusvaatimuksia kuin lähettäjän identiteetin suojaaminen. Se varmistetaan lähettämällä viestit pseudonyyminä.

Kuitenkin jotkut sovellukset ja palvelut käyttävät kohdelähetystä (*unicast*) ja ne voivat sisältää esimerkiksi henkilökohtaisia tietoja. Niiden täytyy silloin käyttää tietoturvapalveluita, joilla varmistetaan, että vain tarkoitetut vastaanottajat voivat nähdä viestien sisällön. Tietojen luottamuksellisuus on varmistettu ensisijaisesti salaamalla viestit ja varmistamalla, että salauksen voi purkaa vain tarkoitettu vastaanottaja.

Luottamuksellisuuden menetelmien tarkat vaatimukset on määritelty standardissa ETSI TS 102 943 [31]. Siitä selviää muun muassa, että CA (*Cooperative Awareness*) -palvelu ei tarvitse luottamuksellisuuspalveluita. Siinä mainitaan myös verkkokerrokseen liittyen, että IPv6-protokollan luottamuksellisuuspalvelut tulisi toteuttaa ESP (*Encapsulating Security Payload*) -protokollan avulla IPsec (*Internet Protocol Security*) -protokollapinon sisällä.

### 5.3 Tietoturvapalvelut

Edellisessä luvussa 5.2 käytiin läpi tietoturvan hallinnan eri menetelmiä. Tässä luvussa tarkastellaan lähemmin eri tietoturvapalveluita, joiden avulla kommunikaatiota turvataan ITS-ympäristössä. Tietoturvapalvelut on määritelty standardissa ETSI TS 102 731 [27].

Pääosin tietoturvapalvelut voidaan jakaa kahteen ryhmään. Jako ryhmiin on määritelty standardissa ETSI TS 102 940 [28]. Ensimmäisen ryhmän palvelut ovat sellaisia, joita ITS-asema voi käyttää kommunikoidakseen turvallisesti toisten asemien kanssa. Nämä palvelut toimivat yhden tai useamman ITS-viitearkkitehtuurin (luku 3.3) yhteydessä esitetyn kerroksen sisällä. Toisen ryhmän palvelut ovat sellaisia, jotka toimivat tietoturvan hallintakerroksen sisällä. Tietoturvapalveluita tarkastellaan näihin kahteen ryhmään jaoteltuina seuraavissa alaluvuissa, jotka perustuvat standardien [27,28] tietoihin.

### 5.3.1 ITS-aseman tietoturvapalvelut

Seuraavassa kuvatut tietoturvapalvelut ovat käytössä ITS-aseman sisällä sen viitearkkitehtuurin yhdellä tai useammalla kerroksella.

**Turvallisuuskäytänteiden hallinta** (*Security Associations Management*) avaa tietoturvavahvistuksen kahden ITS-aseman välille. Tämän yhteyden avulla on mahdollista vaihtaa viestejä turvallisesti. Jotta kaksisuuntainen turvattu kommunikointi asemien välillä olisi mahdollista, tulisi molempien asemien käynnistää tämä palvelu. Palvelu sisältää eri toimintoja, kuten palvelun perustaminen ja päivittäminen, viestin lähettäminen ja vastaanottaminen sekä palvelun poistaminen, kun yhteys lopetetaan.

**Yksittäisten sanomien palvelua** (*Single Message Service*) käytetään turvaamaan yksittäisen sanoman lähettämistä tai vastaanottamista. Tällainen sanoma voi olla esimerkiksi CAM tai DENM. Palvelun sisältämät toiminnot ovat sanoman vahvistaminen, vahvistuksen voimaan saattaminen sanomakohtaisesti, sanoman salaaminen sekä salauksen purkaminen.

**Eheyspalvelua** (*Integrity Services*) käytetään tarkistussumman laskemiseen. Tarkistussumma sisällytetään lähtevään sanomaan. Palvelu myös vahvistaa saapuvan sanoman tarkistussumman avulla, ettei sanomaa ole muutettu matkan aikana. Palvelun toiminnot ovat tarkistussumman laskeminen, vahvistaminen ja asettaminen lähtevään viestiin.

**Toiston suojauspalvelua** (*Replay Protection Services*) käytetään varmistamaan, että sanomat on lähetetty ja vastaanotettu yhdenmukaisilla tavoilla. Tällä pyritään estämään se, ettei samoja sanomia kierrä vahingoittamassa kommunikointia. Varmistus toteutetaan asettamalla aikaleima tai järjestysnumero lähtevään sanomaan ja tarkistamalla nämä saapuvasta sanomasta. Palvelun toiminnot ovat toistolta suojaaminen perustuen aikaleimaan tai perustuen järjestysnumeroon.

**Uskottavuusvahvistus** (*Plausibility Validation*) on palvelu, jolla varmistetaan, että saapuneesta sanomasta purettu tieto on luotettava perustuen sen uskottavuuteen. Tämä toteutetaan vertaamalla sanomasta saatuja tietoja aiemmin saapuneisiin tietoihin. Verrattavia tietoja ovat esimerkiksi maantieteellinen sijainti, kellonaika sekä ajoneuvon nopeus ja suunta. Tämä palvelu ei sisällä tiedonvaihtoa ITS-järjestelmän ulkopuolisten asemien kanssa. Palvelussa on vain yksi toiminto, joka on tiedon uskottavuuden vahvistaminen.

### 5.3.2 Tietoturvan hallinnan tietoturvapalvelut

Seuraavassa kuvatut tietoturvapalvelut toimivat ITS-aseman viitearkkitehtuurin tietoturvan hallintakerroksen sisällä.

**Rekisteröintipalvelu** (*Enrolment Service*) hallitsee rekisteröinnin valtuutuksia. Tämän palvelun avulla ITS-asema saa rekisteröintiviranomaiselta tarvittavat valtuutukset. Palvelun toimitoista ovat valtuutuksien hankinta, päivittäminen sekä poistaminen.

**Oikeutuspalvelu** (*Authorization Service*) hallitsee varmennuslippuja. Rekisteröity ITS-asema saa varmennusliput käyttöönsä tämän palvelun avulla. Ne varmistavat, että asema saa tarvittavat oikeudet käyttää ITS-sovelluksia ja -palveluita. Oikeutuspalvelun toiminnot ovat varmennuslippujen hankinta, päivittäminen, julkaiseminen sekä oikeutustietojen paikallisen säilytyspaikan päivittäminen.

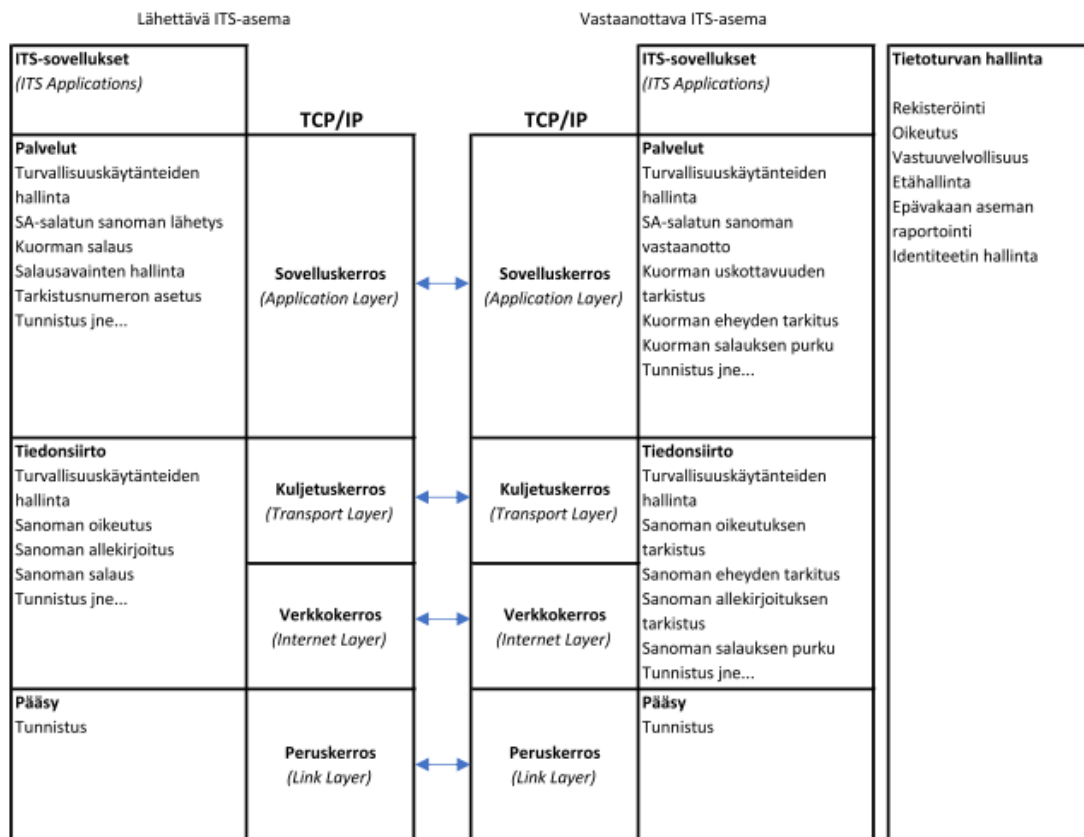
**Vastuuvollisuuspalvelu** (*Accountability Service*) tallettaa saapuvat ja lähtevät sanomat siten, että ITS-asemaa voidaan pitää vastuuvollisena. Palvelun toiminnot ovat sekä lähtevien että saapuvien sanomien tallennus vastaaviin tarkastuslokeihin.

**Etähallinta** (*Remote Management*) mahdollistaa ITS-infrastruktuurin hallinta etäältä epävakaaasti käyttäytyvää ITS-asemaa. Tämä palvelu sallii infrastruktuurin etäältä käynnistää tai kytkeä pois päältä sanomien siirron tietyille ITS-asemalle, jonka käyttäytyminen on epävakaa. Palvelun toiminnot ovat sanomien siirron käynnistäminen ja kytkeminen pois päältä.

**Raportointi epävakaaasti käyttäytyvästä ITS-asemasta** (*Report Misbehaving ITS-Station*) mahdollistaa ITS-asemien raportoida epäilyttävästä toiminnasta infrastruktuurille. Palvelun avulla ITS-asemat voivat ilmoittaa jonkin toisen ITS-aseman käyttäytyvän epävakaaasti ja epäilyttävästi. Palvelun ainoa toiminto on käyttäytymisestä raportointi.

**Identiteetin hallinta** (*Identity Management*) hallitsee sellaisia palveluita, jotka tukevat jatkuvaa tunnistaiden vaihtoa. Näitä tunnistaita ovat esimerkiksi ITS-aseman tunniste, verkon tunniste tai MAC-osoite. Palvelu hallitsee myös kommunikointiin käytettäviä valtuutuksia ITS-aseman sisällä. Toimitoista ovat esimerkiksi tunnisteen vaihtamisen käynnistäminen, lukitseminen ja lukituksen avaaminen, tunnisteen vaihtamisen ilmoitusten tilaaminen ja tilaamisen lopettaminen sekä ilmoittaminen tunnisteen vaihtamisesta.

Kuva 16, joka perustuu standardiin [28], esittää yhteenvetona käytössä olevia tietoturva-palveluita kerroksittain. Havainnollistamisen helpottamiseksi kuvaan on myös liitetty TCP/IP-viitemallin kerrokset. Kuvan vasemmassa reunassa on lähettävä ITS-asema ja oikeassa vastaanottava. Siinä on havainnollistettu eri tietoturvapalveluita, joita käytetään sekä lähettävässä että vastaanottavassa ITS-asemassa. Siniset nuolet kuvastavat tiedonvaihtoa eri kerrosten välillä. Luvussa 5.3.1 esitettyjä tietoturvapalveluita havaitaan kuvassa ITS-aseman eri kerrosten alta sekä luvussa 5.3.2 esitettyjä palveluita havaitaan tietoturvan hallintakerroksen sisältä.



**Kuva 16.** ITS-kommunikaation tietoturvapalvelut kerroksittain.

## 5.4 Uhka-, haavoittuvuus- ja riskianalyysi

Tietoturvaan ja sen mekanismeihin liittyen tärkeässä roolissa on uhka-, haavoittuvuus- ja riskianalyysi. Myös ITS-ympäristön tietoturvassa tämä on otettu huomioon, ja se on määritelty omassa standardissaan ETSI TR 102 893 (*Threat, Vulnerability and Risk Analysis* (TVRA)) [25]. Siinä keskitytään ITS-järjestelmien 5,9 GHz radiokommunikaatioon ja se käsittää V2V- ja V2I-kommunikaatiot.

Ilman järjestelmän tietoturvahkien ymmärtämistä on mahdotonta valita ja kehittää oikeanlaisia vastakeinoja uhkia kohtaan. TVRA-standardia [25] käytetään näiden uhkien tunnistamiseen ja sen apuna käytetään erityistä TVRA-metodia. Metodi koostuu 7 askeleesta:

1. Tietoturvan tavoitteiden tunnistus.
2. Tietoturvan vaatimusten tunnistus.
3. Järjestelmän ja tietovarojen inventointi.
4. Järjestelmän haavoittuvuuksien ja uhkien luokittelu.
5. Hyökkäyksen todennäköisyyden ja vaikutusten määrittely.
6. Riskien määrittely.
7. Yksityiskohtaisten vastakeinojen määrittely.

TVRA-metodin avulla standardissa käydään läpi kaikki ITS-järjestelmään kuuluvat komponentit ja elementit. Näitä ovat ITS-arkkitehtuuri, peruspalvelut (*Basic Set of Applications*, BSA) sekä ITS-kommunikaatio ja sen palvelut. Käytännössä tämä tarkoittaa sitä, että ITS-arkkitehtuurin osalta kartoitetaan asemien (ajoneuvot ja tienvarsiyksiköt) tietoturvaa, BSA-sovellusten osalta sovellus- ja ohjelmistopohjaista tietoturvaa sekä ITS-kommunikaation osalta viestintään ja siinä käytettäviin sovelluksiin liittyvää tietoturvaa.

Edellisten lisäksi standardissa kerrataan ITS-järjestelmien tietoturvatavoitteet ja -vaatimukset. Näitä ovat luottamuksellisuus, eheys, saatavuus, vastuuvollisuus ja oikeellisuus. Kaikki nämä ovat myös toiminnallisia elementtejä, joten standardissa on jokaiselle määritelty monia erilaisia toimintoja, joilla kyseinen elementti vahvistaa suorituskykyään.

Standardissa määritellään myös ITS-järjestelmien varallisuus. Tämä on jaettu ajoneuvojen ja tienvarsiyksiköiden kesken niin toiminnallisiin varoihin kuin tietovaroihin. Ajoneuvojen kohdalla toiminnallinen varallisuus tarkoittaa esimerkiksi protokollien ja palveluiden hallintaa, ITS-sovelluksien hallintaa sekä ajoneuvojärjestelmän hallintaa. Tietovarot tarkoittavat esimerkiksi paikallista dynaamista karttaa tai ajoneuvoinformaatiota. Tienvarsiyksikön kohdalla varallisuus tarkoittaa pääosin samoja asioita kuin ajoneuvojen kohdalla sillä erolla, että tietovaroissa ajoneuvoinformaation tilalla on asemainformaatio.

ITS-järjestelmien uhka-analyysi sisältää mahdollisten hyökkäyspintojen ja hyökkääjien määrittelyn niin ajoneuvoille kuin tienvarsiyksiköille. Ajoneuvojen tapauksessa määritellään muutama hyökkäysmahdollisuus. Mahdollisia hyökkääjiä voivat olla esimerkiksi toinen ajoneuvo, joka voi hyökkäyksellään aiheuttaa suunnittelemtomia toimintoja. Tässä tapauksessa käytetään hyväksi ohjelmistojen suunnitteluvirheitä. Muita hyökkäyksistä aiheutuvia haittoja ovat joutuminen hyökkäyksen välityspalvelimeksi jonkin haittaohjelman seurauksena tai väärän informaation jakaminen toisille ajoneuvoille. Samat hyökkäykset voivat olla mahdollisia myös tienvarsiyksiköltä.

Uhka-analyysissä määritellään haavoittuvuudet ja uhat viitaten tietoturvatavoitteisiin ja -vaatimukseen. Näiden lisäksi siinä määritellään kaikille ITS-asemille yleiset tietoturvauhat, joita ovat esimerkiksi saatavuuteen liittyen palvelunestohyökkäys, eheyteen liittyen manipulaatio, teeskentely, toisto sekä tiedon häviäminen ja muuttuminen. Manipulaatio ja teeskentely liittyvät tunnistuksen tietoturvauhkaan. Luottamuksellisuuteen liittyviä uhkia ovat salakuuntelu ja verkkoliikenteen analysointi.

TVRA-standardin viimeisenä asiakokonaisuutena on määritelty tietoturvauhkien, tietoturvahaavoittuvuuksien ja riskien vastakeinot (*countermeasures*). Tämä on laaja kokonaisuus, jossa on jokaiselle uhalle määritelty yksitellen eri vaihtoehtoja niiden kriittisyyden pienentämiseksi. Muutamana esimerkkinä vastakeinoista on *beacon*-viestinnän ja

muiden viestien taajuuden pienentäminen, lähteen tunnistetietojen lisääminen V2V-viesteihin tai jokaisen viestin digitaalinen allekirjoittaminen järjestelmällä, joka muistuttaa *Kerberos*- tai PKI-järjestelmiä. Kaikki vastakeinot sekä uhka-, haavoittuvuus- ja riskianalyysi ovat yksityiskohtaisesti määritelty standardissa ETSI TR 102 893 [25].

## 5.5 Yhteiset toimintamallit

Kuten jo edellä huomattiin, koostuvat tietoturvamekanismit monesta eri osa-alueesta. Yhteentoimivuuden<sup>5</sup> vuoksi – ja tietoturvan parantamisen kannalta – tärkeänä osana ovat yhteiset toimintamallit esimerkiksi tiedon siirtämiseen ITS-asemien välillä. Tähän liittyy muun muassa standardi ETSI TS 103 097 [35], joka määrittelee tietoturvan otsikkorakenteen ja sertifikaattien mallit. Nämä mallit on kehitetty erityisesti ITS-G5-kommunikaatiota varten. Otsikkorakenteella viitataan normaalin tietoliikennepaketin otsikkorakenteeseen (*header*).

Standardi määrittelee kaikki otsikkorakenteen kentät yksityiskohtaisesti. Muutamana esimerkkinä voidaan esittää joitakin kenttiä. *SecuredMessage*-kentän arvolla määritellään, miten koodataan yleinen salattu viesti. *Payload*-kentän arvolla määritellään, miten salatun viestin kuorma koodataan ja *PayloadType*-kentän arvolla määritellään, millaiset *Payload*-kentän arvot ovat sallittuja. Otsikkorakenteen kenttiä on kaikkiaan 9 ja nämä kaikki määritellään standardissa tarkemmin.

Sertifikaattien osalta standardissa määritellään esimerkiksi, miten sertifikaatit koodataan ja miten niiden otsikot koodataan. Myös otsikon tyypit määritellään eli otsikon on oltava jotain tiettyä tyyppiä, esimerkiksi valtuuslippu (*Authorization Ticket*). Sertifikaatteihin liittyviä tarkkaan määriteltyjä elementtejä on standardissa esitetty 9 kappaletta. Edellisten lisäksi standardi määrittelee tietoturvaprofiilit CAM- ja DENM-sanomille sekä muille allekirjoitetuille sanomille. Myös sertifikaateille määritellään oma tietoturvaprofiili. Nämäkin määritelmät liittyvät sanomien otsikkorakenteeseen ja siihen, mitä kenttiä ja kentän arvoja kunkin otsikkorakenteessa tulee käyttää.

ETSI TS 103 097 -standardin [35] määrittelemien käytänteiden ja algoritmien pohjalta voidaan suorittaa ITS-kommunikaation tietoturvan vaatimustenmukaisuustestausta. Tämä testausprotokolla määritellään standardissa ETSI TS 103 096, joka koostuu kolmesta eri osasta [32–34]. Ensimmäinen osa määrittelee muodolliset testauksen tiedot, jotka perustuvat ETSI TS 103 097 -standardin määrittelemille algoritmeille. Lisäksi testauksen valmistelua varten siinä esitetään valmis täytettävä lomake, johon testauksessa käytettävien laitteistojen tunnistetiedot voidaan merkata. Toisessa osassa määritellään

---

<sup>5</sup> Standardissa ETSI EG 202 798 määritellään viitekehys ITS-järjestelmien vaatimustenmukaisuus- ja yhteentoimivuustestausta varten.

testisarjan rakennetta ja testien tarkoitusta. Tämä osa on varsin kattava 147 sivun mittainen kuvaus testisarjasta. Kolmas osa määrittelee protokollien käyttöönottoon liittyvää lisätietoa.

Kun tutkitaan tarkemmin standardin ETSI TS 103 096 toista, 147 sivuista osaa [33], huomataan, että siinä määritellään tietoturvestien rakennetta. Testauksen rakenne koostuu 9 osasta. Näitä ovat ITS-aseman tiedonsiirto, ITS-aseman oikeutus- ja rekisteröintiviranomaisten käytännöt, sanomien lähettämisen käytännöt, vastaanottamisen käytännöt, yleisten sanomien käytännöt, CAM- ja DENM-sanomien käytännöt sekä sertifikaattien käytännöt. Jos siis suoritetaan V2X-kommunikoinnin tietoturvaan liittyvä testaus, voidaan se tehdä esimerkiksi mittaamalla CAM-sanoman suorituskykyä eli performanssia. CAM-sanoman profiilin koko rakenne esitetään standardissa [33], jolloin mittauksen tuloksena tulisi saada sitä vastaava rakenne. Profiiliin sisältyy 12 eri kohtaa, joiden tulisi mittaustuloksissa vastata standardin mallia.

## 5.6 C-V2X-kommunikoinnin tietoturva

Kuten aiemmin mainittiin, 3GPP-projektin *Release 13* on julkaistu vuonna 2015. Se määrittelee LTE-teknologioita V2X-kommunikointia varten. Tässä on jälleen yksi esimerkki, jossa tietoturva-asioita on ajateltu ja kehitetty jälkikäteen. Todisteena tästä on 3GPP-projektin ja ETSI-järjestön yhteisesti tuotettu standardi ETSI TS 133 185 [37], joka määrittelee tietoturvanäkökulmia LTE-pohjaiseen V2X-kommunikointiin. Todiste jälkikäteen kehityksestä on se, että standardi on julkaistu vasta heinäkuussa 2017. Sen otsikon mukaan siihen on jätetty myös jonkinlainen optio tulevalle 5G-verkkoteknologialle, sillä termi 5G on mainittu niin otsikossa kuin avainsanoissa, mutta ei missään muualla myöhemmin standardissa.

Standardi on todennäköisesti myös tuotettu melko nopealla aikataululla, sillä siihen on jäänyt joitakin selkeitä asia- tai kirjoitusvirheitä. Muuten standardissa ensin kerrataan V2X-kommunikaation yleiset arkkitehtuuriseikat sekä tietoturvan vaatimukset. Sen jälkeen siinä määritellään ratkaisuja V2X-tietoturvaseikkoihin, painottuen LTE-teknologioihin.

Kyseinen standardi [37] on suurilta osin listaus, johon on kerätty useita eri 3GPP- ja muitakin standardeja, joiden ratkaisuilla turvataan V2X-kommunikaatiota. Listattuja standardeja ovat esimerkiksi 3G-teknologioiden IP-kerroksen tietoturvan määrittelevä 3GPP TS 33.210 sekä tunnistuksen määrittelevä 3GPP TS 33.310. Standardin [37] mukaan V2X-sovellusten informaatiota voidaan viestittää sekä PC5- että Uu-rajapintojen kautta. Molempien rajapintojen tulisi toteuttaa sovellustason tietoturva kuten on määritelty ITS-G5-standardeissa.

Yksityisyysasioihin liittyen standardissa mainitaan, että PC5-rajapinnan tulisi toteuttaa samankaltaista yksityisyyttä kuin ITS-G5-standardeissakin, mutta Uu-rajapinnan kohdalla mainitaan, että erityisiä yksityisyystoimintoja ei ole tuettu. Standardista ei selviä, onko tämä kyseinen seikka tarkoitus jäädä tällaiseen pisteeseen vai onko siihen tarkoitus kehittää joitakin ratkaisuja.

## 5.7 Yhteenveto tietoturvamekanismeista

Kuten jo aiemmin muutamaan otteeseen mainittiin, tietoturvaan liittyvät asiat ovat tulleet esille ITS-järjestelmien teknologiseen kehitykseen verrattuna hieman jälkikäteen. Tästä on vain yhtenä esimerkkinä varmennepolitiikka, joka on hyväksytty käyttöön vasta 14.6.2017.

ITS-ympäristön tietoturvan standardeista huomataan, että sosiaalis- ja teknishallinnollinen sekä informaatiollinen tietoturva on melko hyvällä tasolla määritelty. Näiden pohjalta esitettyyn tietoturvan hallintaan kuuluvat niin tunnistus-, rekisteröinti- kuin oikeutuskäytännöt sekä esimerkiksi tietoturvapalvelut ja luottamuksellisuusasiat.

Kuitenkaan fyysistä tietoturvaa ei määritellä ITS-G5-standardeissa missään muodossa, joten on oletettava, että siihen liittyvät seikat tulisi olla samalla tasolla kuin missä tahansa muussakin käyttötilanteessa. Esimerkiksi, jos rekisteröintiviranomaisen palvelinsaliin syttyy tulipalo, sen varalta tulisi kaikki varmuuskopiot olla turvallisessa paikassa. Ja ennen tulipaloa, tulisi olla käytäntö varmuuskopioiden tallettamiseen turvalliseen paikkaan.

ITS-G5-standardeissa ei ole erikseen määritelty toimintoja palomuurin eikä tunkeutumisen eston osalta. Myöskään laitteiston tietoturvamoduulia ei ole niissä määritelty. On siis oletettava, että näissä järjestelmissä on käytössä kaikki samat mekanismit ja toimintatavat kuin muissakin niiden käyttötapauksissa.

V2X-kommunikaation tietoturvan mittauksia varten on määritelty testirakenne. Tämän avulla voidaan mitata esimerkiksi CAM-sanoman suorituskykyä. Kuitenkin kyseinen testirakenne liittyy ainoastaan ajoneuvojen ja tienvarsiyksiköiden väliseen kommunikointiin eikä se ota kantaa kokonaisvaltaiseen tietoturvan testaamiseen. Tällaiseen toimintaan ei ole määritelty yhtenäisiä toimintamalleja. Kokonaisvaltaiseen tietoturvan testaamiseen voisi kuulua esimerkiksi eettistä hakkerointia tai penetraatiotestausta verkon eri komponentteja kohtaan.

C-V2X-tietoturvan kehitystyö on vielä keskeneräistä varsinkin yksityisyysasioihin liittyen. Muutenkin tulevaa 5G-verkkoteknologiaa ajatellen olisi jo nyt hyvä aloittaa tietoturva-asioiden suunnittelu ja kehitystyö, jotta niissäkin päästäisiin samalle aikajanelle muun teknologisen kehitystyön kanssa.

## 6. V2X-KOMMUNIKAATION JA -TIETOTURVAN TESTAUS

Erilaisten tietoturvamekanismien tarkastelun jälkeen voidaan tarkastella muutamia käytännön asioita. Tässä luvussa perehdytään V2X-kommunikaatioon ja sen tietoturvaan liittyviin testauksiin ja tutkimuksiin. Niihin liittyen tätä työtä varten asennettiin V2X-kommunikaation simulointiympäristö, jossa ajettiin perussimulaatio. Sen jälkeen tarkastellaan muiden tekemiä testauksia sekä esitetään omia pohdintoja. Ensin kuitenkin muutamia yleisiä asioita testauksiin liittyen.

### 6.1 Yleistä testauksesta

Kuten myöhemmin tullaan huomaamaan, on V2X-kommunikaation tietoturvaan liittyviä testauksia tehty usein simulointiympäristössä. Siksi tässäkin diplomityössä tutustutaan yhteen simulointiympäristöön hieman tarkemmin. Tärkeää olisi myös todeta ja testata tietoturvamekanismien toimintaa oikeassa kommunikointiympäristössä ja käytännössä. Kuitenkaan tätä diplomityötä varten tehdyissä taustatutkimuksissa ei onnistuttu löytämään yhtään oikean kommunikointiympäristön tietoturvatutkimusta. Toisaalta myöskään tätä työtä varten ei ollut mahdollista päästä itse suorittamaan oikean ympäristön testauksia useista yrityksistä huolimatta. Tämäkin osaltaan kertoo siitä, että tietoturva ei ole vielä tärkeimpänä asiana V2X-ympäristössä.

Miksi tietoturvan testaaminen olisi tärkeää oikeassa V2X-ympäristössä? Ainakin siksi, että simulointiympäristössä on helppoa jättää joitakin asetuksia huomioimatta. Kun jokin asia katsotaan tarpeettomaksi, sitä ei tarvitse ottaa huomioon. Tällöin se on helppoa jättää koodauksen ulkopuolelle ja pois testistä. Tämä saattaa kuitenkin vaikuttaa suuresti myöhempiin tuloksiin.

Testaaminen olisi tärkeää myös siksi, että käyttöön saataisiin kehitettyä jokin testauksen yhtenäinen toimintamalli. Tällöin testaaminen olisi helpompaa, kun kaikilla olisi samat toimintatavat eikä jokaisen tarvitsisi miettiä asioita alusta saakka. Hyvä alku on jo edellä mainittu vaatimustenmukaisuus- ja yhteentoimivuustestaus.

Kuitenkin ehkäpä tärkeimpänä syynä, miksi tietoturvaa pitäisi testata käytännössä, on simulointiympäristön eroavaisuudet oikeaan ympäristöön verrattuna. Tämä tarkoittaa, että simulointiympäristö on aina hallittu ympäristö, jossa olosuhteet tunnetaan ja tiedetään. Oikeassa ympäristössä näin ei aina välttämättä ole, esimerkiksi ruuhkatilanteet voivat muuttua yllättäen. V2X-kommunikoinnin signaalien kantoaallot voivat vaihdella merkittävästi oikeassa ympäristössä, sillä vaihteluun vaikuttaa rakennuksista ja muista korkeista esteistä aiheutuvat kantoaallon vaimentumiset ja kuolleet pisteet. Myös sade vaimentaa

signaalia. Signaalilla on monia muitakin ominaisuuksia, kuten esimerkiksi monitie-etenemä, sironta, heijastuminen, taittuminen, viive ja taipuminen. Näitä ei pystytä esittämään simulointiympäristössä luotettavasti, sillä se perustuu kaksiulotteiseen mallinnukseen, kun taas oikea ympäristö on aina kolmiulotteinen.

## 6.2 V2X-kommunikaation simulointiympäristö

Avoimen lähdekoodin simulointiympäristöjä, joilla voidaan helposti ja edullisesti (ilmaiseksi) simuloida V2X-kommunikaatiota, on olemassa useita. Eräs esimerkki näistä on Berliinin yliopiston ylläpitämä *The V2X Simulation Runtime Infrastructure* (VSimRTI) [47], jolla voidaan simuloida esimerkiksi C-ITS-strategian mukaisia ratkaisuja yksityiskohtaisesti. Toinen esimerkki on *Vehicles in Network Simulation* (VeINS) -simulointiympäristö [46], johon tutustutaan tarkemmin seuraavien lukujen myötä.

Saatavilla on myös sellaisia simulointiympäristöjä, jotka eivät perustu avoimeen lähdekoodiin. Eräs tällainen on *Spirent V2X Emulator* [45], joka tarjoaa niin laboratoriotestausta, simulointiympäristöä kuin kenttätestaustakin. Tämä ympäristö tukee myös V2X-tietoturvan testausta.

Tätä diplomityötä varten tehdyissä testauksissa haluttiin kustannukset pitää minimitasolla, joten testausalusta valittiin avoimen lähdekoodin vaihtoehdoista. Valinta kohdistui VeINS-simulointiympäristöön, joka perustuu kolmen eri sovelluksen yhteistoimintaan. Näistä sovelluksista, niiden asennuksesta sekä niillä simuloinnista on kerrottu seuraavissa luvuissa.

### 6.2.1 VeINS-simulointiympäristön sovellukset

VeINS-simulointiympäristön toiminta perustuu kolmeen sovellukseen ja niiden yhteistoimintaan. Sovellukset toimivat verkkosimulaattorina, liikennesimulaattorina ja ajoneuvosimulaattorina.

*Objective Module Network Testbed in C++* (OMNeT++) -sovellus [41] on avoimen lähdekoodin käyttöliittymä, jolla voidaan kirjoittaa simulaatioita. Sillä kirjoitetaan simulaation verkkoympäristö ja lähdekoodi. Käyttöliittymä on Eclipse-pohjainen, joten yhdenäköisyys ja toimintojen samankaltaisuus sovellusten välillä on suuri. OMNeT++-sovellukseen on kuitenkin lisätty uusia toimintoja. Siinä simulaatiot kirjoitetaan pääosin kolmen eri tiedoston avulla. *Network Description* (ned) -tiedoston avulla mallinnetaan verkko ja sen komponentit ja yhteydet. Ne voidaan mallintaa joko suoraan koodia kirjoittamalla tai käyttämällä graafista ympäristöä, jossa verkkoympäristö voidaan rakentaa erityisillä graafisilla moduuleilla. Tämä vaihtoehto muistuttaa etäisesti LEGO-palikoilla rakentamista. Kumpaa tahansa moodia käyttääkin koodin muokkaamiseen, näkyvät muutokset välittömästi myös toisessa moodissa. Toinen tiedosto on lähdekooditiedosto, jolla luodaan verkossa tapahtuvat toiminnot käyttäen C++-kieltä. Tämä luonnollisesti vaatii

jonkin verran C++-kielen tuntemista. Kolmas tiedosto on *Initialization File* (ini), jolla simulaatiomalli konfiguroidaan ajoa varten.

*Simulation of Urban MObility* (SUMO) -sovellus [42] on avoimen lähdekoodin tieliikenteen simulaatiopaketti, joka on suunniteltu käsittelemään laajoja tieverkkoja. SUMO-sovellus toteuttaa ajoneuvojen liikennevirran karttapohjalle. Karttoja voi ladata olemassa olevista kartoista, joten sovelluksessa voi itse tehdä liikennesimulaation mihin tahansa kaupunkiin tai kaupungin ulkopuolelle.

*Vehicles in Network Simulation* (VeINS) -sovellus on avoimen lähdekoodin viitekehys (*framework*), joka tuodaan ja otetaan käyttöön omana projektina OMNeT++-sovelluksessa. Se on valmiiksi kirjoitettu ajoneuvoverkkojen simulaatio, joka perustuu OMNeT++- ja SUMO-simulaattoreihin. Käytännössä näiden kolmen eri sovelluksen ideana on, että OMNeT++ toimii tapauskohtaisena verkkosimulaattorina, SUMO tieliikenteen simulaattorina sekä VeINS ajoneuvojen verkkosimulaattorina.

## 6.2.2 VeINS-simulointiympäristön asennus

VeINS-simulointiympäristön asennus oli noin yhden työpäivän kestävä prosessi. Siinä ensin ladattiin SUMO-sovellus zip-pakettina, joka purettiin ennalta määriteltyyn tiedostopolkuun. Tämä oli erittäin suoraviivainen prosessi eikä sisältänyt mitään erikoisia työvaiheita. Asennuksia varten valittiin työkansiksi polku `C:\temp\veins\src`, johon myös kaikki tulevat asennukset tehtiin.

Toiseksi ladattiin OMNeT++ 5 -sovellus zip-pakettina, joka purettiin samaan tiedostopolkuun kuin SUMO-paketin tiedostot. OMNeT++-paketin purun jälkeen voitiin avata sovelluksen tiedostoista löytyvä MinGW-komentoriviohjelma, jonka käyttö muistutti hieman Linux-ympäristön terminaalien käyttöä. Komentoriville syötettiin `./configure`-komento, jolla OMNeT++ 5 -sovelluksen kokoaminen valmisteltiin, ja sen jälkeen `make`-komento, joka aloitti simulointiympäristön kokoamisprosessin. Tähän kuului esimerkiksi kaikkien simuloinnissa tarvittavien kirjastokomponenttien kokoaminen. Näiden vaiheiden suorittamiseen kului aikaa hieman yli tunti, jonka jälkeen sovellus oli valmis käyttöä varten. Antamalla `omnetpp`-komento MinGW-komentoriville voitiin avata Eclipse-pohjainen OMNeT++ 5 -käyttöliittymä.

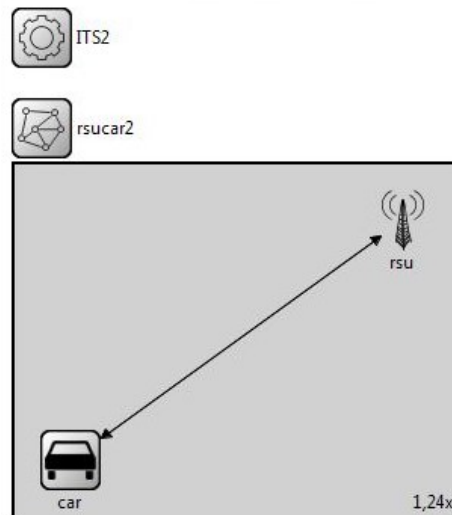
Simulointiympäristöä asennettaessa kannattaa myös ottaa huomioon, että tietokoneessa käytössä oleva virustorjuntaohjelmisto saattaa estää edellisten komentojen suorittamia toimintoja, kuten esimerkiksi projektien yhteydessä tarvittavien kirjastojen luonnin, joten tilanteen niin vaatiessa kannattaa väliaikaisesti sammuttaa suojaustoiminnot. Jos simulointiympäristöä käyttää Windows-käyttöjärjestelmässä, täytyy myös SUMO-sovelluksen antaa läpäistä Windowsin palomuuuri.

Asennuksen kolmantena vaiheena ladattiin VeINS 4.6 -sovellus zip-pakettina, joka myös purettiin samaan tiedostopolkuun edellisten kanssa. Lataus ja purku olivat suoraviivaiset prosessit ilman erikoisia työvaiheita. Kun purku valmistui, voitiin VeINS-projekti tuoda OMNeT++-sovelluksen käyttöliittymän kautta valitsemalla *File*-valikosta *Import*-komento. Tämän jälkeen piti vielä *Project*-valikosta valita ja ajaa *Build All* -komento.

Viimeisenä vaiheena SUMO-sovellus otettiin mukaan VeINS-projektiin. Käytännössä tämä tapahtui OMNeT++-käyttöliittymässä käynnistämällä SUMO-projektitiedosto, joka oli VeINS-projektin sisällä. Tässä vaiheessa siis kaikki kolme sovellusta, SUMO, VeINS 4.6 ja OMNeT ++ 5, toimivat rinnakkain ja niiden yhteistoiminta toteutti V2X-kommunikoinnin simulointiympäristön.

### 6.2.3 V2X-kommunikoinnin simulointi

Jotta kommunikoinnin simulointi voidaan aloittaa, tarvitaan ensin kaksi tai useampi toistensa kanssa kommunikoiva verkkokomponentti. Komponenttien ja verkkoympäristön koodiin ja ohjelmointiin tutustumisen yhteydessä koodattiin yksinkertainen perusesimerkki, jossa on tienvarsiyksikkö ja auto, ja ne kommunikoivat keskenään. Molemmat komponentit koodattiin ned-kielellä, jolla myös niiden kommunikointiportit luotiin. Tämä esimerkki koodista on esitetty liitteessä A. Kuva 17 esittää ned-kielellä koodattujen komponenttien graafisen version, jossa ITS2 viittaa verkkokomponenttiin ja rsucar2 verkkoon. Komponenttien välillä tapahtuva kommunikointi luotiin erillisellä lähdekoodilla, joka kirjoitettiin C++-kielellä. Tämä lähdekoodi on esitetty liitteessä B.

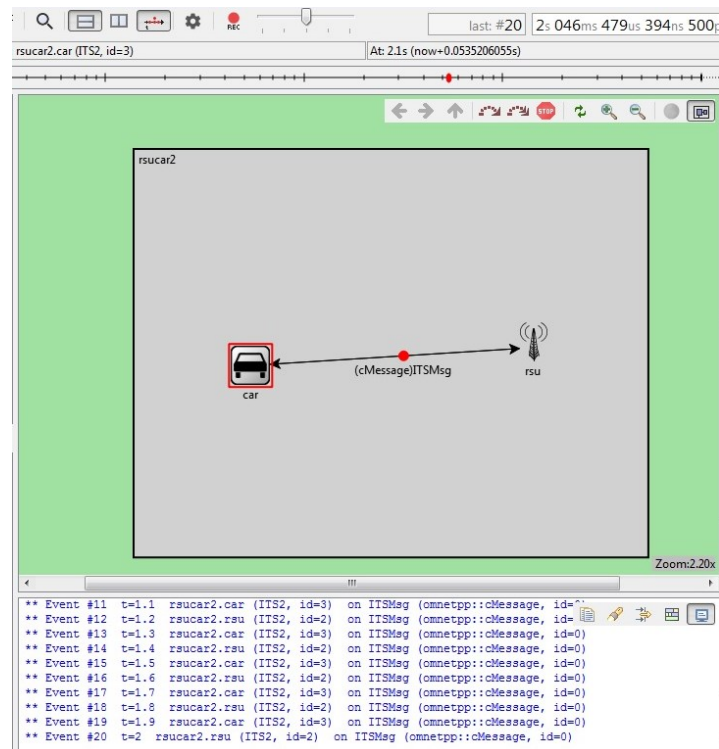


**Kuva 17.** Esimerkki peruskommunikaation graafisesta verkkoympäristöstä.

Verkkoympäristön ja lähdekoodin kirjoittamisen jälkeen piti kirjoittaa vielä ini-tiedosto, jolla simulaatiossa käytettävä verkkoympäristö konfiguroitiin:

```
# omnetpp.ini-tiedosto
[Config rsucar2]
network = rsucar2
# tallennetaan kommunikaatiotapahtumat lokitiedostoon:
record-eventlog = true
```

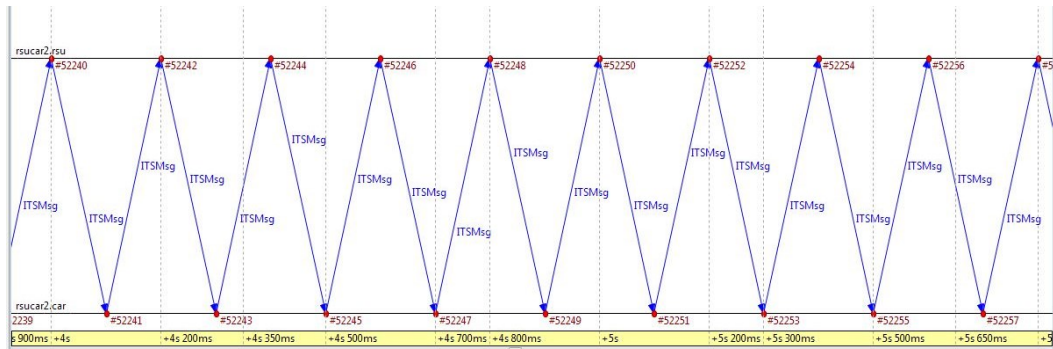
Simulointi aloitettiin valitsemalla ini-tiedoston alta komento *Run as OMNeT++ simulation*, jolloin uuteen ikkunaan avautui valmis simulointiympäristö. Sen työkaluilla simulaatiota voitiin vapaasti ajaa ja pysäyttää. Ajaminen onnistui myös nopeutettuna. Kuva 18 esittää otteen ikkunasta, jossa simulaatio ajettiin. Sen yläreunassa oikealla näkyy aikaruutu, joka ilmaisee simulaation ajan, ei reaaliaikaa. Alareunassa näkyy juokseva kommunikaatiotapahtumien konsoli.



**Kuva 18.** Peruskommunikoinnin esimerkksimulaatio.

Kun ini-tiedoston konfiguraatiossa asetettiin kommunikaatiotapahtumien tallennus päälle, kaikki tapahtumat tallennettiin lokitiedostoon. Sitä voitiin tarkkailla esimerkiksi graafisessa muodossa simulaation päätyttyä. Kuva 19 esittää tapahtumien tallennuksesta graafisen muodon, joka on hyvin yksinkertainen solmulta solmulle etenevä päättymätön kommunikaatiotapahtuma tasaisin väliajoin.

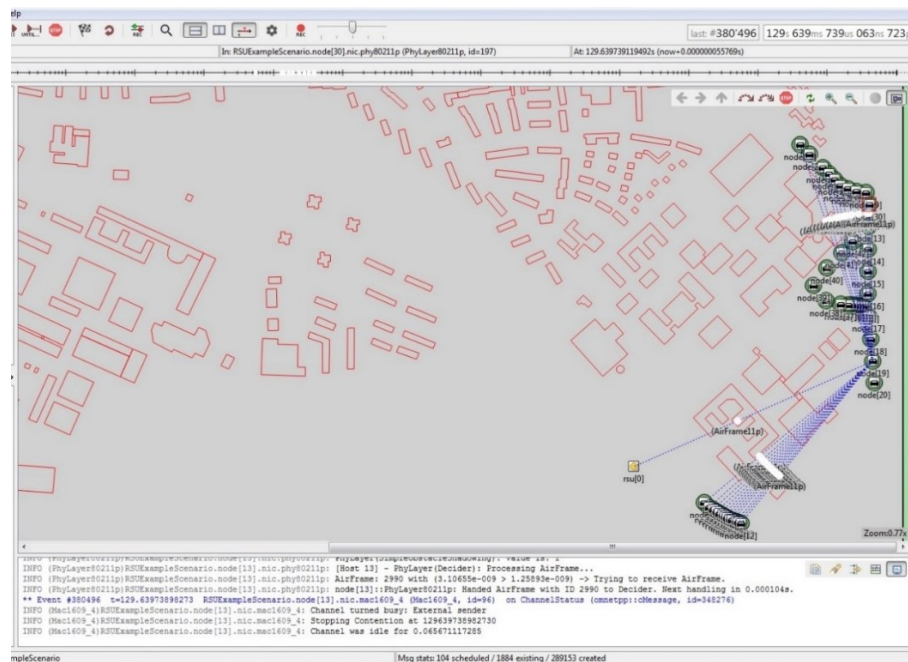
Tämän perusesimerkin ohjelmoinnin jälkeen oli helpompi siirtyä testaamaan VeINS 4.6 -projektin mukana tullutta simulointiympäristöä. Se on ympäristö, jossa myös SUMO-sovellus on mukana toteuttamassa ajoneuvojen liikennevirtaa. VeINS-projektiin



**Kuva 19.** Peruskommunikoinnin simulaation tapahtumat graafisessa muodossa.

oli mahdollista ladata github.com-sivustolta koodiarkisto, joka toteuttaa simulointiympäristöön ITS-G5-standardien mukaisen V2X-kommunikoinnin. Ladattavissa olisi ollut myös LTE-teknologioihin perustuvan kommunikoinnin koodiarkisto.

Kuva 20 esittää tilanteen, jossa VeINS-projektin simulointiympäristön testitiedosto ajettiin. Siinä näkyy harmaalla pohjalla oleva kaupunkiympäristö, joka on saksalaisen kaupungin Erlangen karttapohja. Siinä kaikki rakennukset on esitetty punaisella ja oikealla näkyy kommunikoivia asemia, jotka ovat autoja yhtä lukuun ottamatta. Tämän yhden aseman nimi on rsu[0], joka viittaa tienvarsiyksikköön ja se on esitetty keltaisella värillä. Se lähettää ja vastaanottaa sanomia kaikilta lähistön asemilta sekä myös autot lähettävät toisilleen sanomia. Tämä on esitetty valkoisilla pallοilla, jotka viittaavat lähetettyihin sanomiin. Siniset viivat edustavat sanomien kulkureittejä.



**Kuva 20.** VeINS-projektin mukainen simulointiympäristö.

Tähän testisimulaatioon oli ohjelmoitu tilanne, jossa ensin oli normaalia autoliikennettä Erlangenin teknillisen yliopiston ympäristössä. Simulaation edetessä tapahtui liikenneonnettomuus, josta lähetettiin tapahtumasanoma kaikille asemille. Tämän jälkeen asemat valitsivat toisen reitin, jolla kierrettiin onnettomuuspaikka.

### 6.3 Tietoturvan testauksista

Jotta V2X-tietoturvan testien vertailu keskenään onnistuisi laadukkaasti, tulisi testien suorituksessa olla käytössä joitakin yhtäläisiä ominaisuuksia. Tätä diplomityötä varten tehdyissä tutkimuksissa saatiin selville, että V2X-tietoturvaa on testattu jonkin verran, mutta näiden testien lähtökohdat, parametrit, suoritustavat sekä tulokset poikkeavat toisistaan siinä määrin, että niiden vertailu keskenään ei olisi järkevää. Tämän seurauksena tässä diplomityössä keskitytäänkin tarkastelemaan erilaisia testauksia, joita on suoritettu V2X-tietoturvan ympärillä. Tosin, ainakin tämän diplomityön tutkimuksissa selvisi myös, että tietoturvan kokonaisvaltaiseen testaamiseen ei ole olemassa mitään yhteneväisiä toimintamalleja, joilla testejä suoritettaisiin.

Samoilla linjoilla ovat myös Bayer *et al.* tutkimuksessaan [1], jossa käydään läpi modernien ajoneuvojen tietoturva-asioita. He mainitsevat, että ajoneuvojen verkkoympäristöön liittyen ei ole systemaattista tietoturvatestausta verrattuna esimerkiksi liikenneturvallisuuksikomponentteihin, joita aina testataan systemaattisesti. Heidän mukaan yksi tärkeimpiä suojattavia kohteita olisi autojen IT-pohjaiset sovellukset ja niihin liittyvät komponentit, joita modernissa autossa on jopa satoja. Yksi esimerkki heidän mukaan suojauksen puuttumisesta on, että haittaohjelman avulla voitaisiin auton jarrujärjestelmä tehdä toimintakyvyttömäksi, jolloin autosta luonnollisesti tulisi erittäin vaarallinen liikenteessä. Toinen esimerkki on auton järjestelmiin ja niiden ulkoisiin liityntäportteihin (esimerkiksi USB, Ethernet ja CAN (*Controller Area Network*) -väylä) kohdistuva penetraatiotestaus, jonka avulla saataisiin informaatiota auton toiminnoista. He toteavatkin, että tietoturva tulisi ottaa osaksi ajoneuvojen suunnitteluprosessia.

Moderneissa autoissa IT-pohjaisia sovelluksia ja mikroprosessoreita on myös Ray *et al.* tutkimuksen [12] mukaan satoja. Heidänkin mukaan autot ovat verkottuneita useiden eri pisteiden kautta ja ne sisältävät useiden satojen megatavujen edestä ohjelmistoja. Tulevaisuudessa autot tulevat olemaan samassa verkkoympäristössä kokonaisten älykaupunkien kanssa. Näiden seurauksena he toteavatkin, että tietoturva on perustavanlaatuisen ongelma autojärjestelmien suunnittelussa. Autojärjestelmien tietoturvaseikat ovat haastavia erityisesti kahdesta syystä: uhkien lieventäminen reaaliaikaisesti sekä tietoturvaominaisuuksien muunneltavuus ja venyvyys.

Ben Brahim *et al.* suorittama tutkimus [2] liittyy yhteistoiminnallisen tietoisuuden (*Cooperative Awareness*) tietoturvan suorituskykyyn tiheissä urbaanialueiden ajoneuvo-verkoissa. Tämä tutkimus on suoritettu simulointiympäristössä ja siinä ei ole huomioitu ITS-G5-tietoturvan osalta DCC-ruuhkanhallintamenetelmiä. Heidän tutkimuksessa on

myös käytetty SUMO-simulaattoria liikenteen simulointiin. Tiheällä verkolla he tarkoittavat tilannetta, jossa on 200 ajoneuvoa neliökilometrillä. Heidän mukaan CAM-sanoman viive kasvaa suhteessa verkon tiheyteen – mitä tiheämpi verkko, sitä suurempi viive. Heidän tutkimuksen tulosten mukaan tiheän verkon tapauksessa CAM-sanoman viive on jopa 500 ms.

Myös Lobach *et al.* ovat tutkimuksessaan [7] testanneet kommunikaation tietoturvaa simulointiympäristössä. He ovat kehittäneet Agez-nimisen tietoturvasimulaattorin, jolla voidaan testata esimerkiksi sanomien salausta ja salauksen purkua sekä allekirjoitusta ja varmennusta. He ovat käyttäneet sitä VSimRTI-simulaattorin yhteydessä. Heidän tekemän testin mukaan, jos kaikki lähetettävät sanomat allekirjoitettaisiin ja varmennettaisiin, se pidentäisi prosessointiaikaa 34 kertaa. Prosessointiajan pidennyksen he saivat kuitenkin pienennettyä 9 %:iin useita eri asetuksia muuttamalla.

Kaikki edellä kuvatut tutkimukset liittyvät simulointiympäristöön. Tällaisia tutkimuksia löytyy monia muitakin sillä erolla, että niissä on käytetty eri simulointiympäristöjä. Lisäksi niissä on erilaisia ominaisuuksia jätetty huomioimatta, joten ne saattavat vaikuttaa tutkimusten tuloksiin ja niiden eroavaisuuksiin. Tämän diplomityön tutkimuksissa ei onnistuttu löytämään oikeassa kommunikointiympäristössä tehtyjä tutkimuksia, mittauksia tai testauksia.

## 7. YHTEENVETO

Tässä diplomityössä tarkasteltiin älykkäitä kuljetusjärjestelmiä (ITS) kokonaisuutena historiasta tulevaisuudennäkymiin, viranomaisten määritelmiä ja standardeja, joihin älykkäät kuljetusjärjestelmät pitkälti pohjautuvat, sekä autonomisten ajoneuvojen *Vehicle-to-Everything* (V2X) -verkkoympäristöä. Yleistasolla tarkasteltiin myös oikeaa V2X-kommunikaation testausympäristöä, joka on Tampereelle rakennettu UrbanAutoTest. Näiden yleismallisten kuvausten jälkeen tarkasteltiin isompana kokonaisuutena tietoturvamekanismeja, joita ajoneuvojen verkkoympäristössä käytetään, sekä ajoneuvojen välisen kommunikaation ja sen tietoturvan testausta tutkimusten ja simuloinnin pohjalta. Työssä esitettiin myös joitakin huomioita liittyen uudempaan *Cellular V2X* (C-V2X) -ajoneuvo-kommunikaatioon ja sen tietoturvaan.

Standardit, joita tässä työssä tarkasteltiin, ovat käytössä Euroopan alueella ja niistä käytetään yhteisnimitystä ITS-G5. Niistä huomattiin, että ITS-ympäristössä käytettävä asemien viitearkkitehtuuri vastaa pohjimmiltaan tietoliikennetekniikassa yleisesti käytettävää TCP/IP-viitemallia. Standardeihin on lisätty joitakin palveluita, sovelluksia, hallintaja tietoturvaelementtejä, jotka ovat käytössä vain ITS-ympäristössä. Näistä elementeistä tietoturvaan liittyviä asioita tarkasteltiin laajemmin tässä diplomityössä.

Tietoturvan hallintaan liittyen todettiin, että sen tehtävät ja ominaisuudet on ITS-G5-standardeissa määritelty hyvin. Määriteltyjä asioita ovat esimerkiksi luottamuksen ja yksityisyyden hallinta, pääsynvalvonta, identiteetin hallinta ja luottamuksellisuus sekä monia tietoturvapalveluita. Myös uhka-, haavoittuvuus- ja riskianalyysi sekä yhteisiä joitakin toimintamalleja on määritelty. Kuitenkin tarkentavat määritelmät puuttuvat fyysisen tietoturvan, palomuurin, tunkeutumisen eston sekä laitteistojen tietoturvan osilta. Työssä todettiin myös, että C-V2X-kommunikaation tietoturva-asioissa on vielä paljon aukkoja, esimerkiksi ajoneuvojen ja verkon välisen kommunikaation toteuttavan Uu-rajapinnan yksityisyysasiat.

V2X-kommunikaatiota tarkasteltiin simulointiympäristön kautta ja samalla tutustuttiin yhteen avoimeen lähdekoodiin perustuvaan simulointiympäristöön laajemmin. Siinä tutustuttiin simulaation ohjelmointiin yleistasolla sekä ajettiin V2X-kommunikaation esimerkkisimulaatio.

Tätä diplomityötä varten tehtyjen tutkimusten perusteella voidaan todeta, että yhdessäkään simulointiympäristössä ei ole valmiina mitään tietoturvan simulointiin vaadittavia komponentteja tai moduuleita. Jos simulointiympäristöissä haluaa testata tietoturvaan liittyviä toimintoja, tulee niitä varten tarvittavat moduulit ohjelmoida itse. Varsinkin avoimeen lähdekoodiin perustuvissa ympäristöissä moduuleita voi ohjelmoida itse, jolloin

tarvitaan eri kielten ohjelmointitaitoja. Uusien tietoturvamoduulien ohjelmointi kuitenkin rajattiin tämän diplomityön aihealueen ulkopuolelle.

Etuna joissakin simulointiympäristöissä on, että ne perustuvat avoimeen lähdekoodiin. Tällöin ne ovat vapaasti muokattavissa juuri sellaisiksi kuin itse tarvitsee tai haluaa. Toki näissä tapauksissa täytyy osata jonkin verran ohjelmointia eri kielillä, sillä kaikkia moduuleita – varsinkaan tietoturvaan liittyviä – ei löydy valmiina. Toisaalta simulointiympäristöjen haittapuolena on sen hallinnan ja käyttäytymisen ennustettavuus sekä joidenkin ominaisuuksien puute verrattuna oikeaan ympäristöön. Näitä ovat esimerkiksi sääolosuhteiden ja rakennusten korkeuserojen vaikutukset kommunikaation signaaliin.

Samassa yhteydessä tarkasteltiin joitakin tietoturvan tutkimuksia. Näistä havaittiin, että tutkimuksia on tehty ainoastaan simulointiympäristössä eikä oikean ympäristön tietoturvaan liittyviä tutkimuksia ollut mahdollista löytää. Toisaalta myöskään tätä diplomityötä varten ei ollut mahdollista päästä itse suorittamaan tietoturvan tutkimuksia, mittauksia eikä testauksia oikeaan ympäristöön useista yrityksistä huolimatta. Tästä todettiin, että tietoturva ei ole vielä tärkeimpänä asiana V2X-kommunikaation testausympäristöissä, esimerkiksi Tampereella. Kuitenkin testausympäristössä olisi hyvä ottaa huomioon myös tietoturva-asiat, jotta ne eivät tule ongelmaksi myöhemmässä vaiheessa, kun lopullinen ympäristö otetaan käyttöön. Testaamisen yhteydessä tapahtuvat virheet on helpompi havaita ja korjata kuin lopullisen ympäristön yhteydessä.

Ajoneuvoympäristöön liittyen tietoturvassa on useita lähestymistapoja. Esimerkiksi hyökkäys ajoneuvon IT-pohjaisia sovelluksia vastaan, jolloin on mahdollista pysäyttää jonkin kriittisen komponentin toiminta, kuten jarrujärjestelmän. Täten ajoneuvosta saataisiin liikenteessä erittäin vaarallinen muita tielläliikkujia kohtaan. Toinen esimerkki on hyökkäys, jolla saataisiin ajoneuvon tietojen pohjalta sen omistajan henkilötietoja selville. Tämä voisi johtaa esimerkiksi identiteettivarkauksiin. Kolmas esimerkki on ajoneuvon identiteetin muuttaminen jonkin hyökkäyksen avulla. Tässä tapauksessa minkä tahansa ajoneuvon identiteetti voitaisiin muuttaa vastaamaan esimerkiksi virkavallan ajoneuvon identiteettiä, kuten poliisiautoa. Tällöin hyökkääjä saisi omalle ajoneuvolle virkavallan oikeuksia vastaavat oikeudet. Lisäksi vaarana ovat hajautetut palvelunestohyökkäykset verkon tukiasemaa tai jotain muuta komponenttia kohtaan. Tällä voisi olla mahdollista lamaannuttaa kaikki toiminta verkon kyseisen osan alueella. Sen seurauksena olisi koko liikenteen pysähtyminen kyseisellä alueella hyökkäyksen keston ajaksi.

Vaikka tässä diplomityössä tarkasteltiin monenlaisia seikkoja tietoturvaan ja uuhiin liittyen, oli se vain pintaraapaisu kyseiseen aihealueeseen. Tietoturvassa on paljon huomioitavia ja testattavia seikkoja ennen kuin voidaan täysipainoisesti ottaa käyttöön täysin autonominen ajaminen. Ennen sitä tulisi tietoturvan suorituskykyä testata ja mitata oikeassa kommunikointiympäristössä, jossa ei voida jättää erilaisia ominaisuuksia ja asetuksia huomioimatta simulointiympäristön tapaan. Lisäksi saataisiin kommunikaation signaali

käyttäytymään luonnollisessa ympäristössä esimerkiksi rankkasateen aikana sekä korkeiden rakennusten seinistä heijastellen ja taittuen.

Yleisenä yhteenvedona ajoneuvojen verkkoympäristön tietoturva-asioista todettiin, että ne ovat tulleet esille jälkikäteen muuhun teknologiseen kehitykseen verrattuna. Tästä esitettiin muutamia esimerkkejä, kuten vasta kesäkuussa 2017 hyväksytty varmennepoliitikka sekä heinäkuussa 2017 julkaistut C-V2X-kommunikaatioon liittyvät tietoturvanäkökulmat. Jotta tietoturva-asiat saataisiin ajan tasalle ja samalle tasolle muiden teknologisten kehitystöiden kanssa, tulisi niitä varten kehittää esimerkiksi yhteneväisiä toimintamalleja kokonaisvaltaisen tietoturvan testaamiseen. Kun kaikilla olisi käytössä yhteneväiset toimintamallit, olisi testaaminen helpompaa ja näin ollen testien tuloksia voitaisiin soveltaa myös esimerkiksi ajoneuvojen suunnitteluprosesseissa.

Tässä diplomityössä saatiin onnistuneesti näkyviin tiettyjä puutteellisuuksia sekä kehitystarpeita ajoneuvojen verkkoympäristön tietoturvaan liittyen. Erityisesti nämä liittyivät uuteen matkapuhelinverkkoihin pohjautuvaan C-V2X-kommunikointiin. Myös fyysisen tietoturvan määritelmät puuttuivat kaikista ajoneuvoverkkojen osa-alueista. Lopuksi todetaan, että tietoturvan tulisi elää ja kehittyä samassa tahdissa muiden teknologisten innovaatioiden kanssa eikä sitä tulisi lykätä myöhemmäksi.

## LÄHTEET

- [1] Bayer S, Enderle T, Oka D-K, Wolf M. Automotive Security Testing—The Digital Crash Test. Teoksessa Springer, Cham; 2016 [viitattu 8. syyskuuta 2017]. s. 13–22. Noudettu osoitteesta: [http://link.springer.com/10.1007/978-3-319-19818-7\\_2](http://link.springer.com/10.1007/978-3-319-19818-7_2)
- [2] Ben Brahim M, Ben Hamida E, Filali F, Hamdi N. Performance impact of security on cooperative awareness in dense urban vehicular networks. Teoksessa: 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) [Internet]. IEEE; 2015 [viitattu 8. syyskuuta 2017]. s. 268–74. Noudettu osoitteesta: <http://ieeexplore.ieee.org/document/7347971/>
- [3] European Commission. Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems ( C-ITS ). 2017;
- [4] European Commission. Mobility and Transport - Cooperative, connected and automated mobility (C-ITS) [Internet]. [viitattu 12. elokuuta 2017]. Noudettu osoitteesta: [https://ec.europa.eu/transport/themes/its/c-its\\_en](https://ec.europa.eu/transport/themes/its/c-its_en)
- [5] European Commission. Mobility and Transport - Intelligent transport systems [Internet]. [viitattu 12. elokuuta 2017]. Noudettu osoitteesta: [https://ec.europa.eu/transport/themes/its\\_en](https://ec.europa.eu/transport/themes/its_en)
- [6] Liikenne- ja viestintäministeriö. Liikenteen automaation ja robotiikan kehittämistoimen- piteiden tiekartta 2017 – 2019. 2017;
- [7] Lobach S, Radusch I. Integration of communication security into advanced simulation environments for ITS. IEEE Veh Technol Conf. 2011;
- [8] Lockwood S, Auer A, Feese S. History of Intelligent Transportation Systems [Internet]. 2016. 56 s. Noudettu osoitteesta: <https://ntl.bts.gov/lib/59000/59200/59263/download1.pdf>
- [9] Mikami T. CACS-Urban traffic control system featuring computer control. [viitattu 30. kesäkuuta 2017]; Noudettu osoitteesta: <https://www.computer.org/csdl/proceedings/afips/1978/5086/00/50861265.pdf>
- [10] Pilli-Sihvola E. Automaattiajamisen kokeilut Suomessa. 2016;
- [11] Qualcomm. Leading the world to 5G:Cellular Vehicle-to-Everything (C-V2X) technologies. 2016;(June):1–39.
- [12] Ray S, Chen W, Bhadra J, Al Faruque MA. Extensibility in Automotive Security. Teoksessa: Proceedings of the 54th Annual Design Automation Conference 2017 on - DAC '17 [Internet]. New York, New York, USA: ACM Press; 2017 [viitattu 8. syyskuuta 2017]. s. 1–6. Noudettu osoitteesta: <http://dl.acm.org/citation.cfm?doid=3061639.3072952>

- [13] Scholliers J, Kutila M. UrbanAutoTest : Urban area test bed for connected and automated driving Project overview. 2016;
- [14] Society of Automotive Engineers (SAE). Automated Driving.
- [15] Tokuyama H. Public Roads - Intelligent Transportation Systems in Japan , Fall 1996 - [Internet]. [viitattu 30. kesäkuuta 2017]. Noudettu osoitteesta: <https://www.fhwa.dot.gov/publications/publicroads/96fall/p96au41.cfm>
- [16] 3GPP [Internet]. [viitattu 17. elokuuta 2017]. Noudettu osoitteesta: [www.3gpp.org](http://www.3gpp.org)
- [17] Bosch sees potential for 48-volt systems and brings automated driving to Japan - Bosch Media Service [Internet]. [viitattu 14. elokuuta 2017]. Noudettu osoitteesta: <http://www.bosch-presse.de/pressportal/de/en/bosch-sees-potential-for-48-volt-systems-and-brings-automated-driving-to-japan-43122.html>
- [18] DIRECTIVE 2010/40/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 July 2010. Off J Eur Union [Internet]. 2010;1–13. Noudettu osoitteesta: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:207:0001:0013:EN:PDF>
- [19] ETSI EN 302 637-2 - V1.3.2 - Intelligent Transport Systems (ITS) - Vehicular Communications - Basic Set of Applications - Part 2 : Specification of Cooperative Awareness Basic Service. 2010;1:1–22.
- [20] ETSI EN 302 637-3 - V1.2.2 - Intelligent Transport Systems (ITS); Vehicular Communications; Part 3 : Specifications of Decentralized Environmental Notification Basic Service. 2014;2:1–73.
- [21] ETSI EN 302 663 v.1.2.0 - Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band. 2012;0:1–24.
- [22] ETSI EN 302 665 V1.1.1 - Intelligent Transport Systems (ITS); Communications Architecture. Context. 2010;1:1–44.
- [23] ETSI ES 202 663 - V1.1.0 - Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band. ETSI Stand. 2009;0:1–27.
- [24] ETSI TR 102 638 V1.1.1 - Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions. ETSI, Sophia Antip Cedex, Fr [Internet]. 2009;1:1–81. Noudettu osoitteesta: [http://scholar.google.com/scholar?hl=en%7B&%7DbtnG=Search%7B&%7Dq=intitle:Intelligent+Transport+Systems+\(ITS\);+Vehicular+Communications;+Basic+Set+of+Applications;+Definitions%7B#%7D1](http://scholar.google.com/scholar?hl=en%7B&%7DbtnG=Search%7B&%7Dq=intitle:Intelligent+Transport+Systems+(ITS);+Vehicular+Communications;+Basic+Set+of+Applications;+Definitions%7B#%7D1)
- [25] ETSI TR 102 893 V1.1.1 - Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA). 2010;1:1–86.
- [26] ETSI TS 102 637-1 - V1.1.1 - Intelligent Transport Systems (ITS); Vehicular

- Communications ; Basic Set of Applications ; Part 1 : Functional Requirements. 2010;1:1–60.
- [27] ETSI TS 102 731 V1.1.1 - Intelligent Transport Systems (ITS): Security Services and Architecture. 2010;1:1–68.
- [28] ETSI TS 102 940 V1.1.1 - ITS communications security architecture and security management. Tech Specif. 2012;1:1–29.
- [29] ETSI TS 102 941 V1.1.1 - Intelligent Transport Systems (ITS); Security; Trust and Privacy Management. 2012;1.1.1(102 941):1–30.
- [30] ETSI TS 102 942 V1.2.1 - Intelligent Transport Systems (ITS); Security; Access Control. 2012;1:1–10.
- [31] ETSI TS 102 943 V1.1.1 - Intelligent Transport Systems (ITS); Security; Confidentiality services. 2012;1:1–9.
- [32] ETSI TS 103 096-1 V1.3.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance. 2017;1:1–13.
- [33] ETSI TS 103 096-2 V1.3.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP). 2017;1:1–184.
- [34] ETSI TS 103 096-3 V1.3.1 - Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT). 2017;1:1–28.
- [35] ETSI TS 103 097 V1.2.1 - Intelligent Transport Systems (ITS); Security; Security and certificate formats. 2009;1(34):1–35.
- [36] ETSI TS 123 285 V14.2.0 - Universal Mobile Telecommunications System (UMTS); LTE; Architecture enhancements for V2X services (3GPP TS 23.285 version 14.2.0 Release 14). 2017;0:1–36.
- [37] ETSI TS 133 185 - V14.0.0 - LTE; 5G; Security aspect for LTE support of Vehicle-to-Everything (V2X) services (3GPP TS 33.185 version 14.0.0 Release 14). 2017;0:0–12.
- [38] IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007) IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access C. 2010;
- [39] ITS Standards Fact Sheets [Internet]. [viitattu 26. kesäkuuta 2017]. Noudettu osoitteesta: <https://www.standards.its.dot.gov/Factsheets/Factsheet/80>
- [40] Journey – Waymo [Internet]. [viitattu 14. elokuuta 2017]. Noudettu osoitteesta: <https://waymo.com/journey/>

- [41] OMNeT++ Discrete Event Simulator [Internet]. [viitattu 23. elokuuta 2017]. Noudettu osoitteesta: <https://omnetpp.org/>
- [42] SUMO - Simulation of Urban MObility [Internet]. [viitattu 23. elokuuta 2017]. Noudettu osoitteesta: [http://www.sumo.dlr.de/userdoc/Sumo\\_at\\_a\\_Glance.html](http://www.sumo.dlr.de/userdoc/Sumo_at_a_Glance.html)
- [43] Tesla [Internet]. [viitattu 14. elokuuta 2017]. Noudettu osoitteesta: <https://www.tesla.com/>
- [44] UrbanAutoTest - Home [Internet]. [viitattu 21. kesäkuuta 2017]. Noudettu osoitteesta: <http://www.vtt.fi/sites/urbanautotest/>
- [45] V2X-Emulator [Internet]. [viitattu 23. syyskuuta 2017]. Noudettu osoitteesta: <https://www.spirent.com/-/media/Datasheets/TT/TTsuites/V2X-Emulator.pdf>
- [46] Veins [Internet]. [viitattu 23. elokuuta 2017]. Noudettu osoitteesta: <http://veins.car2x.org/>
- [47] VSimRTI - Smart Mobility Simulation [Internet]. [viitattu 23. elokuuta 2017]. Noudettu osoitteesta: <https://www.dcaiti.tu-berlin.de/research/simulation/>
- [48] World Urbanization Prospects - Population Division - United Nations [Internet]. [viitattu 14. elokuuta 2017]. Noudettu osoitteesta: <https://esa.un.org/unpd/wup/>

## LIITE A: VERKKOKOMPONENTIT NED-KIELELLÄ

```
// Tämä koodi on perusesimerkki auton ja tienvarsiyksikön (RSU)
// välisestä kommunikoinnista.
//
// @author Harri Myllysoo
// @date 6.9.2017

// Simple-moduuli on peruskomponentti, jolle luodaan
// kommunikointiportit.
simple ITS2
{
    gates:
        input in;
        output out;
}

// Luodaan verkkoympäristö rsucar2, jossa kaksi
// komponenttia (rsu ja car) vaihtavat sanomia keskenään.
network rsucar2
{
    @display("bgb=238,189");
    submodules:
        rsu: ITS2 {
            @display("i=device/antennatower");
        }
        car: ITS2 {
            @display("i=device/car");
        }
    connections:
        rsu.out --> { delay = 100ms; } --> car.in;
        rsu.in <-- { delay = 100ms; } <-- car.out;
}
```

## LIITE B: KOMMUNIKOINNIN LÄHDEKOODI C++-KIELELLÄ

```
/*
 * rsucar2.cc
 *
 * C++-kielellä kirjoitettu esimerkkitiedosto tienvarsiyksikön
 * ja auton välisen kommunikoinnin lähdekoodista.
 *
 * Created on: 6.9.2017
 * Author: Harri Myllysuu
 */

#include <string.h>
#include <omnetpp.h>

using namespace omnetpp;

class ITS2 : public cSimpleModule
{
protected:
    virtual void initialize() override;
    virtual void handleMessage(cMessage *msg) override;
};

// Rekisteröidään Module-luokka OMNeT++-sovelluksen kanssa
Define_Module(ITS2);

void ITS2::initialize()
{
    // Simulaation alussa täytyy kutsua Initialize-metodia.
    // Jotta rsu-car-rsu-car -kommunikointi voi alkaa, toisen täytyy
    // aloittaa lähettämällä ensimmäinen viesti. Se olkoon rsu.
    if (strcmp("rsu", getName()) == 0) {
        // Luodaan ja lähetetään ensimmäinen viesti porttiin "out".
        // "ITSmsg" on viestiobjektin nimi.
        cMessage *msg = new cMessage("ITSMsg");
        send(msg, "out");
    }
}

void ITS2::handleMessage(cMessage *msg)
{
    // Kun viesti saapuu moduuliin, kutsutaan silloin
    // handleMessage()-metodia. Tässä viesti lähetetään toiselle
    // moduulille out-portin kautta ja koska molemmat moduulit
    // tekevät samaa, viesti palloilee molempien välillä.
    send(msg, "out"); // lähetetään viesti
}
```