Kristian Käyhty

Ajoneuvojen internetin haasteet ja ratkaisut

Tietotekniikan pro-gradu tutkielma

17. lokakuuta 2022

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Kristian Käyhty

Yhteystiedot: kayhtykr@student.jyu.fi

Ohjaaja: Timo Hämäläinen

Työn nimi: Ajoneuvojen internetin haasteet ja ratkaisut

Title in English: Challenges and solutions of the Internet of Vehicles

Työ: Pro-gradu tutkielma

Opintosuunta: Ohjelmisto- ja tietoliikennetekniikka

Sivumäärä: 99+0

Tiivistelmä: Tässä tutkielmassa tehdään IoV:n, sen haasteiden ja niihin löytyvien mahdollisten viimeisimpien ratkaisuehdotusten kartoitus kirjallisuuskatsauksena toisten tekemien tutkimusten pohjalta. Löytyneen lähdeaineiston perusteella havaittujen tulosten pohjalta tehdään myös omaa pohdintaa. Lopuksi tehdään oma analyysi kaikesta havaitusta. Tutkimuksessa havaittiin, että IoV:n suurimpina ja keskeisimpinä haasteina näyttäisi olevan erilaiset latenssiin, tietoturvallisuuteen, kaistanleveyteen, isojen datamäärien hallintaan, skaalautuvuuteen, standardeihin, autojen suuresti vaihtelevaan liikkuvuuteen ja infrastruktuurin luomisen haastavuuteen ja kalleuteen liittyvät haasteet. Tässä tutkimuksessa havaittiin, että näihin haasteisiin löytyy monia eri ideoita mahdollisiksi ratkaisuiksi ja käytettäviksi tekniikoiksi. Lupaavimpina tekniikoina IoV:n suhteen havaittiin olevan lohkoketju ja 5G. Myös reunalaskenta näyttäisi tarjoavan potentiaalisia mahdollisuuksia IoV:n suhteen. Myös koneoppiminen ja tekoäly vaikuttaisivat tulevaisuuden suhteen lupaavilta tekniikoilta IoV:n toteuttamisen kannalta, erityisesti erilaisten älykästä ja dynaamista päätöksentekoa vaativien sovellusten ja asioiden suhteen.

Avainsanat: Internet of Vehicles, IoV, haasteet, ratkaisut

Abstract: In this thesis, IoV, its challenges and possible latest solutions are mapped as a literature review based on research done by others. On the basis of the results found based on the found source material, one's own reflection is also done. Finally, a personal analysis is made

of everything observed. The study found that the biggest and most central challenges of IoV seem to be various challenges related to latency, information security, bandwidth, management of large amounts of data, scalability, standards, highly variable mobility of cars, and the difficulty and cost of creating infrastructure. This study found that there are many different ideas for possible solutions and techniques to be used for these challenges. Blockchain and 5G were found to be the most promising technologies for IoV. Edge computing also seems to offer potential opportunities in terms of IoV. Machine learning and artificial intelligence would also seem to be promising technologies for the future in terms of implementing IoV, especially in relation to various applications and issues that require intelligent and dynamic decision-making.

Keywords: IoV, Internet of Vehicles, challenges, solutions

Sisällys

1 Johdanto

Viime aikoina sekä tietoliikenneverkoissa että tiedonsiirtonopeuksissa on tapahtunut suuria edistysaskeleita. Ensin tuli 4G-verkot ja nyt on kovaa vauhtia tulossa 5G-verkot. Tämän johdosta myös ajoneuvoihin ja ajoneuvojen välille integroidut yhteydet ovat lisääntyneet. Tällaiset yhteydet ovat mahdollistuneet myös erilaisten lisääntyneiden elektronisten viestintäyksiköiden (Electronic Communication Units[ECU]) avulla. Tällaisia ovat esimerkiksi esineiden internettiin yhdistetyt erilaiset viestintälaitteet, sensorit ja anturit. Edellä mainitut kehitysaskeleet ovat mahdollistaneet esimerkiksi seuraavanlaiset yhteydet ajoneuvojen tapauksessa. Ajoneuvot voivat olla yhteydessä toisiin ajoneuvoihin (engl.Vehicle-to-vehicles (V2V)), ajoneuvot pystyvät kommunikoimaan ihmisten eli niin sanotusti jalankulkijoiden kanssa (engl.Vehicle-to-people (V2P)) ja ne voivat kommunikoida myös tienvarsissa olevan infrastruktuurin kanssa (engl.Vehicle-to-infrastructure (V2I)). Viimeisimmän kehityksen myötä mahdolliseksi on tullut myös ajoneuvojen kommunikointi kaikkeen (engl.Vehicle-to-everything(V2X)). Tämä kaikki on sitten johtanut älykkäiden liikennejärjestelmien (engl.Intelligent Transportation Systems(ITS)) syntymiseen. (Guerrero-Ibanez, Contreras-Castillo ja Zeadally 2021)

Kun verkkoon yhdistettyjen ajoneuvojen määrä kasvaisi liikenteessä, tulisi vastaan välttämättä monia haasteita nykyaikaiseen verkkoon suhteutettaessa. Nykyaikana käytettyihin verkkoihin tällaisten yhdistettävien ajoneuvojen mukana tulisi ongelmia, kuten verkon tukkeutumista, verkkoyhteyden katkeamista ja aiheutuisi luultavasti esimerkiksi korkeaa latenssia. Toisin sanoen verkkoon yhdistettyjen ajoneuvojen lisääntyessä perinteisissä verkoissa erityisesti tiedon levittäminen vaikeutuisi. Tämäkin on yksi niistä syistä, jonka takia alunperin ajoneuvojen internettiä, Internet of Vehicles (IoV), on lähdetty kehittämään. Alkuperäisenä ideana IoV:ia suunniteltaessa on ollut myös sekin, että IoV:n avulla saataisiin ikään kuin yhdistettyä ITS:n ja IoT:n teknologiat keskenään. IoV:n avulla pystytään luomaan tiedonvaihto ajoneuvojen ja niiden ympäristön välille. (Elhadja, Salim ja Abdelhamid 2020)

ITS:n kehitys on kulkenut ajoneuvojen ad hoc-verkoista eli VANETs:sta IoV:iksi. VANETs on kehittynyt alunperin ainoastaan liikenteen tehostamiseen ja liikenneonnettomuuksien vähentämiseen. Nämä ovat edelleen IoV:nkin tavoitteita, mutta IoV:ssa keskitytään turvalli-

suuden lisäksi myös matkan aikana tarjottaviin viihtymisen palveluihin. IoV:iinkin liittyy edelleen monia erilaisia haasteita, jotka tulisi tulevaisuudessa pyrkiä jotenkin ratkaisemaan. (Sleem, Noura ja Couturier 2020)

Tämän tutkielman tarkoituksena on IoV:n, sen haasteiden ja niihin löytyvien mahdollisten ratkaisuehdotusten kartoitus toisten tekemien tutkimusten pohjalta. Ratkaisuehdotukset ja -ideat on pyritty poimimaan enimmäkseen läheisimmiltä vuosilta löytyneiden lähteiden perusteella. Löytyneen lähdeaineiston pohjalta havaittujen tulosten perusteella tutkielman lopuksi tehdään vielä oma analyysi kaikesta havaitusta.

Luvussa 2 esitellään IoV käsitteenä ja samaan asiayhteyteen liittyvät olennaiset muut käsitteet. Lisäksi avataan perusasioita IoV:sta ja sen kehittymisen taustoista, avataan motivaatioita IoV:n kehittämiseen ja avataan myös IoV:n viestintätyyppejä, palveluita ja hyötyjä. Lisäksi avataan IoV:n eroavaisuuksia verraten tarkemmin VANETs:iin. Luvussa 3 kuvataan IoV:n keskeisimpiä haasteita ja ongelmia. Luvussa 4 esitetään ratkaisuehdotuksia ja -ideoita IoV:n ongelmiin ja haasteisiin. Luvussa 5 tehdään vielä koonti löytyneistä tuloksista eli ratkaisuehdoituksista ja -ideoista sisältäen myös omaa pohdintaa. Tämän jälkeen luvussa 6 tehdään vielä oma analyysi kaikesta tutkimuksessa havaitusta.

2 IoV:n esittelyä

Tässä luvussa esitellään lyhyesti Internet of Vehicles (IoV) käsitteenä ja sen yhteyteen olennaisesti liittyviä muita käsitteitä. Lisäksi kerrotaan vielä syvemmin perusasioita IoV:sta ja avataan sen kehittymisen taustoja. Tämän jälkeen avataan vielä motivaatioita ja syitä IoV:n kehittämiseen, IoV:n kehittymisen taustoja, motivaatioita IoV:n kehittämiseen ja avataan myös IoV:n viestintätyyppejä, palveluita ja hyötyjä. Lisäksi avataan vielä IoV:n eroavaisuuksia verraten tarkemmin VANETs:iin.

2.1 Aiheeseen liittyviä olennaisia käsitteitä

Tässä osiossa avataan IoV käsitteenä ja sen yhteyteen olennaisesti liittyvät muut käsitteet.

2.1.1 ITS

Ajoneuvojen kommunikointi kaikkeen (engl.Vehicle-to-everything(V2X)) on tullut mahdolliseksi, joka on sittemmin johtanut siihen, että älykkäät liikennejärjestelmät (engl.Intelligent Transportation Systems(ITS)) on syntynyt. Lisäksi ajoneuvovirrat kasvavat kaiken aikaa. ITS:n tavoitteena on pyrkiä vastaamaan tähän ongelmaan ja edistää liikenteen tehokkuutta kaupungeissa. ITS pyrkii myös vähentämään liikenteessä tapahtuvia onnettomuuksia. ITS pyrkii lisäksi käyttämään erilaisia älykkäitä tekniikoita siihen, että sekä liikenneturvallisuus paranisi että liikenne tehostuisi. Tavoitteena sillä on samalla pyrkiä myös kasvattamaan energiatehokkuutta ja vähentämään liikenteestä aiheutuvaa ympäristön saastumista. Tarkemmin sanottuna ITS pyrkii siis hyödyntämään uusimpia teknologisia ratkaisuja liikenteen ohjaamiseen. ITS yrittää myös käyttää viestintätekniikkaa siihen, että ECU:iden tuottamaa tietoa lähetetään pilvessä oleville palvelimille. Näiden kautta sitten prosessoitua tietoa analysoidaan erilaisten tieliikenneongelmien ratkaisemiseksi. ITS pyrkii myös käyttämään hyödyksi tienvarsi-infrastruktuurien ja ajoneuvojen sisäisten antureiden keräämää tietoa ajaakseen tavoitteitaan liikenteen turvallisuuden ja tehokkuuden parantamiseksi. Näin ITS pyrkii myös siis ennakkoon jo keräämään tietoa ja varoittamaan esimerkiksi vaarallisista olosuhteista. ITS yrittää lisäksi vähentää esimerkiksi liikenneruuhkia ja esittää parempia kulkureittejä kuljet-

tavaksi. Tätä kautta sitten edelleen mahdollistuisi jälleen tehokkaampi liikenteen kulku ja samalla myös onnettomuudet vähenisivät. (Guerrero-Ibanez, Contreras-Castillo ja Zeadally 2021)

2.1.2 Internet of Things (IoT)

"Esineiden internet (IoT) on periaatteessa kuin järjestelmä sellaisten tietokonelaitteiden, mekaanisten ja digitaalisten koneiden, esineiden tai yksilöiden yhdistämiseen, jotka on varustettu ainutlaatuisella järjestelmällä (UID) ilman siirtoa tietojen siirtämiseksi ihmiseltä ihmiselle tai tietokoneelle."(Laghari ym. 2021)

IoT:ssa arkielämän laitteet, kuten esimerkiksi kodinkoneet, teollisuustoimilaitteet, valvontakamerat, liikennevalot ja ajoneuvot pystyvät kommunikoimaan sekä keskenään että muiden Internettiä käyttävien käyttäjien kanssa. IoT:n yksi tavoitteista on siis tehdä Internetistä konseptina laajempi ja immersiivisempi mahdollistamalla helppo vuorovaikutus erilaisten laitteiden välillä. (Guevara ja Auat Cheein 2020)

2.1.3 Road Side Units (RSU)

Liikkumaton tienvarsiyksikkö, jota käytetään tietojen vaihtamiseen. Ne esimerkiksi voivat vaihtaa tietoa sellaisten ajoneuvojen kanssa, joissa on On-Board Unit (OBU). Eli toisin sanoen ne pystyvät vaihtamaan tietoa sellaisten ajoneuvojen kanssa, jotka kykenevät sekä langattomaan viestintään että viestintään toisten läheisten vastaavien ajoneuvojen kanssa. (Sleem, Noura ja Couturier 2020)

2.1.4 Vehicular Ad-hoc Networks (VANETs)

Älykkäät liikennejärjestelmät eli ITS on kehittynyt VANETs:sta IoV:iksi. VANETs on mobiili ad-hoc-verkko ja sitä käytetään RSU:iden ja ajoneuvojen välisessä viestinnässä. VANETs:n tavoitteina on pyrkiä parantamaan liikenneturvallisuutta esimerkiksi liikenteen tehostamisen ja liikenneonnettomuuksien vähentämisen kautta. VANETs:lla olevat monet rajoitteet ja sen kaupallinen kiinnostamattomuus ovat ajaneet lopulta IoV:n kehittämiseen. (Sleem, Noura ja Couturier 2020)

2.1.5 Internet of Vehicles (IoV)

Elhadja, Salim ja Abdelhamid (2020) ovat artikkelissaan tiivistäneet hyvin Internet of Vehicles eli IoV -käsitteen. IoV määritellään IoT:n ja ITS:n yhdistelmäksi. Se pyrkii parantamaan liikenneturvallisuutta ja tarjoamaan erilaisia palveluita kuljettajille lisätäkseen matkustamisen mukavuutta tien päällä toisin kuin VANETs. VANETs sen sijaan keskittyy enemmänkin pelkästään turvallisuuden parantamiseen. IoV mahdollistaa ajoneuvoille yhteyden mihin tahansa esineeseen kattaakseen kaikki tiellä tapahtuvat ongelmatilanteet, kuten esimerkiksi terveydelliset aspektit, rikokset ja erilaiset tieliikenneonnettomuudet, kuten loukkaantumiset ja liikenteessä tapahtuvat kuolemat. Toisin sanoen IoV:n päätavoitteena on pyrkiä mahdollistamaan se, että kuljettajat pääsisivät perille turvallisesti. Tämän lisäksi matkanteosta pyritään vielä samalla tekemään kuljettajille mahdollisimman mukava kokemus tarjoamalla erilaisia palveluita viihdykkeeksi matkan aikana. (Elhadja, Salim ja Abdelhamid 2020)

IoV nähdään IoT:n ja ITS:n yhdistämisen tuloksena. IoV tekee siis mahdolliseksi tiedon siirtämisen ajoneuvojen ja ympäristön välillä. Ympäristöksi katsotaan tässä tapauksessa esimerkiksi RSU:t, anturit, kuljettajat, matkustajat ja jalankulkijat. Tiedon siirtäminen ympäristön ja ajoneuvojen välillä tapahtuu Internetin kautta erilaisten protokollien ja viestintätekniikoiden avulla. Ajoneuvojen ja erilaisten esineiden, kuten toisten ajoneuvojen, RSU:iden ja henkilökohtaisten laitteiden, välinen viestintä mahdollistuu erilaisten viestintäprotokollien, viestintätekniikoiden ja matkapuhelinverkkojen, kuten 4G:n ja sittemmin tulevaisuudessa yhä paremmin 5G:n, avulla. Toisin sanoen ajoneuvojen välinen liitettävyys tapahtuu antureiden, ympäristössä olevien älykkäiden järjestelmien ja ajoneuvon sisäisten älylaitteiden välillä olevan yhteyden kautta osana isompaa kokonaisuutta eli ITS:ää. Näin pystytään sitten tarjoamaan esimerkiksi erilaisia liikenteenhallintaan ja tieturvallisuuteen liittyviä palveluita. Lisäksi pystytään tarjoamaan infotainment -palveluita eli toisin sanoen erilaisia informaatio- ja viihdepalveluita sekä ajoneuvoille että niissä matkustaville ihmisille.(Elhadja, Salim ja Abdelhamid 2020; Sleem, Noura ja Couturier 2020)

IoV nähdään myös IoT-teknologian eräänlaisena sovellusmallina ITS:n mukaisessa teknologiassa, jossa IoV on kolmen eri verkon, ajoneuvojen sisäisen verkon, ajoneuvojen välisen verkon ja ajoneuvojen mobiili-internetin yhdistelmä. IoV on siis ikään kuin valtava käyttöö-

notettava järjestelmä tiedonsiirtoon Vehicle-to-everything (V2X) -viestinnän ja yleisen langattoman viestinnän välillä. V2X -viestintätyyppi tarkoittaa tässä tapauksessa viestintää ajoneuvojen ja kaiken sellaisen välillä, joiden kanssa ajoneuvojen on mahdollista viestiä. IoV:n tärkeimpinä tavoitteina on tehostaa yleisesti liikennejärjestelmää, pyrkiä minimoimaan liikenteestä aiheutuvia kustannuksia ja pyrkiä pitämään asiakkaat tyytyväisinä sen tuottamiin palveluihin. Toisin sanoen IoV:n pääasiallisena tavoitteena on auttaa sekä autoilijoita kulkemaan matkansa turvallisesti että tarjota palveluita viihdykkeeksi matkan aikana tehden matkasta mukavamman kokemuksen. IoV pyrkii myös siis ajoneuvojen ja ympäristön välisen tiedon vuorovaikutuksen kautta auttamaan reaaliaikaisten tietietojen ja tietapahtumien välittämisessä ja turvallisuuden, liikennetehokkuuden ja ajokokemuksen mukavuuden parantamisessa. (Elhadja, Salim ja Abdelhamid 2020)

IoV voidaan nähdä myös VANETs:n laajennuksena ja evoluutiona. Siinä missä VANETs aikaisemmin on tarjonnut vain pelkästään turvallisuussovellusta ajoneuvoihin, IoV muuttaa ajoneuvon käsitteen ikään kuin älykkääksi tarjotessaan sovelluksia ja palveluita myös muihin eri osa-alueisiin ja teknologioihin liittyen. Täten IoV:n myötä käytettäväksi tulee enemmän eri viestintätyyppejä, joita ovat IoV:ssa Vehicles-to-Infrastructure (V2I), Vehicles-to-Personal devices (V2P), Vehicles-to-Vehicle (V2V), Vehicles-to-Roadside units (V2R) ja Vehicles-to-Sensors (V2S). Näistä kaikista muodostuu sitten yhdessä jo edelläkin mainittu Vehicles-to-everything (V2X). IoV:sta on siis tullut IoT:n erityinen sovellus, joka mahdollistaa kuljettajille mukavan ja turvallisen ajokokemuksen. Lyhyesti tiivistettynä IoV:n isoin tavoite on kaiken kaikkiaan saavuttaa turvallisempi, tehokkaampi ja vihreämpi eli ympäristöystävällisempi kuljetusmaailma.(Elhadja, Salim ja Abdelhamid 2020; Sleem, Noura ja Couturier 2020; Li ym. 2020) .

2.2 Tietoa IoV:sta ja IoV:n taustat ja motiivit

Tässä osiossa kerrotaan vielä perustietoa IoV:iin liittyen. Lisäksi avataan IoV:n kehityksen taustat ja motiivit. Myös IoV:n ja VANETs:n eroavaisuuksista kerrotaan vielä tarkemmin.

2.2.1 Perustietoa ja taustaa IoV:sta

Kuten edelläkin käsitteiden yhteydessä mainittiin, älykkäät kuljetusjärjestelmät eli ITS on alunperin keskittynyt ajoneuvojen ad-hoc-verkkoihin eli VANETs:iin. Tarkoituksena on ollut keskittyä pääasiassa liikenneonnettomuuksien vähentämiseen sekä liikenteen kulun tehostamiseen. IoV:ssa nämä ovat toki pääpointteja edelleen, mutta myöhemmin on turvallisuuden lisäksi alettu palveluissa ottaa huomioon myös muita tekijöitä, kuten esimerkiksi viihdepuolta. Sittemmin kehitys on kulkenut ITS:ssä siihen suuntaan, että VANETs:n pohjalta on kehittynyt IoV. Jo VANETs:n tapauksessa on ollut, mutta myös edelleen IoV:n tapauksessa on, paljon erilaisia haasteita, ongelmia ja kehityskohteita. Ne tulisi saada vielä ratkaistua tavalla tai toisella, jotta IoV:ia olisi mahdollista alkaa toteuttamaan ja ottamaan käyttöön täysipainoisesti. (Sleem, Noura ja Couturier 2020) IoV:n haasteista vielä erikseen myöhemmin lisää tarkemmin.

Lisäksi tänä päivänä tutkijoiden keskuudessa yhdeksi kunnianhimoisimmista tavoitteista on tullut esimerkiksi seuraava. Tavoitteena on se, että kaikki sellaiset saatavilla olevat verkot, jotka ovat heterogeenisiä keskenään, saataisiin yhdistettyä yhden universaalin verkon avulla. Tällainen yhdistävä universaali verkko olisi toisin sanoen nimeltään esineiden internetti eli IoT. Tavoitteena olisi, että IoT:n avulla kaikki heterogeeniset laitteet, esimerkiksi kodinkoneet, kannettavat tietokoneet, tabletit, erilaiset anturit, älypuhelimet ja erilaiset ajoneuvot, saataisiin yhteentoimiviksi sen kanssa. Älykkäät ajoneuvot ja näin ollen ITS ja vielä edelleen IoV kuuluvat kaikki siis ikään kuin IoT:n alaisuuteen yksinä kehityskohteina. IoV mainitaankin yhdeksi tämän hetken isoimmista IoT:iin kohdistuvan kehitystyön alla olevista kohteista. IoV on viime vuosina muutenkin ollut suuri kiinnostuksen kohde monien tutkijoiden keskuudessa. (Sleem, Noura ja Couturier 2020)

IoV onkin siis ikään kuin IoT:n erityinen sovellus. Kuten edeltäkin on jo tullut ilmi, IoV:n avulla kuljettajien ajokokemuksesta pyritään erilaisten palvelujen kautta tekemään mahdollisimman mukava, sujuva ja ennen kaikkea turvallinen. IoV-verkon kautta mahdollistettaisiin autonomisten ajoneuvojen tapauksessa se, että ne pystyisivät kommunikoimaan sekä ympärillä olevien toisten yhdistettävien ajoneuvojen kanssa että myös ympäristön kanssa muutenkin. IoV:n tapauksessa siihen kytkeytyvien erilaisten palveluiden mahdollistamiseksi ja IoV:n haastekohtien ratkaisemiseksi on pyritty luomaan erilaisia uusia teknologioita

ja konsepteja. On ehdotettu kokeiltavaksi ja käytettäväksi teknologioita, kuten lohkoketjua (engl.Blockchain), reunalaskentaa (engl.Edge computing), erilaisia anturitekniikoita ja esimerkiksi tekoälyä. Tavoitteena olisi saada IoV:sta mahdollisimman turvallinen ja luotettava. Ajoneuvojen välinen yhteenliitettävyys verkossa mahdollistuu ajoneuvojen sisäisten älylaitteiden ja anturien sekä myös ajoneuvojen ulkopuolisten älykkäiden järjestelmien välityksellä. Tämä kaikki yhteenliittäminen tapahtuu siis niin sanotusti osana ITS:ää ja kuuluu kyseisen käsitteen alaisuuteen. Kyseisenlaista teknologiaa omaaviin autoihin pyritään myös luomaan parhaalla mahdollisella tavalla sellaista tekniikka, että esimerkiksi ajoneuvojen liikeratoja ja kuljettajan käyttäytymistä pystyttäisiin ennustamaan. Edelleen tällä pyritään siis siihen, että liikenne tehostuisi ja onnettomuudet liikenteessä vähenisivät. (Sleem, Noura ja Couturier 2020)

2.2.2 IoV:n viestintätyypit

IoV:n viestintätyyppejä ovat Vehicle-to-Vehicle (V2V), Vehicle-to-Pestrian (V2P), Vehicle-to-Infrastructure (V2I), Vehicle-to-sensor (V2S) ja Vehicle-to-roadside units (V2R). Seuraavaksi näistä jokaisesta vielä hieman tarkemmin erikseen. Ensinnäkin V2V tarkoittaa seuraavaa. Kyseessä on langaton tiedonsiirto kahden eri ajoneuvon välillä. Eli, jos itse olet kuljettajana ajoneuvossa, olet ikään kuin ego -ajoneuvossa. Toinen ajoneuvo, jonka kanssa viestitään omasta ajoneuvosta käsin, on sitten taas kohdeajoneuvo. Eli kyseessä on siis sellainen IoV:n viestintätyyppi, jossa esimerkiksi kaksi ajoneuvoa harjoittavat tiedonsiirtoa keskenään. Tälläisessa tiedonsiirrossa voidaan vaihtaa tietoja liittyen esimerkiksi nopeuteen, sijaintiin, kiihtyvyyteen ja suuntaan liittyen. V2I puolestaan on sellainen viestintätyyppi, jossa tiedonsiirtoa tapahtuu ajoneuvojen ja erilaisten infrastruktuureiden välillä. Infrastruktuureilla tarkoitetaan tässä tapauksessa useimmiten teille ja niiden varsiin asennettuja tieantureita ja tiemerkintöjä ja lisäksi satelliittijärjestelmiä, pysäköintialueita ja esimerkiksi liikennemerkkiantureita. Yhteistä tällaisilla infrastruktuureilla on tässä tapauksessa yleensä se, että ne pystyvät vaihtamaan tietoja ajoneuvojen kanssa. Tälläisen viestinnän tavoitteena on pyrkiä tarjoamaan reaaliaikaista tietoa liittyen eri tekijöihin. Reaaliaikaista tietoa voidaan siis tarjota esimerkiksi liikenteen tiheyteen, tien nykyiseen tilaan, muihin olosuhteisiin tai esimerkiksi sellaisiin ajoneuvoihin liittyen, jotka joko ajavat erittäin nopeasti tai yrittävät vaihtaa kaistaa.

Juuri edellä mainittujen kaltaisella viestinnällä eli V2I ja V2V -viestintätyyppien ja niiden mahdollistamien ominaisuuksien ja tekijöiden kautta on myös todennäköisesti mahdollista vähentää esimerkiksi liikenneonnettomuuksia. Lisäksi niiden avulla pystytään luultavasti tekemään ajokokemuksesta IoV:ssa sekä entistä tehokkaampi että turvallisempi. (El Madani, Motahhir ja El Ghzizal 2022; Elhadja, Salim ja Abdelhamid 2020)

V2S -viestintätyyppi on taas puolestaan seuraavanlainen. IoV:ssa käytetään paljon erilaisia antureita erilaisissa havannointitarkoituksissa. V2S -viestinnässä esimerkiksi solmut, joita voivat olla tässä tapauksessa infrastruktuurit ja autot esimerkiksi, keräävät erilaisia tietoja sisäisiä antureitaan käyttäen esimerkiksi ympäristöönsä ja tien tilaan ja siellä aistittaviin tapahtumiin liittyen. Tällaisia kerättyjä tietoja voidaan sitten edelleen lähettää esimerkiksi kuljettajille, matkustajille tai sitten joillekin ihan muille solmuille IoV:ssa. Kerätyissä tiedoissa voi olla kyse myös vaikkapa kuljettajan terveydestä, ajoneuvon nopeudesta tai muusta vastaavasta. V2P -viestinnässä taas puolestaan erilaiset tienkäyttäjät, kuten esimerkiksi pyöräilijät, moottoripyöräilijät ja ihan tavalliset jalankulkijat eli toisin sanoen ihmiset, vaihtavat tietoja ajoneuvojen kanssa. V2R -viestintätyypissä on kyse seuraavasta. Sillä tarkoitetaan tienvarsiyksiköiden eli RSU:iden ja ajoneuvojen välistä yhteyttä. Eli RSU:iden avulla voidaan esimerkiksi kerätä tietoa toisiin ajoneuvoihin ja erilaisiin uusiin tietapahtumiin liittyen. RSU:ita voidaan sitten edelleen käyttää tällaisten tietojen edelleen lähettämiseen muille liikenteessä liikkuville ajoneuvoille tai kerättyjä tietoja voidaan sen sijaan esimerkiksi jollain muulla tavalla käsitellä. (El Madani, Motahhir ja El Ghzizal 2022; Elhadja, Salim ja Abdelhamid 2020)

2.2.3 IoV:n kehityksen motiivit

IoV:n kehittämiselle on monia motiiveja. Yhdeksi isoimmista alkuperäisistä syistä IoV:n kehittämiselle voidaan nähdä esimerkiksi se, että VANETs:lla on ollut monia ongelmakohtia, rajoituksia ja puutteita. Näitä on sitten IoV:n kehittämisen kautta pyritty lähteä muuttamaan ja kehittämään. Kuten edeltäkin jo käsitteiden yhteydessä tuli ilmi, VANETs on mobiili adhoc-verkko. IoV:iin verrattuna sen infrastruktuurikokonaisuudet koostuuvat ainoastaan ajoneuvoista ja tienvarsiyksiköistä eli RSU:ista. Tämä tarkoittaa taas puolestaan esimerkiksi sitä, että IoV:n viestintätyyppeihin verrattuna VANETs:ssa on mahdollista harjoittaa pelkäs-

tään V2R tai V2V-viestintää. Tämä on esimerkiksi jo yksi rajoittava tekijä VANETs:n tapauksessa. Seuraavaksi tarkemmin rajoittavia tekijöitä ja ongelmia VANETs:n suhteen. Ensinnäkään puhdas ad-hoc-verkko, jollainen VANETs on, ei pysty mahdollistamaan ITS:n tavoittelemia maailmanlaajuisia palveluita. Tämä johtuu puolestaan ajoneuvojen jatkuvasta liikkumisesta, jonka seurauksena yhteydet katkeilevat jatkuvasti. Toinen puute VANETs:ssa, joka aiheutuu ajoneuvojen suuresta liikkuvuudesta, on myös kaistanleveyden menetys. Lisäksi VANETs:n arkkitehtuuri ei mahdollista minkäänlaisten älykkäiden päätösten tekemistä johtuen sen tallennustilan rajoituksista, tietojenkäsittelyyn liittyvistä puutteista ja ajoneuvojen pilvipalveluiden puuttumisesta. Pilvipalveluiden puute ja siitä aiheutuvat tietojenkäsittelyn ja tallennustilan rajoitukset ovat muutenkin yleisesti ongelma VANETs:n tapauksessa. VANETs ei myöskään kykene kommunikoimaan kunnolla nykyaikaisten henkilökohtaisten laitteiden kanssa. Tämä johtuu puolestaan VANETs:n yhteensopimattomasta verkkoarkkitehtuurista. Lisäksi, kuten edelläkin jo on mainittu, VANETs tukee pelkästään liikenteen tehokkuus- ja tieturvallisuuspalveluita. Erityisesti tämän takia ja myös siis kaupallisten palveluiden puuttumisen vuoksi VANETs ei ole kyennyt saavuttamaan riittävää suosiota kaupallisilla markkinoilla, joka on ollut myös yksi motiivi IoV:n kehittämiselle. VANETs:n kaupallisen kiinnostavuuden puutteeseen on vaikuttanut myös sen Internet-yhteyden heikko luotettavuus. Internetin heikko luotettavuus tässä tapauksessa aiheuttaa myös edelleen sen, että kaupalliset sovellukset puuttuvat VANETs:sta, eivätkä siis ole ajoneuvojen kuljettajien eivätkä matkustajien käytettävissä. Yksi ongelma on myös se, että maaseuduilla verkkojen tiheys voi usein olla matalaa. Tästä sitten aiheutuu taas puolestaa sellainen ongelma, että kriittisiä tietoja voi kadota, koska välisolmuista on puutetta. Tästä sitten taas puolestaan voi edelleen aiheutua vielä katastrofaalisempia ongelmia, kuten esimerkiksi liikenneonnettomuuksia. VANETs ei pysty myöskään hyödyntämään esimerkiksi 4G-verkkoja. Tästä aiheutuu sitten taas puolestaan se, että VANETs:n kautta ei pystytä takaamaan palveluita ja niiden jatkuvuutta loppukäyttäjien suhteessa laajoilla alueilla. Yksi motivoiva ongelmatekijä VANETs:n tapauksessa on myös seuraava. Siihen, että ajoneuvoverkosto toimisi kunnolla, vaikuttaa myös paljon verkon käyttäjien yhteistyö. Tällainen riippuvuus verkon käyttäjien välisestä yhteistyöstä puolestaan heikentää VANETs:n tarjoamien palveluiden luotettavuutta ja tähänkin tulisi saada ratkaisu. Edellä mainitut rajoitukset ovat siis yhtiä suurimpia syitä sille, että IoV:ia on alettu kehittämään. (Elhadja, Salim ja Abdelhamid 2020; Kaiwartya ym. 2016)

Toinen asia, jolla on ollut vaikutusta IoV:n kehitykseen, ovat erilaiset inhimilliset tekijät, kuten esimerkiksi kuljettajien käyttäytyminen. Juuri kuljettajien käyttäytyminen ja kuljettajat itsessään ovat usein nimenomaan se, jolla on vaikutusta muun muassa liikenteen ja matkustamisen tehokkuuteen ja liikenneonnettomuuksiin. Liikenneonnettomuudet ovat myöskin isoin syy kuolleisuudelle liikenteessä. Juuri nämä ovat siis myös isoja motiiveja IoV:n kehitystyölle. IoV:n avulla on myös entistä paremmin haluttu lähteä parantamaan liikenteen tehokkuutta ja ennen kaikkea vähentämään liikenteessä aiheutuvia onnettomuuksia. Esimerkiksi IoV:n ja sen tarjoamien palveluiden, kuten esimerkiksi autonomisen ajon, kautta pyritään siis kehittämään näitä tekijöitä. Yksi motiivi, joka on ajanut IoV:n kehitykseen, on ympäristötekijät. Ajoneuvot itsessään saastuttavat ympäristöä. Lisäksi niiden aiheuttamalla saastumiselle on myös esimerkiksi terveyttä heikentäviä vaikutuksia myös ihmisille. Toinen ympäristön saastumista aiheuttava tekijä on liikenneonnettomuudet. Ne saastuttavat esimerkiksi vesistöjä, ilmaa ja aiheuttavat myös melusaastetta. Lisäksi teillä tapahtuvat onnettomuudet voivat esimerkiksi edistää sairauksien leviämistä. Edelleen esimerkiksi erilaisilla terveydellisillä haitoilla ja muullakin saastumisella voi olla negatiivista vaikutusta eri maiden talouksiin. Esimerkiksi liikenneonnettomuuksilla voi olla moniakin erilaisia negatiivisia vaikutuksia sekä rahassa mitattuna kuin muutenkin. Seurauksena voi olla tuotannon menetyksiin liittyviä kustannuksia, henkilökustannuksia, inhimillisiä kustannuksia, tuottavuuteen vaikuttavia kustannuksia, lääketieteellisiä kustannuksia, infrastruktuureihin ja kiinteistöihin kohdistuvia kustannuksia ja muita erilaisia kustannuksia. Myös kaikki tämä on motivoinut lähteä kehittämään IoV:ia ja ratkaisemaan näitä ongelmia ja haasteita sen avulla. (Elhadja, Salim ja Abdelhamid 2020)

Kaikki edellä mainittu on siis esimerkiksi motivoinut lähteä kehittämään IoV:ia. IoV:lla pyritään ratkaisemaan kaikkia näitä ongelmakohtia esimerkiksi sen tarjoaman entistä laajemman verkon ja entistä monipuolisempien suurempien palveluiden kautta. IoV:n kautta liikenteestä pyritään tekemään turvallisempi ja luotettavampi. Lisäksi matkustamisesta halutaan myös tehdä entistä viihdyttävämpää kuljettajille erinäisten IoV:n tarjoamien palveluiden, kuten viihdepalveluiden, kautta. Yksi isoista motiiveista, joka on myös ajanut IoV:n kehittämiseen, on sen tarjoamat valtavat markkinamahdollisuudet. IoV:n kehittämisen kautta avautuu valtavat markkinamahdollisuudet sekä ennen kaikkea autoteollisuudelle, mutta myös monille muille teollisuudenaloille. Tällaisia muita hyötyviä teollisuudenaloja voivat olla esimer-

kiksi ohjelmistoteollisuus, Internet-palveluidentarjoajat ja IT-laitteiden valmistus. IoV:n kehittämisen kautta saataisiin todennäköisesti kasvatettua taloudellista arvoa myös seuraavassa suhteessa. Olennainen tekijä on myös siinä, että IoT:n kasvun suhteen nimenomaan autoteollisuus on yksi nopeimmassa kasvussa olevista teollisuudenaloista. IoV:n keskeisenä tavoitteena ja motiivina on myös matkustusajan tehokas hyödyntäminen. Toinen keskeinen motiivi IoV:n kehittämisessä ja sen tarjoamien markkinamahdollisuuksien suhteessa liittyy IoT:iin. Koska IoV on ikään kuin IoT:n osa, niin juuri nimenomaan IoT vaikuttaa lupaavalta alueelta markkinoiden suhteen. Tämä siksi, että siihen on kohdistettu paljon kehitystä viimeaikoina ja IoT:n kautta saavutetaan todennäköisesti myös korkea markkinoille pääsyn mahdollisuus. (Elhadja, Salim ja Abdelhamid 2020; Kaiwartya ym. 2016)

2.2.4 IoV:n palveluja

Kuten edeltäkin jo ilmi kävi, IoV pystyisi tarjoamaan ison määrän erilaisia palveluita, ainakin VANETs:iin verrattuna. IoV:n palvelujen kautta pystytään myös turvallisuuden lisäksi tarjoamaan ajoneuvojen kuljettajille ja matkustajille erilaisia ajomatkan mukavuutta lisääviä palveluita. IoV:n palveluiden kautta todennäköisesti pystytään myös vähentämään sekä matkustamiseen käytettävää aikaa että siitä koituvia kustannuksia. Seuraavaksi hieman luokittelua erilaisista palveluista, joita IoV:n avulla pystyttäisiin tarjoamaan. Ensinnäkin IoV:n kautta pystyttäisiin tarjoamaan turvallisuus- ja terveydenhuoltopalvelut. Ne koostuvat siis joukosta sovelluksia, jotka on kehitetty esimerkiksi sekä tieliikenneonnettomuuksien vähentämiseen että ohjeistamiseen ja tiedottamiseen sen suhteessa, että kuinka toimia parhaalla mahdollisella tavalla esimerkiksi onnettomuuden sattuessa. IoV:n palveluihin lukeutuu myös liikenteenhallinta- ja navigointipalveluita. Liikenteenhallintapalveluilla voidaan esimerkiksi informoida liikenneolosuhteisiin ja hyviin reittivalintoihin liittyen ja näin edistää liikenteen tehokkuutta. Sitten taas navigointipalveluiden avulla voidaan esimerkiksi myös auttaa ajoneuvoja pääsemään määränpäihinsä tehokkaasti, turvallisesti ja ajoissa. Voidaan esimerkiksi informoida erilaisia matkankestoja arvioiden ajassa mitattuna tietyssä sääolosuhteessa. IoV:n kautta pystytään myös tarjoamaan erilaisia Infotainment-palveluja eli toisin sanoen viihtymiseen liittyviä palveluita. Tällaisiin palveluihin lukeutuvat esimerkiksi internet-yhteys, video- ja äänipuhelut, videoiden katselu, musiikin kuuntelu ja jakaminen ja sosiaalisen me-

dian käyttäminen. IoV:n kautta onnistuu myös sääennustepalvelut, erilaiset kaupalliset palvelut ja esimerkiksi energiatehokkuuteenkin liittyvät palvelut. Sääennustepalveluissa ominaisuutena voi olla esimerkiksi sellainen, että ajoneuvo ottaa tiedon ilmakehästä ja sitten sään vaihtelun mukaisesti säätää myös ajoneuvon sisälämpötilaa. Kaupallisiin palveluihin voi lukeutua esimerkiksi ajoneuvoissa näytettäviä mainoksia lähellä sijaitsevista palveluista, kuten ruokapaikoista ja hotelleista hintoineen. Energiatehokkuuspalveluiden avulla sitten taas puolestaan voidaan pyrkiä eri tavoin vähentämään energiankulutusta liikenteessä. Eli tällaiset palvelut voivat siis auttaa vähentämään esimerkiksi polttoaineen kulutusta säätelemällä automaattisesti ajoneuvon nopeutta ja välttämällä ruuhkaisimpia paikkoja. (Elhadja, Salim ja Abdelhamid 2020)

2.2.5 IoV:n ja VANETs:n vertailua

Seuraavaksi hieman asiaa liittyen VANETs:n ja IoV:n välisiin eroavaisuuksiin. VANETs:n päätavoitteena on liikenneturvallisuuden takaaminen vähentämällä liikenneonnettomuuksia ja parantamalla liikenteen tehokkuutta. IoV:n päätavoitteena on puolestaan liikenneturvallisuuden ja liikenteen tehostamisen lisäksi myös, VANETs:sta poiketen, tarjota kaupallista viihdettä ajajille ja matkustajille tehdäkseen matkasta ja ajokokemusta paremman ja mahdollisimman mukavan. VANETs:ssa on mahdollista pelkästään V2V ja V2I -viestintä, kun taas IoV:ssa on mahdollista V2V, V2I, V2R, V2S ja V2P -viestintätyypit. Lisäksi IoV on yhteensopiva heterogeenisen verkkonsa ansiosta henkilökohtaisten laitteiden ja myös siis esimerkiksi älypuhelimien kanssa, kun taas VANETs ei ole yhteensopiva näiden kanssa ollenkaan. VANETs:n käyttöalue on sekä hyvin diskreetti että paikallinen. Vain rajoitetun mittakaavan sovellukset yleensä toimivat siinä. IoV:ssa taas puolestaan on todennäköisesti mahdollistettavissa globaalit kestävät sovellukset esimerkiksi tekoälyn avulla. Kuten edellä IoV:n kehityksen motiivien yhteydessä kävi ilmi, VANETs:lla on monia rajoituksia ja se ei esimerkiksi tämän vuoksi ole saavuttanut suosiota kaupallisilla markkinoilla. IoV:sta taas on puolestaan kiinnostuttu myös kaupallisessa mielessä erityisesti sen tarjoamien monipuolisten palveluiden ansiosta. IoV:n verkko on joustava ja heterogeeninen, kun taas VANETs puolestaan ei juurikaan sen ominaisuuksien ja rajoitusten takia kykene yhteistyöhön muiden olemassaolevien verkkojen kanssa. Internetin saatavuuden suhteessa VANETs ei ole juurikaan saa-

tavissa sen infrastruktuuripuutteiden takia, kun taas IoV:lla on tavoitteena, että sen verkot olisi saatavissa ja yhdistettävissä kaikkialla kaiken aikaa minkä tahansa kohteen kanssa. VANETs:n datamäärä on rajoittunutta, kun taas IoV pyrkii siihen, että rajoituksia datan suhteen ei juurikaan olisi. Verkon tehokkuuden suhteen IoV pyrkii siihen, että katkoksia ei juurikaan esiintyisi, kun taas VANETs:n suhteen on todettu toistuvia katkoksia ja häiriöitä verkossa. VANETs:ssa ei pystytä älykkäitä päätöksiä tekemään, kun IoV:n suhteen puolestaan luultavasti tekoälyn ja muiden teknologioiden välisellä yhteispelillä saadaan myös jonkinasteisia automatisoituun päätöksentekoon liittyviä asioita aikaiseksi. Pilvilaskenta ei ole myöskään saatavilla VANETS:ssa, kun taas IoV:ssa on siellä mahdollisesti saatavien laajojen reaaliaikaisten liikennetietojen ansiosta. (Sleem, Noura ja Couturier 2020) Edellä siis ikään kuin tiivistettynä jälleen sellaisia tekijöitä ja VANETS:n puutteita, jotka ovat motivoineet ja ajaneet erityisesti IoV:n kehittämiseen.

2.2.6 IoV:n hyötyjä ja etuja

IoV tuo mukanaan paljon erilaisia hyötyjä ja etuja. Seuraavaksi pieni otanta myös näihin liittyen. Ensinnäkin, kuten edellä jo mainittiin, IoV tulee paikkaamaan VANET:lla aikaisemmin olleet puutteet (Ji ym. 2020). Nämä ovat siis kaikki ikään kuin etuja ja nämä voi tarkistaa uudelleen edeltä. Näiden puutteiden paikkaamisen myötä IoV saa älykkäiden kuljetusjärjestelmien kehityksen tulevaisuudessa näyttämään lupaavalta. Lisäksi IoV:n myötä tietojenkäsittelykyky tulee luultavasti parantumaan. Tämän myötä mahdollisesti kehittyvät myös esimerkiksi tekoälyteknologia ja pilvilaskenta. Esimerkiksi näiden kahden kehitys mahdollistaa sitten taas puolestaan sen, että ajoneuvot pystyvät itsenäisesti valitsemaan pääsynsä tehokkaampiin verkkoihin varmistaakseen vakaan verkkoyhteyden. IoV:n myötä vanhaan VANETs:iin verrattuna avautuu todennäköisesti monia mahdollisuuksia niin kuljettajille kuin myös esimerkiksi eri yhteiskunnille ja talouksille. IoV:n myötä mahdollisesti vähentyvien liikenneruuhkien ja parantuvan tieturvallisuuden kautta voi koitua todennäköisesti esimerkiksi huomattavia taloudellisia säästöjä kansanterveysalalla. Mahdolliset reaaliaikaiset liikenneratkaisut yhdistettyjen ajoneuvojen kautta todennäköisesti lisäävät myös tuottavuutta, kun aika ruuhkissa olemisen suhteen vähentyy. Lisäksi IoV:n käyttöönottamisen myötä avautuu luultavasti eri palveluntarjoajille uusia mahdollisuuksia. Käyttöön otetaan mahdol-

lisesti uudenlaisia liikennepalveluita esimerkiksi parkkipaikkojen paikantamiseen, hätäpalveluihin, reaaliaikaiseen liikenteen raportointiin ja sijaintiin perustuvaan asiakaspalveluun liittyen. Sitten taas edelleen tällaisista palveluista tulee olemaan hyötyä eri tavoin sekä käyttäjille että myös yrityksille. Esimerkiksi ajoneuvojen käyttäjille koituvia hyötyjä voivat olla esimerkiksi alenevat vakuutushinnat, pienemmät käyttökustannukset ja he joutuvat todennäköisesti viettämään vähemmän aikaa liikenteessä liikenteen sujuvoituessa IoV:n myötä. Autovalmistajille koituvana hyötynä voi olla puolestaan alemmat palvelu- ja takuukustannukset. Yhteiskunnalle muuten aiheutuvia hyötyjä saattavat olla puolestaan vähenevät kolarit ja onnettomuudet. Lisäksi ruuhkat ja ympäristösaasteet vähenevät. (Ji ym. 2020; Darwish ja Abu Bakar 2018)

3 IoV:n haasteet ja ongelmat

Tässä luvussa kuvataan IoV:n keskeisimpiä haasteita ja ongelmia, jotka estävät vielä IoV:n täysmittaisen toteuttamisen ja vaativat vielä suunnittelua ja pohdintaa tulevaisuudessa. IoV:n kohtaamat haasteet liittyvät monesti muun muassa sellaisiin tekijöihin kuten tehokkuus, suorituskyky, turvallisuus, luotettavuus ja mukavuus (Elhadja, Salim ja Abdelhamid 2020). Esimerkiksi juuri kyseiset tekijät tulisi ikään kuin varmistaa IoV:n toimivuuden ja sen tarjoamien eri palveluiden tapauksessa. Tämä siksi, että kaikki toimisi vaaditulla tavalla, eikä aiheutuisi esimerkiksi onnettomuuksia liikenteessä tai muita ongelmallisia seurauksia. Seuraavaksi tarkemmin erilaisia keskeisiä IoV:n kehittämiseen liittyviä haasteita. (Elhadja, Salim ja Abdelhamid 2020)

Yksi IoV:n suurimmista ellei jopa suurin haaste liittyy tiedon reititykseen ja levitykseen. Solmuista, standardeista ja aliverkoista, joista IoV-verkko muodostuu, aiheutuu seuraavanlainen ongelma, koska ne ovat heterogeenisiä keskenään. Korkean QoS:n, tietyltä palvelulta vaadittavan laatuvaatimuksen, omaavat viestit ovat IoV:n tapauksessa vaikeasti välitettävissä solmulähteestä määränpäähänsä. Täten IoV:n yksi suurimmista ellei suurin haaste liittyykin seuraavaan. Haaste on siinä, että pitäisi saada kehitetty sellaisia lähestymistapoja, joiden avulla pystyttäisiin varmistamaan tarpeeksi alhainen lähetysviive eli latenssi. Myös siitä aiheutuvat kustannukset tulisi saada tarpeeksi alas. Toisin sanoen pitäisi keksiä jokin sellainen tapa, että tietoja pystytään lähettämään kohteisiinsa niin pienellä viiveellä ja alhaisilla kustannuksilla, että se täyttäisi laatuvaatimukset eli toisin sanoen QoS:n kyseisen asian suhteessa. Haasteena on myös optimaalisten ja kiinnostavien palveluiden valinta käyttäjälle siinä suhteessa, että pystyttäisiin sitten tarjoamaan tällaiset myös samalla pitämällä mielessä kustannusten minimointi, toimitusajan lyhentäminen ja asiakastyytyväisyys. Yksi IoV:n haasteista littyy myös massiiviseen tiedonhallintaan eli toisin sanoen big dataan. IoV:n käyttöönoton myötä siinä tulisi olemaan osana massiivinen määrä erilaisia liitettyjä laitteita. Koska IoV-verkko on heterogeeninen, siinä on täten suuri haaste seuraavan suhteen. IoV:ssa olevan datan yhdistäminen, analysointi, käsittely, tallennus ja siihen liittyvä päätöksenteko ovat kaikki asioita, joita on IoV:ssa täten vaikeaa toteuttaa täysin toimivasti. Vaihdettavan datan määrä on valtava ja lisäksi vaihdettava data voi olla myös hyvin erityyppistä keske-

nään. Haasteena ovat myös tietojen integrointi ja toiminnan hallinta. IoV:ssa esiintyy suurta vaihtelua asioiden suhteen ja tämän seurauksena haasteita tulee yhteistyön ja koordinoinnin toteuttamisessa erilaisten verkkojen välillä. Haasteena on, että kyseisen asian suhteen tulisi pohtia ja saada kehitettyä jonkinasteisia uusia menetelmiä, joilla pystyttäisiin varmistamaan esimerkiksi datan integrointi erilaisten heterogeenisten solmujen ja niistä saatujen tietojen välillä. (Elhadja, Salim ja Abdelhamid 2020)

Haaste IoV:ssa on myös suuri solmujen liikkuvuus. Ajoneuvot ovat liikkuvia objekteja. Tästä seuraavan suuren liikkuvuuden takia haasteeksi tulee se, että verkon solmut saadaan pidettyä kytkettyinä tarvittavalla tavalla. Vaikeaa on myös tarjota solmuille tarvittavia resursseja siis siinä suhteessa, että tietoa pystytään sekä lähettämään että vastaanottamaan reaaliaikaisesti, joka on juuri IoV:n ja ajoneuvojen tapauksessa erittäin tärkeää. IoV:n käyttöönoton myötä tulisi monia eri hyötyjä, mutta myös uhkia erityisesti turvallisuuden ja yksityisyyden suhteen. IoV on alttiina monille tietoturva- ja kyberhyökkäyksille. Tämä aiheuttaa sitten edelleen haittaa tietojen luottamuksellisuuden, yksityisyyden ja eheyden suhteen. Lisäksi vaarana on esimerkiksi tietojen katoamiset ja muut vastaavat ongelmat. Haasteena on siis se, että saadaan kehitettyä tavat, joilla IoV:sta saataisiin tehtyä tarpeeksi turvallinen ja luotettava ympäristö. IoV:n haasteita liittyy lisäksi muun muassa energiatehokkuuteen, ympäristösuojeluun ja IoV:n viestinnän standardointiin. Energiatehokkuuden ja ympäristönsuojelun suhteessa haasteena on esimerkiksi se, että kuinka vähentää verkon solmujen energiankulutusta siinä suhteessa, että verkon käyttöikää saataisiin pidennettyä. Lisäksi haasteena on myös liikenneonnettomuuksien vähentäminen ja sitä kautta edelleen niiden aiheuttaman ympäristön saastuttamisen vähentäminen ja välttäminen. Haasteena on myös, että miten IoV:lle saataisiin otettua käyttöön yhtenäisiä standardeja ja arkkitehtuureita, joita sillä ei nyt ole. (Elhadja, Salim ja Abdelhamid 2020)

Monet nykyajan ongelmat estävät siis IoV:n edelleen kehittämistä ja mukauttamista (Sakshi ym. 2021). Seuraavaksi lisää näistä haasteista, joista osaa tuli sivuttua jo edelläkin. Sakshi ym. (2021):n näkemyksen mukaan tämän hetken keskeisimmät IoV:n edistämistä estävät haasteet ovat seuraavat. IoV:n nykyiset haasteet liittyvät erityisesti big datan esikäsittelyyn, standardointiin, sopeutuvuuteen, verkkoyhteyksiin, skaalautuvuuteen, energiatehokkuuteen, infrastruktuuriin, yksityisyyteen ja turvallisuuteen. Big datan esikäsittelyn suhteen esiintyy

seuraavanlaisia haasteita. Ongelmaksi IoV:n kannalta voi koitua erilaisten valtavien tietojen siirtäminen ja kuljettaminen sen kautta, jotka sitten saattavat häiritä IoV-järjestelmää. Erityisesti tällaista valtavaa tiedonsiirtoa aiheutuisi esimerkiksi videoiden kuljettamisesta IoV:n kautta. Siksi tietojen valmistelun ja sen tehostamisen suhteen tulisikin pyrkiä kehittämään jonkinasteisia ratkaisuja ennakolta, että IoV:n mahdollisen käyttöönoton myötä tulevaisuudessa räjähdysmäisesti nouseva tiedon määrä ei kaataisi koko järjestelmää tai ettei aiheutuisi muita vastaavia ongelmia. Tällaisesta big datan esikäsittelystä voi olla myös muita hyötyjä IoV:n kannalta, sillä esimerkiksi muu, ilman viivettä tapahtuvaan tiedonsiirtoon ja tiedon levittämiseen kohdistuva, data-analyysi perustuu myös pitkälti tehokkaasti toteutettuun datan esikäsittelyyn. Lisäksi hyötynä voi olla se, että osataan tehdä paremmin sekä oikea-aikaisia että tietoisia päätöksiä. Tästä voi edelleen olla hyötyä erilaisissa kuljetusalaa koskevissa asioissa, kuten vaikka tietoturvallisuudessa ja liikenteen optimoimisessa. Haasteena edelleen big datan esikäsittelyn ratkaisemisen suhteessa on se, että esimerkiksi turvallisuussyistä johtuen todellisiin tietoihin voi olla vaikea päästä käsiksi. Lisäksi IoV on vielä vasta nousuaan tekevä tutkimuksen ala, joten siihen perustuva aineisto voi olla paikoin vähäistä ja hyvin hajanaista. Kuten edeltäkin kävi ilmi jo, IoV:n suhteen ei ole olemassa vielä mitään sen erityisempiä standardeja. Täten IoV:n suhteessa standardeja ei voi käyttää hyödyksi asioiden, kuten laitteisto- ja ohjelmointityyppien, yhteentoimivuuden ja esimerkiksi taajuuksien käsittelyssä. IoV:lle tulisikin tulevaisuudessa pyrkiä osoittamaan myös jonkinasteisia standardeja tai ainakin tämä vähintään helpottaisi erilaisia asioita ja toimia IoV:iin liittyen. Esimerkiksi standardointi estäisi kehitystyössä esiintyvää niin sanottua harhailua ja haarautumista ideoiden suhteen. Tosin positiivisena puolena on sitten taas tosin se, että standardien puuttuessa kehitys on joustavampaa. Standardointi vähentäisi myös luultavasti esimerkiksi viestintäjärjestelmien, protokollien syntaksin, datasemantiikan ja verkon käyttöönoton yhteentoimivuuden eroja IoV:ssa kauttaaltaan.

Verkkoyhteydet ja niiden skaalautuvuus on myös yksi keskeisistä IoV:n haasteista. Yksi isoista IoV:n toteuttamista rajoittavista sekoista liittyy juuri verkkoyhteyksiin. Haasteena on luoda nimenomaan sellainen internet-yhteys, joka pystyisi käsittelemään IoV:lle vaadittavalla tavalla verkon kuormitusta esimerkiksi liikenteen tiheyden suhteen, joka aiheuttaa vaihtelevaa haasteellista kuormitusta verkolle. Lisäksi IoV:n myötä muutenkin verkon kuormitus kasvaisi valtavasti ja esimerkiksi big datan tuotanto lisääntyisi, kuten edelläkin jo käsiteltiin.

Näistä syistä johtuen IoV tarvitsisi toimiakseen niin vahvan internet-yhteyden, että se pystyisi siis käsittelemään kaiken tämän juuri mainitun tarvittavalla tavalla. IoV-verkon tulisi olla tarpeeksi skaalautuva myös sen suhteen, että sitä voitaisiin parhaalla mahdollisella tavalla soveltaa myös syrjäisemmillä alueilla. Lisäksi Internet-yhteyden tulisi omata tarpeeksi alhainen latenssi eli viive, tarpeeksi korkea tiedonsiirtonopeus ja tarpeeksi hyvä skaalautuvuus vaihtelevan liikenteen määrän ja täten datatiheyden suhteen. Lisäksi myös verkon kuormitus tulisi saada hajautettua tai alennettua muuten jollain sopivalla tavalla vaadittavalle tasolle. Latenssi tulisi saada alhaiseksi myös ennen kaikkea turvallisuuden takaamiseksi. Erilaiset turvallisuuteen liittyvät tiedot, kuten muiden autojen sijainti, on välttämättä saatava lähetettyä mahdollisimman nopeasti, jottei minkäänlaisia törmäyksiä, kolareita ja muita vastaavia katastrofaalisia seurauksia pääse aiheutumaan. Erityisesti tietoturvan suhteen tämän viiveherkkyyden tapauksessa ongelmana on kuitenkin esimerkiksi myös seuraava. IoV:n reaaliaikaisuuteen liittyvät rajoitukset ja vaatimukset tekevät siitä haavoittuvan esimerkiksi palvelunestohyökkäyksille. Näin ollen myös reaaliaikaisten hyökkäysten havaitseminen on IoV:n kannalta kriittistä. IoV:n käyttöönoton mahdollistaisi käytännössä jo nyt nopeat internet-yhteydet ja niiden saatavuus. Samaan aikaan haasteena kuitenkin edelleen asian suhteen on myös resurssien vaikea saatavuus ja puute tarvittavista taajuuksista. Nämä sitten taas juuri nimenomaan estävät esimerkiksi internet-yhteyksien tarjoamisen täyden kapasiteetin kera. (Sakshi ym. 2021; Guevara ja Auat Cheein 2020)

IoV:ssa on myös vielä esimerkiksi erilaisia verkon siirtoon, yhteentoimivuuksiin ja reititysprotokolliin liittyviä ongelmia. Yksi haaste liittyy IoV-teknologian ja siihen vaadittavan infrastruktuurin sopeutumiskykyyn erilaisissa tilanteissa. Olennainen haaste IoV:ssa on siis tiedon jakaminen ja sen sekoittuminen. IoV:iin liittyvien asioiden omaksumiseen ja sopeutuvuuteen voi vaikuttaa vaihtelevuus monien eri tekijöiden, kuten esimerkiksi eri kulttuurien, tietosuojan, luottamuksen ja turvallisuuden, kesken. IoV:n sopeuttaminen, mukauttaminen, käyttöönotto ja siis siltä vaadittavan infrastruktuurin rakentaminen eri alueiden ja maiden kesken tuleekin vaatimaan massiivisia kustannuksia ja panostuksia. Tästä aiheutuu iso haaste. Samassa yhteydessä voidaankin havaita jälleen yksi IoV:n haaste eli infrastruktuurin toteuttaminen. Haasteena IoV-infrastruktuureiden rakentamisessa on myös se, että sen tulisi toimia käytännössäkin eli itse suorituksen yhteydessä. Infrastruktuuri tulisi kehittää myös siten, että samalla pidettäisiin mielessä IoV-teknologian soveltaminen. Kuten jo edelläkin tuli

ilmi, isoin ongelma infrastruktuureiden suhteen on kuitenkin ennen kaikkea niiden rakentamisesta ja mukauttamisesta aiheutuvat valtavat kustannukset. Lisäksi eroavuudet eri alueiden suhteen voi koitua ongelmaksi. Nämä infrastruktuurin haasteetkin tulisi siis jollain tavalla saada ratkaistua. Myös esimerkiksi langattomasta tiedonsiirrosta aiheutuu IoV:lle haaste esimerkiksi ajoneuvojen keskinäisen viestinnän suhteessa. Tälläinen viestintä voi tehdä verkon alttiiksi erilaisille valetietohyökkäyksille. Myös muun muassa erilaisten ajoneuvojen paikannusjärjestelmien suhteen voi syntyä haasteita. Esimerkiksi sateelliittipohjaisia paikannusjärjestelmiä ei välttämättä ole aina saatavissa esimerkiksi silloin, jos ajoneuvo kulkee vaikkapa tunnelin läpi. Tästä voi aiheutua edelleen sellainenkin ongelma, että järjestelmä altistuu mahdollisesti jälleen hyökkäyksille, kuten esto- ja huijaushyökkäyksille. (Sakshi ym. 2021; Guevara ja Auat Cheein 2020) Myöhemmin, tässä pro-gradussa, ratkaisuideoiden ohessa vielä lisää erilaisista tietoturvan haasteista ja erityisesti siihen kohdistuvista erilaisista uhkatekijöistä ja tietoturvahyökkäyksistä.

Kuten edelläkin tuli jo ilmi, energiatehokkuus on IoV:n haaste. Energiatehokkuuden haasteen ratkaiseminen on ensiarvoisen tärkeää IoV:n kannalta esimerkiksi seuraavista syistä. Energiatehokkuuden parantamisen kautta saadaan todennäköisesti ratkaistua seuraavanlaisia IoV:n toisiinsa liittyviä ominaisuuksia. Tällaisia ominaisuuksia ovat muun muassa verkkoyhteyksien käyttöikä ja energian ehtymättömyys reitittimissä, reunalaitteissa ja muissa vastaavissa laitteissa, joita käytetään IoV:n käyttöönoton varmistamisessa. Lisäksi energiatehokkaat IoV:n sovellukset, kuten älykkäät valaistusjärjestelmät, älykäs seuranta ja esimerkiksi liikenteen valvonta ovat mahdollisesti todella tärkeitä tekijöitä ajoneuvoverkkojen kehityksessä tulevaisuudessa. Edelleen, kuten jo aiemminkin sivuttiin, turvallisuus ja yksityisyys on keskeinen IoV:n haaste, johon liittyvät ongelmat tulisi ehdottamasti saada ratkaistua ennen IoV:n toimeenpanemista. Ennen kaikkea asiakkaiden turvallisuus, tietoturvallisuus ja yksityisyys on turvattava IoV:ssa. Turvallisuus ja yksityisyys tulisi varmistaa jonkinlaisin keinoin kaikilla IoV:n osa-alueilla. Pohdinnat asian suhteen jatkuvat edelleen. Monesti tutkijat ovat ehdottaneet esimerkiksi erilaisia todennusjärjestelmiä ratkaisuksi asian tiimoilta. Näillä ei kuitenkaan ole pystytty kaikkia verkon porsaanreikiä ja ongelmia havaitsemaan, joka on johtunut osittain myös haasteista ja ongelmista ei täysin toimivan verkkoyhteyden toteutuksen suhteen. Jonkinlainen ratkaisu tulisi siis keksiä sen suhteen, että saataisiin havaittua kaikki mahdolliset sekä aktiiviset että passiiviset tietoturvahyökkäykset ja muut vastaavat

haittatekijät. Lisäksi esimerkiksi myös erilaisten ajoneuvotietojen saatavuus, eheys ja todennus käyttäjille sekä pilvipalveluiden että muiden tapojen kautta olisi varmistettava. (Sakshi ym. 2021)

Yksi haaste voi liittyä myös esimerkiksi seuraavaan. IoV:n vaatimukset voivat olla monimutkaisia ja vaatimustasoltaan korkeita esimerkiksi autonomisten järjestelmien aiheuttavien epävarmuustekijöiden vuoksi. Tämän vuoksi perinteisesti käytetyt testausmenetelmät ja -tekniikat eivät välttämättä ole enää toteutettavissa IoV:n tapauksessa. Testauksen suhteenkin tulisi siis kehittää jonkinlaisia vaihtoehtoisia lähestymistapoja. Autonomisilla itseohjautuvilla ajoneuvoilla voi olla myös suuntautumiseen liittyviä haasteita. Esimerkiksi teillä tilanteet voivat olla hyvinkin dynaamisia ja vaihtelevia. Tiet voivat esimerkiksi poiketa alunperin suunnitellusta. Teillä voi esiintyä erilaisia poikkeamia, kuten rakennustyömaita, puuttuvia liikennemerkkejä, puuttuvia merkintöjä tai muuta vastaavaa. IoV:n haasteisiin liittyy myös erilaisia oikeudellisia tekijöitä. Haasteiksi voi tulla oikeudellisten asioiden ja autonomisten ajoneuvojen suhteessa esimerkiksi se, että kuka on vastuussa erilaisissa hätätilanteissa, törmäyksissä ja onnettomuuksissa. Lakeja voi siis joutua tarkistamaan tällaisten tapausten varalta. Haasteita voi muodostua autonomisten ajoneuvojen myötä myös erilaisiin moraalisiin ja eettisiin näkökohtiin liittyen. Suuri haaste voi olla esimerkiksi päätöksenteko erilaisissa hätätilanteissa. Tien päällä hätätilanteissa voi tulla eteen jopa tilanteita, joissa pitäisi tehdä moraalisia päätöksiä. Esimerkkinä voi olla tilanne, jossa pitäisi päättää matkustajien ja jalankulkijan hengen vaarantamisen väliltä. Eli joko törmäisi jalankulkijaan vaarantaen hänen henkensä tai sitten painaisi jarrua, jotta osuma jalankulkijaan vältettäisiin, mutta sitten taas puolestaan itse matkustajien henki saattaisi vaarantua. Lisäksi jo autonomisten ajoneuvojen kehittämisestä ja käyttöönotosta aiheutuu valtavia taloudellisia kustannuksia, mikä on myös haaste. Tämä on haaste myös seuraavassa suhteessa. Jotta autonomiset ajoneuvot saataisiin otettua käyttöön kunnolla, tulisi niiden teknologian olla tulevaisuudessa paljon edullisempaa. Tämä siksi, että niiden lopullisten hintojen tulisi olla sellaisella tasolla, että muillakin kuin pelkästään rikkaimmilla olisi varaa niitä ostaa. Yksi uhka autonomisten ajoneuvojen suhteen voi olla myös siis jopa ihmisten välisen eriarvoisuuden ja varallisuuden polarisoitumisen kasvu. Esimerkiksi suurella osalla väestöstä ei välttämättä ole mahdollisuutta hankkia teknisesti edistyksellistä autoa ja vielä myös siten, että mukaan tulisi kaikki vaadittavat turvavarusteet. Tämä voi puolestaan sitten eskaloitua jopa niin pitkälle, että alkaa ikään kuin uusi

luokkataistelu. Monet ihmiset eivät myöskään välttämättä pystyisi näin ollen sopeutumaan teknologian kehitykseen ja tämän johdosta sitten syrjäytyisivät myös sosiaalisesti. (Singh ja Baljit 2021; Arena, Pau ja Severino 2020)

4 Ratkaisuehdotuksia ja -ideoita IoV:n ongelmiin ja haasteisiin

Tässä luvussa tuodaan esille keskeisimpiä IoV:n haasteisiin löytyviä ratkaisuehdotuksia, ratkaisuideoita ja erilaisia tekniikoita, joilla IoV:n haasteita olisi potentiaalista ratkaista.

4.1 Lohkoketju

Lohkoketju (engl.Blockchain) on sekä hajautetun infrastruktuurin että hajautetun laskennan paradigma. Lohkoketjulle on ominaista, että se käyttää salattuja ketjutettuja lohkorakenteita sekä tietojen tallentamiseen että validointiin. Lohkoketjuteknologiassa käytetään lisäksi älykkäitä sopimuksia sekä tietojen käsittelyyn että ohjelmointiin ja konsensusalgoritmeja tietojen päivittämiseen ja luomiseen. Lohkoketjuteknologian lohkorakenteissa lohkot koostuvat erilaisista tapahtumista, jotka sitten validoidaan ja varmistetaan hajautetusti. Toisin sanoen lohkoketjun hallinta toteutuu useiden osallistujien kautta toisin kuin perinteisissä tietokannoissa, joita hallitaan yleensä vain pelkästään yhden organisaation toimesta. Yksi lohkoketjuteknologian tärkeistä ominaisuuksista on myös se, että sillä pystytään helposti sekä seuraamaan että tarkistamaan tietoja. Lohkoketjun toteuttamiseen verkossa on olemassa kolme eri tapaa, joita ovat yksityinen, konsortio ja julkinen. Yksityinen lohkoketjun toteutus tarkoittaa sitä, että sääntöjen ja solmujen ohjaus tapahtuu keskitetysti yhden organisaation toimesta. Lohkoketjun toteutuksessa konsortio tarkoittaa taas puolestaan sitä, että jokin tietty, samoja tavoitteita omaava, yritysten ryhmä toteuttaa solmujen ja niillä olevien sääntöjen hallinnan ja ohjaamisen. Julkiselle toteutukselle lohkoketjussa on taas ominaista sitten se, että mikä tahansa solmuista voi osallista johonkin toimintaan osana koko hallintaprosessia. Yleensä tavoitteena sillä, että lohkoketjua käytetään IoV:ssa, on verkon turvallisuuden parantaminen. (Queiroz ym. 2020)

IoV:n käyttöönoton myötä massiivinen määrä älykkäitä ajoneuvoja kommunikoisivat keskenään ja yrittäisivät myöskin usein päästä pilveen. Tästä puolestaan erittäin todennäköisesti aiheutuisi se, että keskitetyn pilvipalvelun käyttäminen sekä valtavaa datan tallennustilaa varten että liikenteen hallintaan miljardien eri solmujen välillä, olisi tehotonta IoV:n kan-

nalta. Tämän keskitetyn pilvipalvelun mahdollisen kaatumisen johdosta sitten voisi aiheutua koko IoV:n järjestelmäyhteyden tuhoutuminen. Lohkoketju tuo potentiaalisia ratkaisuja esimerkiksi juuri tämän asian suhteessa. Lohkoketju on siis ikään kuin luettelo tallennetuista tiedoista. Se koostuu lohkoista, joissa jokaisessa on yhdistetyt solmutiedot ja tämän lisäksi linkit aina sekä seuraaviin että edellisiin lohkoihin. Solmut voivat olla esimerkiksi RSU:ita tai ajoneuvoja. Eri solmut on lohkoketjun tapauksessa kytkettyinä erillisiin palvelimiin. Nämä eri palvelimet voivat tallentaa tietoja solmuista yksitellen sekä alilohkoina että yhdistettynä pääpilvipalvelimeen. Näin ollen lohkoketjuista on hyötynä esimerkiksi se, että ne lisäävät verkon turvallisuutta, vähentävät viestintäviiveitä ja tarjoavat todella ison tilan tietojen tallentamiseen. Näin ollen tästä kaikesta myös seuraisi se, että liikenne todennäköisesti yleisesti tehostuisi IoV:n tapauksessa. Lisäksi lohkoketju on yleisesti ottaen vahvin teknologia IoV:lla olevien erilaisten keskitettyjen organisaatio-ongelmien ratkaisemiseen ajoneuvoverkoissa. Tämä siksi, että lohkoketjuteknologian kautta pystytään mahdollistamaan todennäköisesti erilaisten ajoneuvotietojen reaaliaikainen kerääminen, käsittely ja tallentaminen hajautetusti. Lohkoketjun kautta pystytään myös hoitamaan kahden eri solmun välinen tapahtumien tallentaminen turvallisesti. (Fadhil ja Sarhan 2020)

Konsensusmekanismilla tarkoitetaan lohkoketjun tapauksessa tiivistetysti seuraavaa. Lohkoketjuteknologiassa konsensusmekanismeja käytetään siksi, että saataisiin luotua luottamus myös joidenkin epäluotettavien tahojen tai yksiköiden välille. Lohkoketjussa on monia eri konsensusmekanismeja. Näillä on jokaisella omat ainutlaatuiset algoritminsa ja sääntönsä. Niiden avulla muodostetaan vaatimuksia, joita eri entiteettien tai solmujen on noudatettava, jotta lohkoketjuun saataisiin sisällytettyä uusia lohkoja. Kyseisten konsensusmekanismien idea ja tavoite on siinä, että niiden avulla annetaan eri tahoille mahdollisuus sopia yhdestä kelvollisen lohkon versiosta siten, että läpinäkyvä ja johdonmukainen näkymä saadaan varmistettua. Tämä sitten yleensä lopulta ratkaisee ristiriidat ei niin luotettavien eri tahojen välillä. Älykkäällä sopimuksella puolestaan tarkoitetaan lohkoketjun tapauksessa seuraavaa. Älykäs sopimus koostuu skripteistä. Nämä skriptit sijaitsevat lohketjulla olevissa lohkoissa. Tarkoituksena älykkään sopimuksen täytäntöönpanolla lohketjussa on seuraava. Sen avulla pyritään usein luomaan itsenäinen mistään luotettavasta tahosta riippumaton järjestelmä. Tavoitteena on siis, että tällainen itsenäinen järjestelmä pystyy sitten itsenäisesti tarjoamaan johdonmukaisia ja tehokkaita palveluita. Konkreettisesti älykkäässä sopimuksessa on kyse

myös seuraavasta. Nämä edellä mainitut skriptit, jotka sijaitsevat lohkoissa, kykenevät suorittamaan jotain automaattisesti heti, kun esimerkiksi jotkin jo ennalta määritellyt säännöt täyttyvät. Lohkoketjun yhteydessä mainittavalla kryptografialla puolestaan taas tarkoitetaan seuraavaa. Lohkoketjuissa erilaisia kryptografisia tekniikoita käytetään yleensä esimerkiksi yksityisyyden, turvallisuuden ja nimettömyyden varmistamisessa. Yleensä kryptografiassa käytetään esimerkiksi lohkoketjun lohkoissa ainutlaatuisia hash-arvoja. Niillä lohkot saadaan yhdistettyä toisiinsa ja lohkoista tulee niin sanotusti muuttumattomia. Tällaisen menetelmän avulla saadaan usein varmistettua muun muassa tietojen eheys. Usein käytetty tekniikka kryptografiassa on myös digitaalinen allekirjoitus, jonka avulla saadaan usein taattua todennus ja kiistämättömyys. (Mollah ym. 2021)

4.1.1 Lohkoketjun edut, hyödyt, ongelmat, haasteet ja ratkaisut IoV:n suhteen

Lohkoketjutekniikka on yksi potentiaalinen keino tarjota runsas määrä mahdollisuuksia ja täten mahdollisesti myös ratkaisuja IoV:n eri haasteisiin ja skenaarioihin liityen. Lohkoketjun integroimisella IoV:hen pystytään kehittämään IoV:iin liittyvien järjestelmien toiminnan automaatiota ja suorituskykyä. Lisäksi lohkoketjutekniikan avulla pystytään parantamaan luottamusta, turvallisuutta ja täten myös yksityisyyttä IoV:ssä. Koska IoV:ssa jouduttaisiin käsittelemään massiivista määrää tietoa, lohkoketjuteknologian avulla olisi mahdollista yrittää ratkaista tätä ongelmakohtaa. Lohkoketjuteknologia tarjoaisi myös siis joustavuutta massiivisen tiedonkäsittelyn suhteessa. Sellainen IoV, joka olisi rakennettu lohkoketjuteknologian päälle, voisi kenties luoda uudenlaisen ekosysteemin sekä autoteollisuudelle että liikenteelle. Tällaisessa ekosysteemissä arvoja ja niiden vaihtamista voitaisiin sitten mahdollisesta hallita esimerkiksi tehokkaammin, muuttumattomasti, läpinäkyvästi ja ennen kaikkea turvallisesti. Toisin sanoen lohkoketjun integroimisesta IoV:n kanssa saattaisi luultavasti seurata se, että IoV parantuisi huomattavasti esimerkiksi tiedonsaannin, tehokkuuden ja turvallisuuden saralla. (Mollah ym. 2021; Tripathi, Abdul Ahad ja Sathiyanarayanan 2019)

Jos hieman tiivistetyssä muodossa selkeyttää asiaa, niin IoT:n teknologian avulla varmistetaan yleisesti muun muassa se, että kaupungeissa olevien liikennejärjestelmien kaikki elementit pystytään yhdistämään. Näin kyetään sitten taas edelleen luomaan hyvin yhdistetty ja kommunikoiva verkko eli IoV. Sitten, kun tähän vielä lisätään lohkoketjuteknologia mu-

kaan, voidaan luultavasti vielä parantaa entisestään IoV-verkostoa. IoV-verkostosta pystytään potentiaalisesti tekemään lohkoketjun avulla turvallisempi läpinäkyvä tietoväline, jossa myös muun muassa yksityisyyden suoja olisi otettu huomioon. Lohkoketjun avulla IoV:sta pystyttäisiin mahdollisesti tekemään lisäksi turvallisempi myös siinä mielessä, että IoV verkostoineen olisi sekä hajautettu että muuttumaton samanaikaisesti. (Tripathi, Abdul Ahad ja Sathiyanarayanan 2019)

Syitä sille, miksi lohkoketjuteknologia on yksi potentiaalisista ratkaisuista IoV:n kehittämiselle ja miksi lohkoketjua on alettu yrittää integroida osaksi IoV:tä, on olemassa muun muassa seuraavia. Lohkoketjun avulla on mahdollista toteuttaa hajautetut IoV-verkot. Hajauttaminen mainitaan yhdeksi lohkoketjun pääominaisuuksista. Hajautuksen avulla pystytään toteuttamaan IoV-verkkoihin hajautettuja kokonaisuuksia. Tällaisia kokonaisuuksia voivat olla esimerkiksi ihmiset, ajoneuvot tai tienvarsiyksiköt eli RSU:t. Edistystä on tässä suhteessa se, että nykyisen, pääasiallisesti keskitettyyn päätöksentekoon perustuvan, IoV-verkon toiminta ja sen periaatteet muuttuvat hajautetun mallin mukaiseksi. Nykyisen keskitetyn päätöksenteon sijaan tällaiset hajautetut kokonaisuudet pystyisivät hallitsemaan toimintaansa itsenäisesti. Täten IoV-verkon toiminta yksinkertaistuisi ja luultavasti tämä kaikki parantaisi myös käyttäjien kokemusta ajoneuvojen palveluista. Hajautettu lohkoketju tekisi myös mahdolliseksi tehokkaat ja nopeat tapahtumat. Lisäksi tiedon jakaminen tapahtuisi luotettavasti. Älykkäät sopimukset myös helpottaisivat maksutapahtumien ja transaktoiden automaattista suorittamista. Täten erilaiset transaktiot, kuten verot, vakuutukset, pysäköintimaksut ja muutkin maksut olisi mahdollista tehdä aikatehokkaasti. (Mollah ym. 2021; Tripathi, Abdul Ahad ja Sathiyanarayanan 2019)

Lohkoketjun avulla olisi luultavasti mahdollista torjua myös erilaisia tietoturvauhkia, kuten erilaisia keskeytyksiä ja pätkimisiä verkossa. Lisäksi erilaisia tietoturvahyökkäyksiä, kuten esimerkiksi saatavuushyökkäyksiä kyettäisiin luultavasti torjumaan lohkoketjun avulla. Tämä kaikki puolestaan mahdollistuisi luultavasti muun muassa sen takia, että lohkoketjun avulla pystytään mahdollistamaan sen replikaatio ja synkronointi kaikkien sellaisten vertaissolmujen välillä, jotka ovat kytkettyinä verkkoon. Tästä seikasta johtuen sitten taas puolestaan eri palvelut pystyisivät toimimaan katkeamattomasti, vaikka yksi tai useampi solmuista jotenkin vaarantuisi. Lisäksi tietoturvauhkia pystyttäisiin estämään lohkoketjuteknologialla

siksi, että yhteisten turvallisuus- ja yksityisominaisuuksien varmistamiseksi lohketjuteknologiassa käytetään nykyaikaisia salaustekniikoita. (Mollah ym. 2021)

Lohkoketjun avulla pystytään myös poistamaan pilvijärjestelmien riippuvuus tietojen hallinnasta ja tallentamisesta. Lohkoketju pystyy älykkään sopimuksen avulla mahdollistamaan myös seuraavan asian. Sen sijaan, että kolmannet osapuolet, kuten muun muassa ohjauskeskus, keskuspalvelupäällikkö, luotetut välittäjät ja ylläpitäjät, ylläpitäisivät ajoneuvopalveluita, lohkoketjuverkoston osallistujat pystyisivät itse ylläpitämään ajoneuvopalveluita. Tämä sitten taas edelleen esimerkiksi vähentäisi erilaisia ajoneuvopalveluista aiheutuvia käyttökustannuksia. Lohkoketjun avulla olisi myös potentiaalista tehdä IoV-palvelut muuttumattomaksi. Tämä tarkoittaa sitä, että lohkoketjussa olevat lohkot ylläpitävät ketjua. Tämän kautta ne voivat sitten muodostaan yhteyden toisiinsa kunkin lohkotietueen hash -arvojen välityksellä. Tämän muuttumattomuuden avulla pystyttäisiin estämään tiedon muokkaaminen ja peukalointi. Lisäksi muuttumattomuuden avulla tiedot pystyttäisiin myös tarkastamaan tarkasti ja lisäksi erilaisten ennalta määriteltyjen komentosarjojen ja sääntöjen täytäntöönpano ja käyttöönottaminen mahdollistuisi. (Mollah ym. 2021)

Lisäksi lohkoketjuteknologian kautta pystytään mahdollistamaan sekä peer-to-peer (p2p) -kaupankäynti että jakaminen ja viestintä kahden kokonaisuuden välillä. Toisin sanoen p2p-verkon avulla mahdollistuu se, että sekä palvelun tarjoajat että palvelun pyytäjät pystyvät muodostamaan suoraan yhteyden keskenään. Tämä on sitten taas hyödyllinen ominaisuus IoV:n kannalta, kun esimerkiksi tietojen jakaminen RSU:iden ja ajoneuvojen välillä on mahdollista tehdä turvallisesti. Lisäksi, kun kommunikointi tapahtuu suoraan ilman minkäänlaisia välittäjiä, johtaa tämä edelleen myös luultavasti alhaisen latenssin omaaviin ajoneuvopalveluihin. Tämä olisi myös IoV-verkon kannalta erinomainen juttu. IoV:n tavaksi mainitaan myös sellaisten heterogeenisten kokonaisuuksien yhdistäminen, jotka eivät ehkä ihan täysin luota toisiinsa. Myös tähän seikkaan pystyttäisiin puuttumaan lohkoketjun konsensusmekanismien avulla. Konsensuksen avulla lohkoketjuteknologialla on mahdollista luoda siis syvä luottamus jopa tällaisten epäluotettavien kokonaisuuksien keskuudessa. Toinen lohkoketjun keino tällaisessa luottamuksen parantamisessa on älykäs sopimus. Älykkään sopimuksen ja sen komentosarjojen avulla pystytään luultavasti saavuttamaan sekä automaattinen ja itsenäinen järjestelmä että luottamus sellaisissa tilanteissa, joissa päätöksiä joudutaan tekemään

ilman luotettavaa tahoa. Lisäksi nimenomaan julkista lohkoketjua käytettäessä myös IoV:n läpinäkyvyys luultavasti kasvaisi. Tämä siksi, että julkinen lohkoketju mahdollistaa täydellisen pääsyn lohkoketjuun tallennettuihin tietoihin, sillä se on yleensä avoin kaikille tahoille. (Mollah ym. 2021)

IoV:n avulla olisi myös mahdollista kerätä erilaista ajoneuvoon liittyvää tietoa, kuten esimerkiksi tietoa liittyen kuljettajan käyttäytymiseen. Tällaista tietoa voisivat sitten käyttää hyväksi esimerkiksi vakuutusyhtiöt. Erittäin tärkeää tällaisissa tilanteissa olisi, että kerätty tieto olisi eheää. Lohkoketjun avulla saataisiin luotua tällaisiinkin tilanteisiin ratkaisu lohkoketjuteknologian muuttumattoman luonteen avulla. Täten kyseisenlaista tietoa pystyttäisiin mahdollisesti tarjoamaan luotettavasti ja muuttumattomasti erilaisia tilanteita, kuten esimerkiksi juuri vakuutuskorvauksien arviointeja, varten. Toisin sanoen tieto säilyisi siis lohketjuteknologian ansiosta luultavasti eheänä. Edelleen samojen lohkoketjun ominaispiirteiden avulla myös tietojen jakamista sekä itseohjautuvien ajoneuvojen välillä että ajoneuvojen ja tien välillä pystyttäisiin parantamaan. Hajautettu luonne edesauttaa tällaisissa tilanteissa siten, että IoV:n eri kokonaisuudet pystyvät pitämään kirjaa koko IoV-järjestelmästä. Tämä puolestaan parantaa edelleen koko IoV-järjestelmän vikasietoisuutta ja joustavuutta. Lisäksi lohkoketjun ansiosta edellä mainitun kaltaiset tiedonvälitykset sekä ajoneuvojen itsenä että niiden ja ympäristön välillä olisivat kryptografisesti suojattuja ja allekirjoitettuja omistajan julkisella avaimella. Tämä sitten edelleen pitäisi huolen siitä, että kyseisenlainen tieto olisi eheää. (Tripathi, Abdul Ahad ja Sathiyanarayanan 2019)

Itseohjautuvien ajoneuvojen ja erilaisen automaation lisääntyessä liikenneturvallisuuden ylläpitämisestä tulisi arvoitus siinä mielessä, että IoV-järjestelmät ovat alttiina erilaisille uhkille. Tällaisia uhkia voivat olla esimerkiksi erilaiset hakkeroinnit ja tietovarkaudet. Lohkoketjuteknologialla mahdollisesti saataisiin luotua tällaiseenkin tilanteeseen ratkaisu. Kuten edellä tuli jo ilmi tämäkin, lohkoketjuteknologia on luonteeltaan muuttumaton ja hajautettu. Tämä sitten taas puolestaan toisi IoV:n suhteen sellaisen edun, että IoV-järjestelmästä voisi tulla tarpeeksi vikasietoinen ja tätä kautta sitten taas edelleen turvallisempi. Lohkoketjuteknologian ominaispiirteisiin kuuluu myös korruptoimattomuus. Tämä puolestaan vaikeuttaisi liikennesääntöjä ja muitakin sääntöjä rikkovien tahojen väärentää tietoja IoV:ssa. Toinen etu lohkoketjusta saman asian suhteen olisi se, että pystyttäisiin mahdollistamaan yk-

silöllinen tunnistaminen. Lohkoketjuteknologian ansiosta yksilöllisiä tunnuksia pystyttäisiin liittämään IoV-järjestelmien isompiin kokonaisuuksiin. Tämän kautta sitten taas edelleen erilaisia rikkomuksia liikenteessä pystyttäisiin mahdollisesti seuraamaan ja tunnistamaan. Toisin sanoen lohkoketjuteknologian avulla liikennesääntöjen noudattamisen valvonta tehostuisi IoV:ssä. (Tripathi, Abdul Ahad ja Sathiyanarayanan 2019)

Tripathi, Abdul Ahad ja Sathiyanarayanan (2019) luettelevat konferenssissaan muun muassa seuraavanlaisia tietoturvauhkia IoV:ssa. Yhdeksi uhkaksi mainitaan vaarantunut tietoturva luvattoman pääsyn osalta. Vaarana on siis, että IoV:n tietoja ja tätä kautta myös ajoneuvoja hakkeroitaisiin jollain tavalla. Uhkaksi mainitaan myös tietoturvaan kohdistuva hyökkäys nimeltään palvelunesto (engl.Denial of Service) eli lyhennettynä DoS. Eli toisin sanoen kyseessä on seuraavanlainen tietoturvaan kohdistuva hyökkäys. Siinä vaikutetaan laittomilla tavoilla tai toimilla haitallisesti palvelun sekä laatuun että tätä kautta myös luotettavuuteen. Yksi tietoturvauhka on taas puolestaan tiedonsiirto-ongelmat eli erilaiset luvattomaan tietojen käyttöön ja tietojen menetykseen liittyvät asiat. Erilaisiin antureihin ja sensoreihin liittyvät ongelmat ovat myös yksi uhka. Eli tässä on kyse erilaisista IoV-verkoston kattavuuteen ja kantavuuteen liittyvistä ongelmista. Myös IoT:iin liittyvät ongelmat ovat usein IoV:inkin ongelmia, koska IoV on osa IoT:ia. Eli myös IoT:n verkkoturvallisuus ja siihen kohdistuvat hakkeroinnit ovat uhka myös IoV:lle. Tietojen tallentaminen ja jakaminen IoV-verkossa on myös yksi uhka. Tällaisia tietoja voidaan salakuunnella tai sitten esimerkiksi niiden säilytys voi olla jotenkin laadullisesti riittämätöntä.

Mahdollisia tietoturvauhkia IoV:lle luokitellaan myös IoV:lta vaadittavien tietoturvallisuusvaatimusten kautta. Näitä IoV:n tietoturvalta vaadittavia ominaisuuksia on kyseisessä tekstissä luokiteltu mahdollisiksi tietoturvahyökkäyksen ja tietoturvauhkien kohteiksi. IoV:lta vaaditaan ensinnäkin erilaista saatavuutta ja saavutettavuutta. Uhkana on, että tietoturvahyökkäykset pääsevät vaikuttamaan IoV:n käytettävyyteen esimerkiksi siten, että IoV-verkon lähetystehoa ja kaistanleveyttä häiritään tai että nämä saadaan tehtyä täysin käyttökelvottamaksi. Yksi IoV:lta vaadituista ominaisuuksista on myös tietojen eheys. Uhkana eheyden suhteen voi olla esimerkiksi viestien ja niiden sisällön peukaloiminen, jolla voidaan huonolla tavalla vaikuttaa myös viestin vastaanottajan vastauksiin ja päätöksiin. Tätä kautta edelleen taas puolestaan kenties koko IoV saattaisi olla uhattuna. IoV:lta vaaditaan myös todennettavuut-

ta. Uhkana todennettavuuden tapauksessa on esimerkiksi erilaiset henkilöllisyyksien väärennökset. IoV:n tulisi olla myös luotettava ja esimerkiksi hyökkäykset, jotka vaarantaisivat järjestelmää käyttävien tahojen yksityisyyttä, on uhka. Reitityksen tulisi olla myös kunnossa IoV:n verkostossa. Reitityksen suhteen on vaarana erilaiset tietoturvauhkat, kuten esimerkiksi sellaiset hyökkäykset, joilla väärennetään viestien alkuperäistä reittiä tai sisältöä. Tässä suhteessa uhkana voi olla esimerkiksi myös viestien salakuuntelu. (Abbas ym. 2021)

Lisäksi IoV:lta vaadittavia erilaisia tietojen yksityisyyteen liittyviä tietosuojavaatimuksia on muun muassa lueteltu seuraavanlaisia. Yksi on vaatimus ajoneuvotietojen tietosuojasta. Ajoneuvotietoja voivat olla esimerkiksi ajoneuvon kunnosta kertovat tiedot, rekisteröintitiedot ja sellainen tieto, jota kyseessä oleva ajoneuvo on levittänyt ja tuottanut. Sovelluksen purkamisen aikana ajoneuvon tiedot useimmiten siirretään tehokkaampiin yksiköihin käsiteltäväksi tarkemmin. Käsittelyä varten purettavat tiedot tarvitsevat riittävän tietosuojan, jottei hyökkääjät tässä kohdin pääse esimerkiksi sieppaamaan yksityisiä tietoja. Vaatimuksena yksityisyyteen perustuville tiedoille on myös henkilötietojen tietosuoja. IoV-verkoissa olevia yksityisiä henkilötietoja, kuten autojen omistajien ja kuljettajien ajokorttiin liittyviä tietoja tai heidän nimiään, ei ole sallittua paljastaa. Vastaavasti esimerkiksi ajoneuvojen omistajien tai kuljettajien tulisi olla myös tietoisia siitä, että millaisia henkilötietoja heistä tullaan tallentamaan IoV-palveluihin ja IoV-järjestelmiin. Pahimmassa tapauksessa hyökkääjät voivat päästä hyödyntämään tällaisia yksityisyyteen liittyviä henkilötietoja, jos suojausta ei toteuta tarpeeksi hyvin. Tietojen yksityisyyteen liittyväksi vaatimukseksi on mainittu myös sijaintitietojen tietosuoja. IoV:n tapauksessa tällainen vaatimus liittyy esimerkiksi ajoneuvojen sijaintitietojen ja kohdereittien salassa pitämiseen. Tällaisetkin tiedot tulisi pyrkiä säilyttämään turvallisesti, jottei näitä voida käyttää hyväksi erilaisiin hyökkäyksiin. (Osibo ym. 2021)

Erimuotoisia tietoturvahyökkäyksiä on myös tunnistettu. Nämä ovat edelleen olemmassa olevia uhkia myös IoV:n tietoturvan tapauksessa. Esimerkkeinä mainittakoon sybil-hyökkäys, GPS-petoshyökkäys tai GPS-huijaushyökkäys, naamioitumishyökkäys, madonreikähyökkäys ja toistohyökkäys. Toistohyökkäyksessä on kyse siitä, että rikollinen toistaa verkossa aiemmin jo lähetettyjä vanhoja viestejä. Tämä tehdään, jotta muita verkon solmuja pystyttäisiin peittämään ja korkean prioriteetin omaavat viestit saataisiin pudotettua viestijonosta. Tällainen hyökkäys saattaa lisätä esimerkiksi kohteena olevan järjestelmän kaistanleveydestä ai-

heutuvia kustannuksia. GPS-petoshyökkäyksessä tai GPS-huijaushyökkäyksessä on taas kyse siitä, että GPS-signaaleja siepataan tai manipuloidaan. Näin sitten johdetaan esimerkiksi ajoneuvojen kuljettajia harjaan. Tällä voi sitten luontaisesti olla erilaisia vahingollisia seurauksia. Naamioitumishyökkäyksessä puolestaan jokin solmu esittää olevansa jokin toinen solmu varastamalla kyseessä olevalla solmulla olevan henkilöllisyyden. Näin esimerkiksi väärennetyn identiteetin omaava solmu voi päästä nauttimaan kyseessä olevalla identiteetillä olevista käyttöoikeuksista. Madonreikähyökkäys on sellainen, jossa kaksi rikollista tahoa eli tässä tapauksessa kaksi niin sanotusti haitallista ajoneuvoa luovat välilleen yksityisen tunnelin. Tätä luotua tunnelia käytetään sitten siepatun tiedon välitykseen haitallisten tahojen välillä. (Abbas ym. 2021; Osibo ym. 2021)

Sybil-hyökkäys on puolestaan sellainen hyökkäys, jossa hyökkääjä luo yhteen verkossa olevaan solmuun useamman identiteetin. Eli IoV-verkon tapauksessa, vaikka kyseessä olisi todellisuudessa yksi ajoneuvo tietoineen, ulospäin saadaan näyttämään siltä, että tiellä olisi useampi ajoneuvo identiteetteineen ja tietoineen. Näin ulkopuolisille välitetään esimerkiksi väärää tietoa liikenteen tiheydestä. Näin pyritään vaikuttamaan esimerkiksi muiden ajoneuvojen reittivalintoihin. Yksi tietoturvahyökkäyksen muoto voi olla salakuunteluhyökkäys. Salakuuntelusta on kyse siinä kohtaa, kun hyökkääjät onnistuvat pääsemään luvatta käsiksi jonkin ajoneuvon tai ajoneuvojen viestintään tai viesteihin ylipäätänsä. Tällainen hyökkäys pääse yleensä tapahtumaan esimerkiksi huonosti suojatuissa ajoneuvoverkoissa, joissa hyökkääjät onnistuvat sieppaamaan haltuunsa erilaisia tietoja esimerkiksi joko lähetettyjä tai vastaanotettuja sellaisia. Tällainen salakuuntelu on yleensä luonteeltaan passiivinen hyökkäys, jossa tietoja ei usein sinänsä mitenkään muuteta tai häiritä. Tällaisen hyökkäyksen havaitseminen voikin olla erityisen vaikeaa. Tietoturvahyökkäys voi olla myös eräänlainen Man-in-the-Middle -hyökkäys. Siinä hyökkääjät jollain tavalla sieppaavat kahden osapuolen välisen viestinnän IoV:n viestintätyypeissä, kuten esimerkiksi V2I:ssa, V2P:ssa tai V2V:ssa. Tässä hyökkäyksessä hyökkääjä on ikään kuin keskellä erillisten osapuolten viestintää ja esimerkiksi kaappaa, tarkkailee ja hallitsee salaa kyseistä viestintää. Hyökkääjät voivat esimerkiksi huijata toista ajoneuvoa, joka on vastaanottavana osapuolena. Tämä esimerkiksi saa sitten vastaanottavan osapuolen myös toimimaan hyökkääjän lähettämän viestinnän perusteella ja tästä voi sitten aiheutua haittaa. Lisäksi hyökkäykset voivat olla luonteeltaan myös jonkin asteisia häiriöitä. Hyökkääjät voivat esimerkiksi häiritä ja pahimmassa tapauksessa estää ko-

konaan palveluita toimimasta. Tämä voi tapahtua esimerkiksi ylikuormittamalla järjestelmä pitäen viestintävälineet erittäin kiireisinä jatkuvalla tietoliikenteellä. (Abbas ym. 2021; Osibo ym. 2021)

Edellä mainittuihin tietoturvahyökkäyksiin liittyen on ehdotettu muun muassa seuraavanlaisia ratkaisuideoita. Sybil-hyökkäyksen torjumiseksi on ehdotettu, että voitaisiin käyttää esimerkiksi ryhmäallekirjoituksia, istuntoavaimen varmenteita, tapahtumapohjaista mainejärjestelmää tai esimerkiksi digitaalisia jalanjälkiä. GPS-petoshyökkäyksessä tai GPS-huijaushyökkäyksessä ja sen torjumisessa voitaisiin käyttää puolestaan menetelmää, kuten kuollutta laskentaa tai sitten jonkinlaisia allekirjoituspohjaisia mekanismeja. Naamioitusmishyökkäyksien suhteen torjuvana ratkaisuna voisi sitten taas olla ehkä esimerkiksi digitaalisten varmenteiden tai henkilöllisyyteen perustuvien kryptografioiden käyttö. Madonreikähyökkäyksien torjuntaan voisi toimia maantieteelliset hihnat -menetelmä ja toistohyökkäysten torjuntaan puolestaan aikaleimojen käyttäminen. (Abbas ym. 2021)

Edellä mainitut tietoturvauhkat ovat myös samalla yksi, kuten jo edellä on tullut ilmi, IoV-järjestelmän keskeisimpiä haasteita tällä hetkellä. Tällaiset tietoturvauhat ovat edelleen jaettavissa sovellustason, viestintätason ja fyysisen tason haasteisiin. Viestintätasolla haasteita on muun muassa latenssin ja energiatehokkuuden alalla eli tarkemmin sanottuna esimerkiksi verkkoyhteyksien ja virrankulutuksen saralla. Fyysisellä tasolla taas puolestaan haasteita on luvattoman tietojen käytön ja muiden laittomien toimien suhteen, jotka ovat uhka tietoturvallisuudella ja tätä kautta sitten myös palvelun laadulle ja luotettavuudelle. Sovellustasolla ongelmia voi syntyä pilvipalveluihin ja eri sovelluksiin liittyen. Tämä sitten puolestaan voi johtaa edelleen tietojen katoamiseen ja laittomiin muokkauksiin. (Tripathi, Abdul Ahad ja Sathiyanarayanan 2019)

Näistä asioista on mainittu jo edelläkin, mutta seuraavaksi vielä tarkemmin lohkoketjuteknologian ja sen ominaisuuksien tarjoamista potentiaalisista ratkaisuista erityisesti IoV:n tietoturvauhkiin. Yksi lohketjun tarjoamista mahdollisista ratkaisuista liittyy konsensukseen eli toisin sanoen yhteisymmärrykseen. Tämä tarkoittaa sitä, että mikään yksittäinen taho ei voi yksinään tehdä päätöksiä ja hyväksyä toimenpiteitä ja tapahtumia IoV:ssa. Sen sijaan kaikki osallistujat yhdessä osallistuvat päätösten tekemiseen ja erilaisten toimenpiteiden hyväksymiseen. Tämä taas vaikuttaa mahdollisesti IoV:iin siten, että huijaukset vähenevät tai pois-

tuvat kokonaan. Lisäksi IoV:ssa tapahtuvista toimenpiteistä, ratkaisuista ja päätöksistä tulee tehokkaampia, nopeampia, avoimempia ja luotettavampia. Ratkaisuja tulisi myös läpinäkyvyyteen, aikaleimattuihin tietotietueisiin ja turvallisuuteen liittyen jäljempänä mainittavalla tavalla. Lohkoketjuteknologian tuoma läpinäkyvyys lisäisi luottamusta IoV:n eri sidosryhmien välillä, kun eri tapahtumat ja tietueet olisivat kaikkien nähtävillä. Lohkoketjuteknologiassa myös kaikki lohkot aikaleimataan aina ensin. Vasta sen jälkeen ne lisätään sitten lohkoketjuun. Tietueiden tiedot olisivat siis aikaleimattuja, josta sitten puolestaan taas aiheutuisi edelleen se, että tapahtumat olisivat nähtävillä oikeassa järjestyksessä IoV-järjestelmässä. Lohkoketjun avulla turvallisuus lisääntyisi myös esimerkiksi yksityisyyden osalta, sillä lohkoketjun kryptografiset toiminnot varmistaisivat luultavasti turvallisuuden, läpinäkyvyyden ja yksityisyyden samanaikaisesti. (Tripathi, Abdul Ahad ja Sathiyanarayanan 2019)

Lisäksi lohketjun ominaisuuksien avulla tietojen ja tietueiden tunnistus voidaan suojata hyvin. Lohkoketjun mukanaan tuoma ratkaisu olisi myös luultavasti se, että verkon entiteetit eli kokonaisuudet voisivat mahdollisesti olla kaikkien osallistujien nähtävillä, mutta kuitenkin siten, että kenenkään henkilökohtaisia tietoja ei paljastettaisi. Lohkoketjuteknologian avulla myös jäljitettävyyteen liittyen saataisiin ehkä ratkaisu, koska lohkoketjun avulla, kuten edellä jo mainittiin, tietueet olisivat aikaleimattuja ja niihin olisi kirjattuna myös tunniste. Täten eri asioita ja tapahtumia pystyttäisiin jäljittämään kronologisessa järjestyksessä. Ratkaisuja saataisiin edelleen myös todennäköisesti pseudonymiteettiin liittyen. Tämä siksi, että lohkoketju lisää tietueiden läpinäkyvyyttä ja lisäksi sen avulla pystyttäisiin käyttämään käyttäjien tunnistamisessa digitaalista allekirjoitusta ja käyttäjätunnusta. Eli IoV:n kannalta ratkaisu tulisi siihen, että esimerkiksi ajoneuvot ja niihin liittyvä tieto olisi mahdollista tunnistaa esimerkiksi julkisella avaimella ja käyttäjätunnuksella. Ratkaisuja tulisi potentiaalisesti IoV:n kannalta myös siihen, että tietojen todellisesta alkuperästä säilyisi todisteet ja tieto olisi täten muutenkin eheää. Sellaista tietoa, joka olisi keretty kirjata jo IoV:iin ei voisi myöskään ihan tuosta vain kieltää ja poistaa. Kuten myös monta kertaa edelläkin on tullut jo ilmi, lohketjun kautta tulisi ratkaisuja myös sen tarjoaman muuttumattomuuden ja hajautetun luonteen kautta. Hajautetusta luonteesta ainakin tulisi se hyöty, että IoV:ssa ei olisi pelkästään yhtä hallitsevaa tahoa ja kolmannet osapuolet eivät olisi mukana. Sen sijaan paino olisi enemmänkin käyttäjien yhteisessä hallinnassa. Näin IoV-järjestelmä myös luultavasti toimisi sulavammin ja ei olisi niin altis erilaisille keskeytyksille tai muille häiriöille. Muut-

tumattomuuden suhteen taas jokaisella IoV:n kokonaisuudella voi olla hallinnassaan jostain tietueesta kopio digitaalisessa muodossa. Tämä sitten voisi tuoda IoV:n suhteessa ratkaisuja vikasietoisuuden, korruptoituneisuuden, organisoituneisuuden ja läpinäkyvyyden suhteen. (Tripathi, Abdul Ahad ja Sathiyanarayanan 2019)

Vielä yhteenvetäen edeltävää. Lohketjun IoV:iin integroimisen kautta mahdollisuuksia olisi monia. IoV-järjestelmän yhteentoimivuus, tietoturva, yksityisyys, jäljitettävyys ja luotettavuus luultavasti kehittyisi. Lisäksi erilaiset autonomiset vuorovaikutukset, kuten maksutapahtumat ja kommunikointi ajoneuvojen välillä paranisi, kun kolmannet osapuolet eivät tulisi väliin. Lisäksi myös järjestelmien keskinäisen kommunikoinnin automaatio, ilman ihmisten väliintulemista, olisi luultavasti paremmin toteutettavissa. Myös erilaisten ajoneuvopalveluiden laatu, liitettävyys, luotettavuus ja esimerkiksi sovellustuki mahdollisesti paranisi paljonkin.(Tripathi, Abdul Ahad ja Sathiyanarayanan 2019)

Kuitenkin edelleen lohkoketjunkin osalta on useita ongelmia, jotka olisi saatava ratkaistua ennen lohketjuteknologian integroimista osaksi IoV:ia. Yksi ongelmatekijä on juuri, kuten edelläkin tuli jo esille, tietoturvan haavoittuvuus ja alttius erilaisille uhkille. Vaikka sinänsä lohketju tarjoaisikin potentiaalisia ratkaisuja tässäkin suhteessa, on mahdollista, että lohkoketjun mukanaan tuomat ominaisuudet muun muassa tietojen ja viestien salaukseen, valtuutukseen ja niiden todentamiseen liittyen eivät välttämättä kaikesta huolimatta toimisikaan IoV:ssa. Täten turvallisuus voi sen sijaan, että se parantuisi, puolestaan vaan heiketä. Lohketjun käyttäminen tarjoaisi kyllä potentiaalisia mekanismeja tietosuojan tarjoamiseen, mutta silti voi olla, että aiheutuisi kaikesta huolimatta vielä jonkin asteisia tietosuojavuotoja. Ongelmana ovat myös erilaiset IoV-järjestelmään liittyvät resurssirajoitukset. Lohkoketjuteknologian käyttöönotto edellyttäisi suurta laskentatehoa ja energiaa kuluisi huomattavasti enemmän. Lisäksi järjestelmissä ja laitteissa on oma rajallinen kapasiteettinsa prosessoinnin ja tallennustilan suhteen, joten tästäkin voi aiheutua ongelma. Lisäksi myös IoV-verkon katkeamattomuus ja vakaus tulisi saada niin varmalle tasolle, että lohkoketjun käyttöönottaminen olisi konkreettisesti edes mahdollista. Myös siis IoV-verkon luotettavuus sen korkean käytettävyyden, oikea-aikaisten tapahtumien ja yleensäkin tehokkuuden suhteen tulisi saada ensin riittävän varmalle tasolle. Lohkoketju ei myöskään ole sen tarjoamista potentiaalisista ratkaisumahdollisuuksista huolimatta vielä sellainen tekniikka, joka olisi laajalti hyväksytty

käyttöönotettavaksi. Ongelmaksi tässä suhteessa tulee esimerkiksi erilaiset lait, joiden kohdalla on paljon myös maakohtaista vaihtelua. Lohkoketjun toteutuskin ja laaja käyttöönotto on siis vielä edelleen ikään kuin vasta tulevaisuudessa häämöttävä tavoite. Tässäkin suhteessa lohkoketjun luotettavuus on kyseenalaista. Myös skaalautuvuus on ratkaisematta oleva ongelma. Eli toisin sanoen ongelma on IoV:n myötä käsiteltäväksi tuleva massiivinen tietomäärä ja sen toimivuus ja katkeamattomuus käytettävien järjestelmien ja laitteiden suhteen. Lohkoketju tarjoaa myös sinänsä teknologiana ratkaisun IoV:n käyttöönoton myötä kasvavaan tehon ja energian tarpeeseen ja kulutukseen. Kuitenkin lohkoketjun sisäisestikin löytyy vielä puutteita täysin kestävien energiatehokkaiden ratkaisujen suhteessa. IoV-järjestelmän käyttöönoton myötä kerättävä massiivinen datamäärä olisi myös todennäköisesti todella vaihtelevaa muodoltaan. Täten eri muodoissa tulevaa tietoa pitäisi saada jotenkin muunnettua yhtenäisempään yleisesti hyväksyttävissä olevaan muotoon. Lisäksi lohkoketjuteknologian ammattilaisista vallitsee runsas pula. IoV:n käyttöönotto ja sen toimivuus vaatii myös tehokasta, toimivaa ja katkeamatonta verkkoyhteyttä. Jokaisella alueella asia ei ole näin ja tässä suhteessa aiheutuu sitten taas haasteita IoV:n toteuttamiselle. (Tripathi, Abdul Ahad ja Sathiyanarayanan 2019)

4.2 5G

5G-verkko on nykyisen 4G-verkon jälkeen tuleva uuden sukupolven verkko. 5G-verkko on alkanut syntyä vuonna 2016. Yksi sen tavoitteista on ollut saavuttaa alhaisen latenssin omaava tiedonsiirto. Lisäksi 5G-verkon vankka infrastruktuuri mahdollistaisi huomattavasti aikaisempaa nopeammat latausnopeudet.(Khan ja Chowdhury 2021)

4.2.1 5G ja sen edut ja hyödyt IoV:lle

IoT-palvelujen perustaso on ollut periaatteessa mahdollista saavuttaa jo aikaisemman 4G-mobiiliteknologian avulla, mutta silti sillä on ollut vielä monia rajoituksia. Uuden sukupolven 5G-mobiiliteknologia on tekemässä tuloaan. 5G on noususssa oleva teknologia, joka tulee lisäämään verkkojen lähetysnopeutta merkittävällä tavalla. 5G:n avulla on erittäin todennäköistä, että 4G:n puutteet ja rajoitukset saataisiin vihdoin poistettua. 5G tarjoaisi siis täysin uudenlaisia mahdollisuuksia esimerkiksi älykkäille kaupungeille ja niissä toimiville

verkkoyhteyksille. Jos asiaa ajattelee IoV:n verkkoyhteyksien suhteen, 5G on yksi suurista potentiaalisista ratkaisuista myös IoV:n suhteen. 5G tarjoaisi myös älykkäille liikennejärjestelmille eli ITS:lle mahdollisuuden integroitua älykkäiden kaupunkien verkkojen ja järjestelmien kanssa. Tämä mahdollistuisi siten, että 5G:n avulla olisi mahdollista ylläpitää verkkoa kaikkialla ja sallia massiivinen määrä samanaikaisia yhteyksiä. 5G:n avulla tulee olemaan mahdollista ylläpitää verkkojen yhteyksiä koko ajan katkeamattomasti joka paikassa. Tämä tarkoittaa sitä, että kaikki verkon laitteet on mahdollista yhdistää. Tämä tarkoittaa myös yleisesti, mutta juuri tässä tapauksessa erityisesti IoV -verkkojen kannalta, seuraavaa. IoV-verkot vaativat toimiakseen sen, että määrältään massiivisten samanaikaisten yhteyksien ylläpitäminen mahdollistuu. Lisäksi vaaditaan myös erityisesti se, että verkkojen yhteyksien ylläpitäminen on toimivaa ja katkeamatonta myös erityisesti korkean liikkuvuuden tilanteissa ja tiheästi asutuissa paikoissa. 5G toisi IoV:n kannalta mahdollisesti ratkaisun tällaisiin ongelmiin. 5G-tekniikka tulee olemaan siis iso tekijä älykkäiden kaupunkien ja ITS:n edistämisessä. Näin ollen 5G tulee edelleen olemaan suurena mahdollistajana sekä IoT:n että edelleen IoV:n suhteen. 5G:n avulla tulee olemaan mahdollista yhdistää massiivinen määrä erilaisia laitteita ja antureita tiukkojen siirto- ja energiatehokkuusrajoitteiden kera. Lisäksi alhainen latenssi ja massiivinen datan määrä ovat 5G-verkkojen ominaispiirteitä, mikä on iso mahdollistava tekijä IoV:n laajalle käyttöönotolle tulevaisuudessa. 5G:n avulla pystyttäisiin siis todennäköisesti mahdollistamaan laajalle alueelle ulottuvat sekä turvalliset että toimivat yhteydet, jotka toimisivat kaiken lisäksi vielä nopealla yhteydelläkin. Yksi mahdollistava tekijä on myös siinä, että reunalaskentakehyksen perusviestintä on rakennettu 5G-verkkoon. 5G tuo siis mukanaan monia uusia ennen näkemättömiä ominaisuuksia erilaisten palveluiden ja verkkojen suhteen. 5G-teknologia tarjoaa ominaisuuksia ja ratkaisuja myös seikkojen, kuten verkon jatkuvuuden, paremman nopeamman tiedonsiirtonopeuden ja alhaisemman latenssin suhteen. Nämä ovat samalla potentiaalisia ratkaisuja myös IoV:n suhteen, sillä edellä mainitut asiat ovat samalla myös IoV:n haasteita. 5G:n käyttö IoV-sovelluksissa lisäksi todennäköisesti kehittäisi autoteollisuuden palveluja, kuten esimerkiksi erilaisia viihtymisen palveluja ajoneuvoissa ja autonomiseen ajamiseen muutenkin kytkeytyviä erilaisia palveluita. 5G myös luultavasti parantaisi eri IoV-järjestelmien välistä yhdistettävyyttä. Lisäksi todennäköisesti dataa pystyttäisiin kerämään monilla eri tavoilla paremmin kuin aiemmin. (Guevara ja Auat Cheein 2020; Wu ym. 2021; Wu, Xu ja Bilal 2021; Elfatih ym. 2022)

5G:n avulla voidaan mahdollisesti IoV:n tapauksessa luoda ja saavuttaa myös erilaisia liikkuvuuteen perustuvia sovelluksia ja palveluita. Tällaisia voivat olla esimerkiksi reitti- ja tiensuunniteluprosessit, erilaiset autonomiseen ajoon perustuvat palvelut ja älykkään liikenteen palvelut. Tällaiset palvelut tulisivat todennäköisesti laajentumaan myös niihin osallistuvien erilaisten taloudellisten toimijoiden suhteessa. Myös kuten edelläkin jo hieman sivuttiin, monissa muissakin ajoneuvosovelluksissa, kuten esimerkiksi AR-navigoinnissa, videoiden pakkauksessa ja kaikissa muissakin vastaavanlaisissa matkalla viihtymiseen vaikuttavissa sovelluksissa pystytään ottamaan edistysaskeleita 5G:n kautta. (Elfatih ym. 2022; Ning ym. 2021)

4.2.2 5G:n haasteet IoV:n suhteen

Vaikka 5G-teknologiakin sinänsä suuri ratkaisu IoV-tekniikankin toimivuuden suhteen olisi, niin 5G:lläkin ja sen toteuttamisella ja integroimisella IoV:n kanssa on omia haasteita ratkaistavana vielä. Ensinnäkin yksi 5G:n täydellisen toteuttamisen estävistä haasteista on seuraava. 5G:n tapauksessa ei ole vielä sellaista yhtenäistä arkkitehtuuria olemassa sen teknisen yhteenliitettävyyden tapauksessa, että olisi täysin mahdollista jakaa teknologista tietoa aina kansainväliseen käyttöön asti. Lisäksi tässä tapauksessa puuttuu myös täysi mahdollisuus teknologisen tiedon laillistamiseen kansainvälisen käytön suhteessa. Yksi 5G:n haasteista taas puolestaan liittyy standardien integrointiin ja siihen, että sen ympärillä on monenlaisia standardeja ja sääntöjä. Useat eri ryhmät ja toimijat työskentelevät ja joutuvat työskentelemään myös taaksepäin yhteensopivien vanhempien teknologioiden, kuten esimerkiksi 3G:n tai 4G:n kanssa. Täten erilaisten standardien integroinnin suhteen syntyy haasteita. Yksi iso haaste on myös uuden toimivan infrastruktuurin luominen, joka tulisi olemaan massiivinen urakka. Infrastruktuurin luomiseen liittyen myös erilaisten antennien asentamisen ja niiden taajuuksien suhteen tulee olemaan myös haasteita. Esimerkiksi taajuuksien tapauksessa haasteita tulee olemaan siinä, että esimerkiksi 5G:n lisäksi myös 4G on käytössä. Signaalit eivät täten pysty matkustamaan 4G:n taajuuksien yli niin pitkälle kuin olisi mahdollista. Lisäksi 5G tulee luultavasti ainakin osittain tukeutumaan korkeamman taajuuden omaaviin taajuuskaistoihin. (Storck ja Duarte-Figueiredo 2020; Wu ym. 2021)

Yksi ongelma 5G:n tapauksessa on erilaiset esteet. Muun muassa huono sää, puut, rakennukset ja muut vastaavanlaiset esteet voivat aiheuttaa erilaisia häiriöitä ja katkeamisia tie-

tojen kulkuun. Esimerkiksi yksi tällainen häiriö tai katko voi olla IoV:n tapauksessa jo katastrofaalistakin. Myös laitetukeen liittyen on ollut haasteita 5G:n tapauksessa. Tämä haaste on kuitenkin jo selätetty osittain, sillä 5G yhteensopivuudella varustettuja älypuhelimia on tällä hetkelläkin jo saatavilla kaikkialla olevaan verkkoon. Lisäksi autonomista ajoneuvotekniikkaakin on jo käytössä, mutta tosin vielä hyvin rajoitetussa muodossa. Yksi haaste 5G:llä on lisäksi se, että täysin toimiva verkko saataisiin luotua myös syrjäisimmille alueille. Iso haaste tässä on myös siitä aiheutuvat suuret kustannukset. Haasteita liittyy myös 5G:n V2X -viestinnän suhteeseen. Ongelma tässä liittyy erityisesti mmWave-teknologiaan, jolla on vahvat suunnatut korkeiden radiotaajuuksien ominaisuudet. Ne vaativat puolestaan toimivan Line-Of-Sight (LOS) -yhteyden, IoV:n tapauksessa erityisesti, sekä lähettävän että vastaanottavan ajoneuvon välillä. Tämän asian suhteen toimiva tilanne on puolestaan vaikea saavuttaa erilaisten maantieteellisten asetusten ja tieinfrastruktruktuureiden takia. Esimerkiksi tästä johtuen, IoV:n tapauksessa, erilaiset onnettomuuksista varoittavat järjestelmät olisi vaikea toteuttaa. Ongelmia 5G:n ja V2X -viestinnän suhteessa ovat myös seuraavat. Auton katto soveltuu huonosti 360:n asteen antennipeittoon ja lisäksi auton antennit ovat matalia. Laajakaistoilla on myös vahvat suuntaominaisuudet, joka ei ole aina hyvä juttu. Myös suuret automäärät itsessään saattavat blokata tehokkaasti tiedonkulkua teillä, mikä on myös haaste IoV:n ja 5G:n integroimisen suhteessa. Haasteita on liittynyt myös tietojen siirron lisääntymiseen ja tietoturvallisuuteen. 5G:n ja IoV:n integroinnin suhteessa haasteita tulee myös siis kasvavaan tiedonsiirtoon liittyen seuraavassa suhteessa. Haasteena on esimerkiksi se, että kuinka saada jaettua anturitietoja ja muita tietoja kaikkia eniten hyödyttävimmällä tavalla, kun yhidstettynä on kaikki tienpäällä olevat ajoneuvot. Eli esimerkiksi kuinka antaa usean eri ajoneuvon neuvotella esimerkiksi paras tapa ylittää risteys, kun neuvotteluoikeudet asian suhteen annetaan kaikille tienpäällä oleville ajoneuvoille. 5G:n tapauksessa myös tietoturvallisuus ja siihen liittyvä yksityisyys on yksi sellaisista haasteista, joka on onnistuttu jo ratkaisemaan. Tämä siten, että 5G:lle on saatu luotua erilaisia toimivia standardeja ja tietoturvaan liittyviä varoituksia. Näillä sitten puolestaan on kyetty edelleen rakentamaan eri verkkojen välille hyvä luottamus. (Storck ja Duarte-Figueiredo 2020; Wu ym. 2021)

Lisäksi, jos verrataan tämän hetkisiin 4G-verkkoihin, 5G-verkon haittoina ovat muun muassa myös sen tukiasemien pieni peittävyys ja siitä aiheutuvat korkeat kustannukset. Koska 5G:n tukiasemien peittävyys, toisin sanoen kattavuus, on pientä, joudutaan pystyttämään

paljon reunapalvelimia, joka tulee erittäin kalliiksi. Resurssien allokointi eli kohdentaminen ja hallinta ovat myös yhtiä IoV:n verkon suorituskykyyn liittyvistä keskeisimmistä haasteista. Lisäksi mahdollisimman toimivien ja tehokkaiden ajoneuvojen sisäisten viestintäverkkojen luominen on myös haastavaa. Myös big data ja käsiteltävänä oleva massiivinen tiedon määrä muutenkin ovat haasteista. Vaikka 5G:n avulla pystyttäisiin tekemään monia kehitysaskeleita esimerkiksi ajoneuvoissa olevien palvelujen, kuten viihdepalvelujen suhteen, tässäkin suhteessa ongelmana on vielä seuraava. Yksittäisten ajoneuvojen laskennan resurssit ovat vielä tällä hetkellä rajallisia. Lisäksi niiden tallennuskapasiteettikin on vielä rajallinen. Tämän lisäksi ongelma asian suhteen on myös seuraavassakin. Laskentaresurssien ja tallennuskapasiteetin pitäisi pystyä toimimaan kunnolla myös ajoneuvosovellusten tiukkojen viiverajoitusten puitteissa, jotta ajoneuvosovellukset toimisivat riittävällä tavalla. Yhteydet eivät saisi katketa tai pätkiä, sillä muuten seuraukset voivat olla tietyissä tapauksissa jopa kohtalokkaita. (Storck ja Duarte-Figueiredo 2020; Wu ym. 2021; Elfatih ym. 2022; Ning ym. 2021; Yang ja Hua 2019; Yin ym. 2021)

IoV:n lisäksi 5G tarjoaa siis yleisesti mahdollisuuksia kaikkien langattomien yhteyksien suhteen kaikissa uusissa sovelluksissa ja erilaisissa käyttötapauksissa. 5G:n kokonaistavoitteena onkin kyetä tarjoamaan yhteydet kaikkialla kaikentyyppisiin sovelluksiin ja laitteisiin. Siinä suhteessa, että 5G:hen pystyttäisiin vielä täysin luottamaan yhteistyössä IoV:n verkkojen kanssa, on myös seuraavanlaisia ongelmia vielä. Ensinnäkin, vaikka 5G-teknologialla sinänsä pystytään käsittelemään valtavaa datamäärää, tulee IoV:n mahdollisen synnyn myötä datatiedostojen määrä kasvamaan kuitenkin niin suureksi, että tapahtuu seuraavaa. Jos pelkästään 5G:n kautta tullaan siirtämään kaikki tämä valtava datan määrä, syö se huomattavasti 5G:n resursseja. Luultavasti tulevaisuudessa IoV:n kasvaessa entisestään 5G:n resurssit eivät siis yksinkertaisesti enää ehkä riitä. IoV ja sen sovelluskenttä tulee siis luultavasti laajenemaan huomattavasti. Täten 5G-tukiasemilta ajoneuvoille jaettujen tiedostojen ja tietojen määrät tulevat olemaan IoV:ssa erittäin valtavia. Edelleen, jos kaikki tämä tapahtuu vain 5G:n varassa, 5G-palvelujen kautta syntyy mahdollisesti valtavia viestintämaksuja, joka koituu myös ongelmaksi. (Storck ja Duarte-Figueiredo 2020; Wu ym. 2021; Elfatih ym. 2022; Ning ym. 2021; Yang ja Hua 2019; Yin ym. 2021)

Kuten edeltäkin tuli jo ilmi IoV:n haasteiden erittelyn yhteydessä, vastaavasti myös 5G:n

IoV:iin mahdollistamien ominaisuuksien yhteydessä voi nostaa esiin mahdollisesti syntyvät eettiset haasteet. Automatisoitujen ajoneuvojen tapauksessa voi syntyä esimerkiksi pahimmassa tapauksessa nopeita tilanteita, joissa jopa eettiset valinnat voivat tulla kyseeseen. Muutenkin itseohjautuvien ajoneuvojen tapauksessa riskinä on erilaiset pahatkin onnettomuudet. Lisäksi henkilötietojen yksityisyys on haasteena, koska ajoneuvojen käyttäjien henkilötietoja tulee kulkemaan massiviinen määrä pilvipalveluissa. Kehitettävää 5G:n ja IoV:n suhteen on myös identiteetinhallinnassa. Ajoneuvot ovat liikkuvia objekteja, joten latenssin tulee olla alhainen ja tiedonsiirtonopeuden nopeaa. Tästäkin johtuen ajoneuvoja käyttävät tulisi jollain tavalla todentaa ja yksilöidä hyvissä ajoin IoV-verkoissa. Lisäksi käyttäjien pääsyä erilaisiin ajoneuvojen etäpalveluihin tulisi valvoa muutenkin tarkoin. Erilaiset varmenteet olisi siis hyvä päivittää hyvissä ajoin. Viestintä IoV:ssa vaatii siis todella nopean tiedonsiirtonopeuden sekä alhaisen latenssin toimiakseen kunnolla. Tämä johtaa myös siihen, että todentamisen eli autentikoinnin täytyisi olla 5G:n myötä huomattavasti nopeampaa kuin aiemmissa verkoissa. Seuraavaksi kiteytettynä vielä kaikesta edellisestä. Eli vaikka 5G toisi IoV:nkin tapauksessa monia potentiaalisia ratkaisuja, silti haasteita liittyy vielä erityisesti sovellusten kaistanleveyteen ja reaaliaikaisuuden toimivuuteen ja kattavuuteen liittyen. Haasteita löytyy myös tiedonsiirtonopeuteen, energiatehokkuuteen, samanaikaisiin yhteyksiin, luotettavuuteen, liikkuvuuteen ja latenssiin liittyen. Seuraavaksi vielä tarkemmin näihin liittyvistä mahdollisista ratkaisuista. (Guevara ja Auat Cheein 2020)

4.2.3 5G:n mahdollistamat potentiaaliset ratkaisut IoV:n suhteen

Guevara ja Auat Cheein (2020) artikkelissaan luettelevat joitain potentiaalisia ideoita ratkaisuista edellä mainittuihin 5G:n haasteisiin ja ongelmiin. Tämä erityisesti silloin, kun 5G:tä integroidaan IoV:n kanssa. Yksi keino parantaa latenssia, samanaikaisten yhteyksien toimivuutta, tiedonsiirtoa ja energiatehokkuutta on seuraava. Edellä mainittu olisi mahdollisesti toteutettavissa esimerkiksi siten, että tiedonsiirto tehdään läheisten laitteiden välillä välittämättä tietoa ollenkaan verkkoinfrastruktuurin kautta. Tällaisella niin sanotulla suoralla lähetyksellä saataisiin sitten edellä mainitun kaltaisia positiivisia vaikutuksia aikaan. Päästä päähän -latenssi esimerkiksi vähenee, kun tällöin käytössä on lyhyen kantaman linkit. Lisäksi, koska laitteet olisivat tällöin lähellä toisiaan, lähetystehon vaade olisi pienempi. Li-

säksi myös energiankulutus vähenisi ja energiatehokkuus paranisi. Tällainen uusi Device-to-Device eli D2D-teknologiaan perustuva 5G voisi mahdollisesti olla yksi tärkeistä tekijöistä IoV-palvelujen kehityksen suhteen (Elfatih ym. 2022).

Lisäksi ainakin Elfatih ym. (2022) artikkelissaan näkevät, että IoV:n suhteen 5G-viestinnästä on etua juuri nimenomaan ainakin ajoneuvojen välisessä eli V2V -viestinnässä. Tämä siksi, että kyseessä on juuri nimenomaan pääosin laitteiden välinen viestintä eli D2D-viestintä 5G-verkostossa. D2D-viestintä toisi myös seuraavanlaisia mahdollistavia ja positiivisia tekijöitä IoV:n kannalta. Se lisäisi tehokkuutta taajuuksien ja signaalien suhteessa eli toisin sanoen spektrin tehokkuutta. Lisäksi IoV-palveluiden suhteen todennäköisesti myös käyttökokemus paranisi. Myös erilaisia IoV:n viestintäsovelluksia olisi todennäköisesti mahdollista laajentaa täten entisestään. Mainitaan, että Long-Term Evolution (LTE) -tekniikka on sinänsä yksi ratkaisuista tällaisen D2D-tekniikan suhteessa. LTE ei kuitenkaan vielä tällä hetkellä kykene ylläpitämään normaalisti V2V -viestintää. Yksi ratkaisu taas edelleen kyseessä olevaan tapaukseen on mahdollisesti seuraava. D2D:n avulla joka tapauksessa kyetään mahdollistamaan laitteiden välinen suora viestintä. Täten yksi mahdollisuus on käyttää infrastruktuuria apuna D2D-viestintätekniikan toteutuksessa. Infrastruktuuriavusteisella D2D:llä olisi siis todennäköisesti mahdollista saavuttaa luonnollisella tavalla tehokkaat ja luotettavat V2V -yhteydet 5G:ssä. Syrjäisempien alueiden suhteen yksi ratkaisu 5G:n suhteen voisi olla puolestaan seuraava. Koska kaikki tiet eivät pysty mitä luultavimmin kuulumaan 5G:n piiriin, on tähän ehkä ratkaisuna ad-hoc -verkkopohjaisten järjestelmien käyttö kyseisenlaisilla alueilla. Ad-hoc -verkon kautta pystyttäisiin luultavasti jakamaan suurikokoisia tiedostojakin. Lisäksi se on yhteensopiva esimerkiksi juuri 5G:n kanssa ja näitä kahta pystytään käyttämään myös rinnakkain. Tämä vähentäisi sitten puolestaan mahdollisesti soluresurssien käyttöä. Ennen kaikkea hyötynä ad-hoc -verkkojen käytöstä olisi juuri se, että suurikokoisia tiedostojakin voitaisiin jakaa syrjäisemmillä alueilla myös siis ilman 5G palveluita. Tämä voisi siis olla ikään kuin eräänlainen väliaikaisratkaisu IoV:n syrjäseutuhaasteeseen. (Elfatih ym. 2022)Yin2021

Toinen mahdollinen ratkaisu taas olisi esimerkiksi nimeltään Massive Multiple-Input Multiple-Output (MIMO). Eli käytettäisiin suuria antenniryhmiä tukiasemissa, jotta saataisiin luotua langaton verkko. Näin luodun verkon kautta pystyttäisiin sitten sekä lähettämään että vas-

taanottamaan useampikin kuin yksi tieto. Ratkaisun näin luotu valtava verkko tarjoaisi seuraavaan. Se kykenisi toimimaan katkeamattomasti ja tiedonsiirroltaan nopeasti myös tiheällä alueella, jossa läsnä olisi samanaikaisesti paljon eri käyttäjiä. Juuri nämä tekijät ovat myös sellaisia, että MIMO olisi siis myös erinomainen potentiaalinen tapa käsitellä tehokkaasti IoV-verkon toimintaa. Yhdeksi potentiaaliseksi ratkaisuksi mainitaan myös niin sanotut pienet solut. Tällaisella pienellä solulla tarkoitetaan tässä tapauksessa sellaista kannettavaa miniatyyristä tukiasemaa, joka vaatii hyvin pienen määrän virtaa toimiakseen. Tällaisia asemia olisi asennettava kuitenkin suuri määrä älykkäisiin kaupunkeihin, jotta etenemishäviötä ei pääsisi tapahtumaan. Tällaisten pienten solujen avulla saataisiin luultavasti parennettua muun muassa datakapasiteettia, tiedonsiirtonopeutta ja näin ollen ylipäätään myös koko verkon toimivuutta. Niitä myös tavallisesti käytetään tyypillisesti alueilla, joissa tietoliikenne on tiheää. Näin ollen tämä olisi myös potentiaalinen ratkaisu tiheän ajoneuvoliikenteen ja siinä käytettävien monien samanaikaisten yhteyksien tapauksessa. Lisäksi tällaisilla soluilla pystyttäisiin myös todennäköisesti vastaamaan liikkuvuuden vaatimukseen IoV-verkon tapauksessa. Esimerkiksi verrattuna edellä mainittuun MIMO -tekniikkaan, erona näiden pienien solujen tapauksessa olisi seuraava. Pienet solut olisivat siirrettäviä. Ne pystyttäisiin sijoittamaan liikkeessä olevien ajoneuvojen sisälle huolehtimaan kommunikoinnista kulloinkin kyseessä olevan ajoneuvon käyttäjien kanssa. MIMO:n tapauksessa kommunikointi tapahtuisi ajoneuvon ulkopuolella olevien ulkopuolisten tukiasemien kanssa. Ongelma kuitenkin tällaisten solujen kanssa on vielä, että 5G vaatii entistä suuremman ja vaadittavalla tarpeellisella tavalla luodun soluinfrastruktuurin. Tällaisessa tarpeellisella tavalla luodussa soluinfrastruktuurissa esimerkiksi hyödynnettäisiin antennin kokoa oikealla tavalla, jotta vaadittava tarvittava suorituskyky kyettäisiin saavuttamaan. Antennit voisivat olla pienien solujen tapauksessa pieniä, jolloin ne saataisiin kätevämmin kiinnitettyä erilaisiin paikkoihin. Kuitenkin tällaisen infrastruktuurin luominen olisi erittäin kallista ja tämä ongelma tulisi vielä asian suhteen ratkaista parhaalla mahdollisella tavalla. Yksityisyyden ja erilaisten henkilökohtaisten tietojen luottamuksellisuuden säilyttämisen suhteen on yritetty käyttää paljon muun muassa tietojen salausta. 5G:n tapauksessa yksityisyyden suojaaminen on kuitenkin edelleen yksi keskeisimmistä haasteista vieläkin, jossa on paljon parannettavaa edelleen. (Guevara ja Auat Cheein 2020)

Kuten edeltäkin ITS:n avaamisessa tuli jo ilmi, sen avulla liikenteestä saataisiin mahdolli-

sesti sekä aika- että energiatehokkaampaa. Reittien optimointien kautta ruuhkat ja mahdollisesti myös onnettomuudet vähenisivät. Tätä kautta aikaiseksi saataisiin mahdollisesti myös ympäristöä säästäviä vaikutuksia, kun saastetasoja saataisiin todennäköisesti jonkin verran vähennettyä sekä liikenteen tehostumisen että tätä kautta ruuhkien vähentymisen myötä. Automatisoitujen ajotoimintojen myötä myös ajo olisi todennäköisesti tasaisempaa. Tätä kautta sitten taas esimerkiksi kulut polttoaineisiin liittyen vähenisivät ja taloudellinen tuottavuus paranisi. Muutenkin, kun erilaisia kestävyyden vaikutuksia mietitään 5G:n integroimisessa IoV:n kanssa, on havaittu seuraavanlaisia tekijöitä ja myös mahdollisia ratkaisuideoita niihin. On havaittu, että suurimpia ruuhkia aiheutuu isoimmissa kaupungeissa nimenomaan parkkipaikkojen etsinnän ja risteysten takia. Ruuhkat sitten puolestaan taas saastuttavat ympäristöä. Mainitaan, että yksi potentiaalinen kehityskeino kyseiseen asiaan olisi älykkäiden liikennevalojen luonti 5G:n avulla. Ruuhkia sanotaan aiheutuvan esimerkiksi nykyisten liikennevalojen ja myös liikennemerkkien muuttumattoman luonteen takia. Nykyiset liikennevalot ovat esiohjelmoitu toimimaan aina vain tietyllä tavalla. Sen sijaan yksi potentiaalinen ratkaisu voisi olla se, että liikennevaloihin luotaisiin esimerkiksi 5G-teknologian avulla dynaaminen luonne. Eli tällöin ne mittaisivat liikennettä reaaliaikaisesti ja säätyisivät dynaamisesti kulloinkin vallitsevan liikenteen määrän ja luonteen mukaan. Yhdeksi ratkaisuideaksi kyseisen aiheen tiimoilta mainitaan myös älykäs navigointi. Se sitten puolestaan nopeuttaisi ja tehostaisi ajajien perille pääsemistä. Ruuhkat vähenisivät ja sitä kautta edelleen jälleen myös saasteet. Yksi parannuskeino voisi olla myös julkisen liikenteen kehittäminen esimerkiksi siten, että pystyttäisiin tarjoamaan reaaliaikaista verkkoliikennetietoa julkisen liikenteen aikatauluihin liittyen. Tämä voisi mahdollisesti johtaa jopa yksityisautoilun vähentymiseen osittain ja näin jälleen ympäristön saastuminen lieventyisi. Pysäköintiä kaupungeissa voisi myös tehostaa siten, että pystytettäisiin jonkin sortin antureita. Näiden kautta pystyttäisiin siten verkosta näkemään jo ennalta vapaana olevat pysäköintipaikat. Tämä vähentäisi parkkipaikkojen etsinnästä aiheutuvaa turhaa ajelua. Näin ruuhkat ja edelleen siitä aiheutuvat ympäristöpäästöt vähenisivät. (Guevara ja Auat Cheein 2020)

Yksi potentiaalinen tekijä ratkaisuiden suhteen piilee myös siinä, että reunalaskentakehyksen perusviestintä on rakennettu 5G:hen. Reunalaskennan avulla 5G:n reunapalvelimiin pystytään sisällyttämään paljon erilaisia laskelmia. Tämän avulla puolestaan pystyttäisiin todennäköisesti vastaamaan sekä kaistanleveyden että alhaisen latenssin haasteisiin ja näin ollen

myös pitkälti koko IoV:n kehitykseen. Kuten edelläkin jo mainittiin, 5G tarvitsee sen tukiasemien pienen peittävyyden takia suuren määrän kalliita reunapalvelimia. Tämän haasteen edistämiseksi yksi mahdollinen keino olisi esimerkiksi seuraava. Tienvarsiin voitaisiin yrittää järjestää solmupisteitä. Näillä voitaisiin auttaa ajoneuvoilla olevien tehtävien siirtämisessä tukiasemalle. Joka tapauksessa kyseisen haasteen suhteessa aikaiseksi tulisi saada sellainen tekniikka, jolla pystyttäisiin mahdollistamaan pitkän matkan tiedonsiirtokin nopeasti. Kun tämä saataisiin toteutettua, 5G-verkkojen tukiasemien määrää saataisiin laskettua siten, että koko verkon toimivuus ei kärsisi tästä liikaa. Lopputulemana olisi se, että 5G-verkkoon liittyvät kustannukset alenisivat ainakin kyseisen seikan tiimoilta. (Wu ym. 2021)

Edellä IoV:n kuvailun yhteydessä mainittiin myös Vehicle-to-everything eli V2X -viestintätyyppi. Juuri nimenomaan 5G-teknologian avulla saadaan V2X luotua IoV:ssa (Wu, Xu ja Bilal 2021). V2X tarvitsee pohjalle toteutuakseen ja toimiakseen myös toimivan IoT-verkoston, joka sekin paljolti tulee mahdollistumaan 5G-teknologian avulla. Myös IoV:n yhteistyö juuri nimenomaan 5G:n kanssa mahdollistaa myös IoV:n eri viestintätyypit, jotka kaikki tulikin esiteltyä jo edellä. 5G ja edelleen V2X mahdollistaa IoV:ssa seuraavaan. IoV:ssa saadaan tuettua verkkoyhteyksiä ajoneuvojen, latauspisteiden, antureiden ja RSU:iden välillä. 5G:n avulla saadaan IoV:n kannalta edistystä myös seuraavaa ajatellen. Itseohjautuvien autojen kehitys todennäköisesti tulee tehostumaan huomattavasti sen tulon myötä. Tämä johtuu taas puolestaan siitä, että 5G:n avulla viestinnän viiveitä saadaan vähennettyä merkittävästi. Lisäksi 5G:n avulla tullaan todennäköisesti saamaan aikaiseksi edistysaskeleita myös IoV-verkon haasteisiin, kuten esimerkiksi turvallisuuteen, yksityisyydensuojaan ja luotettavuuteen liittyen. IoV:n tietosuoja ja -turvallisuus on kuitenkin kuin kaksiteräinen miekka 5G:n kannalta. Toisaalta 5G tuo mahdollisia ratkaisuja IoV:n tietoturvallisuuteen ja siihen kohdistuviin erilaisiin hyökkäyksiin nähden.Kuitenkin samalla sen mahdollistamien uusien palvelujen ja ominaisuuksien myötä IoV:n tietoturvaan ja yksityisyyteen liittyen tulee myös juuri sen takia lisää ongelmia ja haasteita. 5G:n ominaispiirteiden avulla pystytään IoV:ssa toisaalta mahdollistamaan esimerkiksi viestintäviiveiden vähenemistä sekä ajoneuvojen itsensä että ajoneuvojen ja muiden laitteiden välillä. Toisaalta sitten esimerkiksi 5G:n mahdollistamien IoV-verkossa kulkevien itseohjautuvien ajoneuvojen korkea kaikenaikainen liikkuvuus aiheuttaa ongelmia. Epävarmuutta tässä suhteessa luo esimerkiksi se, kun läheiset ajoneuvot ja näin ollen myös anturit vaihtuvat ympärillä kaiken aikaa. Toisin sanoen resurssien kohden-

taminen eli allokointi ja siis IoV-verkon hallinta nopeasti liikkuvien ajoneuvojen tapauksessa on haaste. Mainitaan, että juuri edellä mainitun takia tarvittaisiin tietoturvan suhteessa esimerkiksi jonkinasteisia toimivia salauspohjaisia yksityisyyden suojan toteuttavia tietosuojajärjestelmiä kiireellisesti, jotta ongelma pystyttäisiin ehkä todennäköisesti ratkaisemaan edes jollain tasolla. (Wu, Xu ja Bilal 2021; Elfatih ym. 2022; Osibo ym. 2021)

Myös tekoälyn kautta saataisiin mahdollisesti ratkaistua ongelmia sekä 5G:n että IoV:n suhteessa. Tästä vielä tarkemmin jäljempänä. Joka tapauksessa, kuten edelläkin tuli jo sivuttua, 5G kuitenkin tarjoaa mahdollisuudet päästä eroon IoV:iin liittyvistä haasteista. Eli haasteista kuten liian suuresta viiveestä eli latenssista, liian pienestä kaistanleveydestä ja riittämättömästä tiedonsiirtonopeudesta. Toisin sanoen 5G-verkko siis sinällään tarjoaa ratkaisun avaimet alhaisen latenssin ja viiveen vähentämisen, suuren tiedonsiirtonopeuden ja suuren kaistanleveyden suhteen. Täten myös koko IoV-verkko kokonaisuutena ja sen suorituskyky yleisesti paranisi, sillä ratkaisuja saataisiin juuri yhtiin olennaisimpiin haasteisiin sen kannalta. Vielä kuitenkin on pohdinnassa, että kuinka kaikki esimerkiksi juuri 5G:n ja IoV:n suhteen saataisiin ihan konkreettisella tasollakin toimimaan tarpeeksi hyvin. Yksi ratkaisu on myös mahdollisesti reunalaskennan ja 5G:n yhdistäminen. Tämän yhdistelmän avulla pystytään käyttämään laajaa valikoimaa eri yhteyksiä ja tekniikoita samanaikaisesti ilman katkoksien aiheutumista verkoissa. Kyseinen yhdistelmä voi olla myös ratkaisu ajoneuvojen suuren liikkuvuuden ja epäsäännöllisen jakautumisen haasteisiin. Ajoneuvojen IoV-verkkoihin lähettämät tiedot, kuten sijainti, navigoinnit tai esimerkiksi nopeus, ovat yleensä sellaisia tietoja, että ne tulisi pystyä lähettämään tiettyjen aikavälien sisällä verkkoon. Näiden tietojen olisi myös aina ilman poikkeuksia seurattava niiden optimaalista reittiään ilman minkään sortin tietojen menetyksiä tai pudotuksia verkossa, jotta ei tapahtuisi mitään vakavaa. 5G:n ja reunalaskennan yhdistelmä voisi olla ratkaisu siinä mielessä, että sen avulla myös pystyttäisiin potentiaalisesti mahdollistamaan seuraava. Sen avulla ajoneuvot pystyisivät erittäin nopeasti sekä liittymään että poistumaan IoV:n viestintäverkoista. (Wu, Xu ja Bilal 2021; Elfatih ym. 2022; Osibo ym. 2021)

4.3 Ratkaisuideoita etäajoon liittyen

Tässä eräitä muita ideoita ratkaisuiksi IoV:n toteuttamiseen ja haasteisiin liittyen. Autonominen ajo eli toisin sanoen etäajo mainitaan tärkeäksi 5G:hen pohjautuvaksi sovellukseksi IoV:n ja sen toteutuksenkin kannalta. Etäajo luottaa täysin 5G-teknologian mahdollistamiin ominaisuuksiin eli alhaisempaan latenssiin, suurempaan kaistanleveyteen ja näin ollen myös korkeampaan luotettavuuteenkin ylipäänsä. Tekniikka tulisi saada niin luotettavalle ja turvalliselle tasolle, että etäajo olisi täysin mahdollista toteuttaa kunnolla. 5G:n mahdollistamassa etäajossa itseohjautuvien ajoneuvojen ohjaus-, päätös- ja esimerkiksi tunnistustoiminnot siirretään pilvipalveluun. Etäohjaus voi tapahtua pilvipalvelun tai ihmisen avulla. Etäajon myötä myös luultavasti vähentyisi riippuvuus erilaisista ajoneuvojen antureista ja näin ollen pystyttäisiin mahdollistamaan erittäin tarkka ajoneuvojen ohjattavuus.(Qiu ym. 2019)

Konkreettisemmin katsottuna etäajo pystyttäisiin luultavasti mahdollistamaan seuraavin keinoin. Ensinnäkin etäajon 5G:hen pohjautuvan järjestelmän arkkitehtuuri olisi pääpiirteittäin seuraavanlainen. Se sisältäisi ensinnäkin etäajon kauko-ohjaus- ja pilvirajapinnan. Lisäksi etäajon järjestelmäarkkitehtuuri koostuisi 5G-verkkojärjestelmän ja ajoneuvon etäajon ohjausohjelmistosta. Kauko-ohjausrajapinnan käyttöliittymä puolestaan sisältäisi sekä ohjaukseen että ohjauksen antamaan palautteeseen perustuvan järjestelmän. Kyseiseen rajapintaan sisältyy myös siis ohjauspyörä ja polkimet. Etäajon pilvirajapinta puolestaan sisältää verkon optimointikomponentin, palautekomponentin, tietoturvakomponentin, videokomponentin ja ohjauksen. Ajoneuvon etäohjauksen ohjausohjelmisto puolestaan sisältää seuraavaa. Siihen kuuluu toimintoja, kuten videon pakkaaminen, etäajon toimintarakenteet, etäkäyttösovellukset ja komponenttien optimointi. 5G-verkkojärjestelmä sisältää ydinverkon, 5G-tukiaseman sekä päätelaitteen tai jonkin vastaavan laitteen. (Qiu ym. 2019)

Seuraavaksi hieman kuvailua siitä, että minkälaisten eri vaiheiden kautta etäajo pystyttäisiin mahdollisesti toteuttamaan käytännössä. Etäajon yleisiä vaiheita voivat olla esimerkiksi seuraavat. Ensinnäkin yksi taktiikka olisi asentaa eri puolille ajoneuvoa esimerkiksi viisi kameraa kuvaamaan tapahtumia ajoneuvon ympärillä. Kameroita asetettaisiin ajoneuvon etupuolelle, panoraamapuolelle, sisäpuolelle sekä oikealle että vasemmalle puolelle. Videot välitettäisiin sitten kuljettajan puolelle. Videot lähetettäisiin 5G:n välityksellä reaaliaikaisesti, jotta synkronointikin saataisiin varmistettua. Ajonhallintakomponentti ja näyttö sijaitsisivat

myös kuljettajan puolella. Ajoneuvosta välittyvät tiedot esitettäisiin sitten auton kuljettajalle oikea-aikaisesti arvioituna sekä tiestön että ajoneuvon kunnon mukaan. Itseohjautuva ajoneuvo myös vastaanottaa ohjaussignaaleja ja suorittaa niiden mukaan toimintoja, kuten hidastaminen, kiihdytys, kääntyminen ja jarrutus. Etäajon suhteen tulee kuitenkin vielä saada varmistettua, ennen kuin se voidaan täysin ottaa käyttöön, täysi toimivuus siltä vaadittujen ominaisuuksien, kuten erittäin suuren kaistanleveyden, erittäin alhaisen latenssin ja erittäin korkean luotettavuuden suhteen. (Qiu ym. 2019)

Yksi ratkaisu itseohjautuvien ajoneuvojen suhteen voisi olla myös eräänlainen platooning -ratkaisu. Tässä on kyse eräänlaisesta joukkoliikenneratkaisusta, joka voi olla esimerkiksi seuraavanlainen. Tiellä ensimmäisenä ajava ajoneuvo on joko miehitetty tai autonominen itseohjautuva ajoneuvo. Tämän ajoneuvon takana tulevat ajoneuvot ovat sitten puolestaan yleensä autonomisia ajoneuvoja. Nämä takana tulevat ajoneuvot pitävät yllä reaaliaikaista tietoa vuorovaikutuksessa edellä ajavan niin sanotun pääajoneuvon kanssa. Tällainen vuorovaikutus tapahtuu V2X -viestinnän välityksellä. Tällaisessa platooning -ratkaisun kaltaisessa ryhmässä monet ajoneuvot voivat itsenäisesti seurata tätä pääajoneuvoa tietyin väliajoin tietyllä nopeudella. Ajoneuvot voivat myös liittyä joukkueeseen tai lähteä tästä joukkueesta ja suorittaa esimerkiksi joukon kesken yhteistoiminnallisen hätäjarrutuksen tarvittaessa. Seuraavaksi vielä hieman tarkemmin kuvailua tällaisen ryhmäjärjestelmän erilaisista vaiheista ja käyttötapauksista. Yksi tilanne on esimerkiksi joukkoon liittyminen. Tilanne voi mennä tällaisessa esimerkiksi seuraavasti. Ryhmä ajaa tiellä, jossa ajoneuvo A johtaa ja hallitsee ryhmää ja sen toimintaa. Ulkoinen ajoneuvo B sitten haluaa liittyä mukaan tähän ryhmään. B lähettää oman statuksensa eli tilansa ympäristöönsä ja hakee siis ryhmään. A huomioi ensin, että millainen tilanne on sen ryhmässä ja päättää sitten tämän perusteella B:n liittymisestä ryhmään. A antaa tämän jälkeen ryhmän tiedot B:lle. Sitten esimerkiksi ryhmässä olevat ajoneuvot C ja D varaavat puolestaan paikan B:lle A:n antaman huomautuksen mukaan. Lopulta ulkopuolinen ajoneuvo B pääsee liittymään ryhmään. Tämän jälkeen A vielä päivittää ryhmän tiedot ja lähettää ne myös kaikkien ryhmässä olevien ajoneuvojen tietoon samanaikaisesti. Toinen tilanne voi olla puolestaan taas ryhmästä poistuminen. Jos esimerkiksi ajoneuvo B haluaa nyt sitten poistua ryhmästä, se lähettää tästä tiedon ryhmälle. Kun B poistuu, toinen ryhmässä oleva ajoneuvo esimerkiksi D kiihdyttää täyttämään vapaan paikan, josta B juuri poistui. Ryhmä palauttaisi siis esimerkiksi tässä tapauksessa sen saman ikään kuin nor-

maalin tilan, kuin sillä oli ennen kuin B liittyi ryhmään. Taas vastaavasti johtava ajoneuvo A päivittää ryhmän tiedot tilanteen mukaiseksi ja tiedottaa myös muita ryhmän ajoneuvoja. Yksi tapaus tällaisessa ryhmässä voi myös liittyä esimerkiksi johonkin seuraavista eli kiihdytykseen, käynnistykseen, jarrutukseen, hidastukseen tai välttämiseen. Esimerkiksi A saatuaan ajopäätöstiedot lähettää nämä ajotiedot samaan aikaan sitä seuraaville ajoneuvoilla B ja C, kun A säätää itse omaa ajotilaansa. Tämän jälkeen toinen ryhmän ajoneuvo suorittaa käynnistys-, kiihdytys-, hidastus-, jarrutus- tai välttämistoiminnan joko synkronisesti tai järjestyksessä. (Qiu ym. 2019)

Seuraavaksi puolestaan hieman tyypillisistä käyttötapauksista tällaisessa platooning -ratkaisussa. Tyypillisten käyttötapausten vaatimusten mukaisesti verkkoarkkitehtuurissa viestintä ajoneuvosta ajoneuvoon, ajoneuvosta pilveen, ajoneuvosta tielle ja tieltä pilveen ovat välttämättömiä, että erilaiset viestintävaatimukset pystyttäisiin takaamaan tällaisessa ryhmätilanteessa. Ensinnäkin ajoneuvojen välisessä viestinnässä tulisi vaihtaa tällaisissa tilanteissa tietoja ryhmää johtavan ajoneuvon sekä sitä seuraavien ajoneuvojen välillä. Tämä siksi, että synkronointi ja seuranta olisi helpompaa. Ajoneuvosta tielle -viestinnässä taas puolestaan tulisi kerätä mahdollisimman hyvin tietoa tiestön kunnosta RSU:lta, jotta ryhmäajoa saataisiin tuettua mahdollisimman hyvin. Ajoneuvon ja pilven välisessä viestinnässä taas puolestaan tulisi kerätä ajoneuvon ajotietoja pilveen esimerkiksi ajokäyttäytymisen analysointia ja data-analyysiä varten. Tieltä pilveen -viestinnässä RSU:lta kerätyt tiedot tieolosuhteista tulisi välittää pilveen. Sieltä kyseisiä tietoja voidaan käyttää sitten taas puolestaan hyödyksi ajopäätösten tekemisessä. Platooning -ratkaisun hyötyjä voivat olla mahdollisesti myös seuraavat tekijät. Sen avulla voidaan luultavasti esimerkiksi vähentää kuljettajien vastuuta ajamisesta, pienentää tuulenvastusta ja tätä kautta sitten vähentää myös polttoainekulujakin. Kyseinen ryhmäajo voi myös vähentää onnettomuuksia ja niiden mahdollisuutta, kun takana tulevat autot seuraavat heti pääautolta tulevia käskytyksiä. Ryhmittelyn avulla voidaan myös vapauttaa enemmän tietä toisille ajoneuvoilla. Tämä sitten puolestaan taas saattaa lisätä liikenteen tehokkuutta ja vähentää ruuhkia. (Qiu ym. 2019) Tässä siis edelle hieman esimerkkiä, että millaisia ideoita on esimerkiksi olemassa etäajon toteuttamiseen liittyen IoV:ssa.

4.4 Ratkaisuideoita liittyen saatavuuteen, tietojen eheyteen, luottamuksellisuuteen ja todennukseen

Seuraavaksi ratkaisuideoita IoV:n toimivuuden kannalta keskeisten ominaisuuksien, kuten saatavuuden, tietojen eheyden, luottamuksellisuuden ja todennuksen suhteen. Saatavuudella tarkoitetaan erilaisten IoV:n verkkojen, esimerkiksi V2V, V2I, V2P ja muiden vastaavien, käyttöaikaa IoV:ssa (Osibo ym. 2021). Kyseessä on keskeinen ja tärkeä turvallisuusvaatimus sekä samalla ominaisuus IoV:n toimivuuden kannalta. Saatavuuden tulee olla ajoneuvojen tapauksessa hyvä, jotta tarvittavat liikenne- ja tietiedot päivittyvät ajoneuvoilla riittävällä tavalla. Jos saatavuus on heikko tai sitä ei ole ollenkaan, koko IoV-ympäristö kärsii siitä. Pahimmassa tapauksessa koko IoV-ympäristö voi pysähtyä esimerkiksi tietoturvahyökkäysten seurauksena.(Osibo ym. 2021) Edellä jo erilaisia tietoturvahyökkäyksiä tulikin lueteltua. Tietoturvahyökkäyksistä erilaiset häiriöt, DDoS ja Dos ovat esimerkiksi yleensä hyökkäyksiä juuri saatavuuteen liittyen IoV:ssa (Osibo ym. 2021). Yhdeksi ratkaisuksi saatavuuteen kohdistuvia tietoturvahyökkäyksiä vastaan on ehdotettu muun muassa paketintunnistusjärjestelmää, joka havaitsisi IoV:n ajoneuvoverkoista löytyviä tukoksia. Tämä toimisi esimerkiksi siten, että paketin saapuessa kahteen tunnistusjärjestelmään, paketintunnistusmoduuli tarkistaa signaalin havaitsemisen aika-alueella, kun taas toiset monitorit tarkkailevat mahdollisia impulssihäiriöitä. DoS-hyökkäysten torjumisessa taas puolestaan yksi mahdollinen keino on tiedon louhintaan perustuva lähestymistapa, jossa häiritsevät DoS-hyökkäykset havaitaan ajoneuvojen välisessä V2V-viestinnässä. Tässä ehdotetussa menetelmässä yritettäisiin saada ymmärrys siihen, miksi ylipäätään ajoneuvot usein menettävät viestejä ryhmässä. DoS-hyökkäysten ennalta ehkäisemiseen IoV:n verkoissa myös esitettiin esimerkiksi potentiaaliseksi ratkaisuksi jonkinlaista pakettien havaitsemisalgoritmia. Se havaitsisi haitallisia solmuja, solmuja jotka lähettävät asiaankuulumattomia paketteja häiritäkseen verkkoa, IoV-verkoissa. (Osibo ym. 2021)

Luottamuksellisuus puolestaan tarkoittaa IoV:ssa seuraavaa. Ajoneuvojen ja käyttäjien tiedot pidetään salaisina. Lisäksi pidetään huolta, että ne eivät pääse asiaankuulumattomien ja väärien tahojen käsiin ja että niitä ei väärinkäytetä. Lisäksi muiden kuin asianomaisten pääsyä tiettyihin tietoihin, kuten vaikka esimerkiksi tietoihin ajoreitteihin tai ajoneuvon sijainteihin liittyen, on rajoitettava tai estettävä kokonaan. Tietoturvahyökkäyksistä salakuuntelu

on yleisin, joka kohdistuu nimenomaan IoV:n luottamuksellisuuteen. Yhdeksi ideaksi salakuuntelun torjunnassa ehdotettiin mallia, jossa luotaisiin tietoliikenteessä valepaketteja. Nämä valepaketit ohjattaisiin vain tietyille RSU:ille, jotta liikennetilastojen suhteen hyökkääjiä saataisiin johdettua harhaan. Lisäksi tämän kautta myös suojattaisiin kriittisimpiä RSU:ita mahdollisilta hyökkääjiltä. Toinen ehdotettu taktiikka salakuuntelun torjumiseksi on eräänlainen pyöritettyyn häirintää perustuva (engl.rotated-jamming-based) ennakoiva salakuuntelujärjestelmä. Sen avulla pystyttäisiin sitten mahdollisesti tarkkailemaan lähteen ja kohteen välillä olevaa mahdollisesti epäilyttävää yhteyttä. Kyseisellä järjestelmällä suoritettaisiin ensisijaisesti kaksi toimintoa. Nämä olisivat tietojen sieppaus ja epäilyttävän linkin häiritseminen. Salakuuntelua vastaan tekniikaksi esitettiin myös eräänlaista tien kunnon valvontajärjestelmää, jossa tarkkaillaan tieolosuhteita reaaliaikaisesti pilvipalvelimen kautta. Kyseinen salakuuntelun estämiseksi ehdotettu järjestelmä kykenisi todennäköisesti estämään yhteistoimintahyökkäyksiä ja hyökkäyksiä RSU:iden kautta. Täten sillä pystyttäisiin todennäköisesti estämään erilaisten ajoneuvojen ja niiden käyttäjien arkaluontoisia tietoja paljastumasta hyökkääjille. (Osibo ym. 2021; Baruah ja Dhal 2020)

Tietojen eheys IoV:n tapauksessa tarkoittaa taas puolestaan seuraavaa. Se on eräänlainen varmistus sille, että IoV:ssa jaettuja tietoja ei ole muokattu millään tavalla luvattomien henkilöiden toimesta. IoV:ssa oleva tieto on siis eheää eli niin sanotusti vahingoittumatonta. Toisin sanoen eheydellä tarkoitetaan tässä tapauksessa sitä, että vastaanotetut tiedot tulee olla samat, kuin mitä ne ovat olleet lähetettäessä. Yleinen tiedon eheyttä vastaan kohdistuva tietoturvahyökkäys on Man-in-the-middle -hyökkäys. Sen torjuntaan ja käsittelemiseen IoV:n verkoissa ehdotetaan esimerkiksi luottamusmallia yhdistettyihin ajoneuvoihin. Ehdotettu malli on sellainen, joka kykenee tunnistamaan hyökkäyksiä verkkoon aloittamassa olevia haitallisia solmuja. Näin ollen tällaisten haitallisten solmujen tunnistetietoja pystytään havaitsemisen jälkeen tarvittaessa perumaan. Toisena torjuntakeinona ehdotetaan esimerkiksi pseudo-identiteettiin perustuvaa järjestelmää ajoneuvoverkoille. Siinä olisi ehdollinen todennus, anonyymiteetti ja datan eheys. Kyseisessä järjestelmässä käytettäisiin myös pseudonyymiä todellisen identiteetin sijaan prosessissa, jossa liitytään RSU:iden kanssa. Täten järjestelmässä tarjotaan näin ollen ehdollinen anonyymiteetti, jotta saataisiin paljastettua haitallisilla ajoneuvoilla oleva todellinen henkilöllisyys. (Osibo ym. 2021)

Todennuksella tarkoitetaan puolestaan IoV:n tapauksessa seuraavaa. Todennus on olennainen osa IoV:n tietoturvaa. Sen avulla todetaan ja vahvistetaan eri käyttäjien ja järjestelmien henkilöllisyys IoV-ympäristössä. Kun joko uusi ajoneuvo tai solmu tulee IoV-verkkoon, pitäisi näiden henkilöllisyys vahvistaa ja todeta todennusjärjestelmällä, jotta tietoturva IoV:ssa säilytettäisiin. Todennukseen yleisesti kohdistuva tietoturvahyökkäys on esimerkiksi sybilhyökkäys. Se on autentikaatiota eli todennusta rikkova hyökkäys, jossa hyökkääjät väärentävät henkilöllisyytensä. Tähän esitetään ratkaisuksi, erityisesti V2V -viestinnässä, hajautettua kevyttä todennusjärjestelmää. Toinen kyseistä hyökkäystä vastaan ehdotettu torjuntakeino on puolustusmekanismi, joka käyttää anonyymiin sijaintiin perustuvaa reititystä. Tässä mekanismissa huomioon otetaan aikaisempi viestien vaihto vyöhykkeen yli. Sitten saapumiskulmaan perustuen solmut ryhmitellään erilaisiin vyöhykkeisiin. Vyöhykkeet luokitellaan vastaavasti vaarallisiin, turvallisiin ja niin edelleen. (Osibo ym. 2021)

4.5 Reunalaskenta

IoV on järjestelmänä pohjimmiltaan hajautettu. Sekä ajoneuvot, anturit ja RSU:t voidaan nähdä hajautettuina solmuina. Kyseisillä solmuilla on sekä kyky viestintään että kommunikointiin, mutta ne ovat myös kyvykkäitä suorittamaan paikallisia laskelmia. Täten erilaisten hajautettujen järjestelmien kehitys ja tätä kautta myös kehitys siinä, että vuorovaikutusta pystytään luomaan viestinnän ja laskennan välillä, tehostaa myös siis IoV:n käyttöönottamista. Esimerkiksi juuri reunalaskenta- ja myös pilvilaskentaominaisuuksien lisääntyminen tekee mahdolliseksi seuraavan. Ajoneuvoja pystytään käyttämään täten integroituna osana erilaisia reuna- ja pilvipohjaisia palveluita. Reunalaskennankin kautta ehkä pystyttäisiin kenties paremmin ymmärtämään viestinnän ja laskennan välistä vuorovaikutusta. Tämän kautta saatettaisiin puolestaan edelleen saada ideaa IoV:n perustavanlaatuisten puitteiden rakentamiseen. Ajoneuvojen reunalaskenta on myös potentiaalinen paradigma seuraavassa mielessä. Sen avulla mahdollisesti kyettäisiin mahdollistamaan massiivisen multimediasisällön tallentaminen välimuistiin ajoneuvojen läheisyydessä. Tällä puolestaan saataisiin mahdollisesti minimoitua sisällön toimitusviive IoV:ssa. (Li ym. 2020)

Edelleen erilaiset ajoneuvosovellukset ja myös siis IoV, ovat nousseet suureksi kiinnostuksen kohteeksi esimerkiksi teollisuuden taholta. Myös massiivisesti kasvava data ja sen käsit-

teleminen on noussut mietinnän aiheeksi. Edellä mainitusta johtuen erilaisten tietoliikenne-, tallennus- ja laskentaresurssien tarve on lisääntynyt. Tämä on puolestaan tarkemmin ottaen sitten edelleen johtanut vielä entistä tiukempiin suorituskykyvaatimusten vasteaikoihin. Lisäksi esimerkiksi vaatimukset verkon kaistanleveyden suhteen ovat kasvaneet. Mobiilireunalaskenta eli lyhennettynä MEC (engl. Mobile Edge Computing) on mahdollisesti yksi varteenotettava mahdollistava tekniikka näiden edellä mainittujen haasteiden ratkaisemiseen. Tällaisella mobiilireunalaskennalla tarkoitetaan tiivistetysti ETSI:n (European Telecommunications Standards Institute) määrittelemää sellaista verkkoarkkitehtuurikonseptia, jonka avulla on mahdollista toteuttaa pilvilaskentaominaisuuksia ja IT-palveluympäristö sekä matkapuhelinverkon että yleisesti ottaen minkä tahansa verkon reunalla. Reunalaskennan avulla pystytään esimerkiksi työntämään tehokkaita tallennus- ja laskentakapasiteetteja etäpilvestä verkkojen reunaan lähelle ajoneuvojen käyttäjiä. Tämä sitten puolestaan potentiaalisesti mahdollistaa sekä pienentyneen kaistanleveyden kulutuksen että tarpeeksi alhaisen latenssin. Reunalaskentaa on myös yritetty integroida erilaisten ajoneuvoverkkojen kanssa. Tämän seurauksena on muodostunut kokonaan uusi paradigma ja käsite. Se on nimeltään ajoneuvojen reunalaskenta eli lyhennettynä VEC (engl. Vehicular Edge Computing). (Liu ym. 2021)

VEC muodostuu MEC:n integroimisesta perinteisten ajoneuvoverkkojen kanssa. VEC:n avulla pyritään tuomaan ratkaisua siihen, että erilaiset laskenta-, viestintä- ja välimuistiresurssit saataisiin siirrettyä ajoneuvon käyttäjien läheisyyteen. Joten lupaavasta asiasta on kyse myös IoV:n kannalta. VEC:n avulla voi olla mahdollista vastata kasvaviin vaatimuksiin alhaisen latenssin ja suuren kaistanleveyden suhteen. Ajoneuvot omistavat VEC:ssä tietynlaisia laskentaan, viestintään ja tallennukseen liittyviä resursseja. RSU:iden avulla sitten puolestaan pyritään keräämään, käsittelemään ja tallentamaan erilaisia tietoja sijoittaen ne ajoneuvojen läheisyyteen. RSU:t toimivat siis useimmiten reunapalvelimina. Yksi ratkaisu ajoneuvojen rajallisen kapasiteetin suhteen onkin sitten mahdollisesti seuraava. Ajoneuvot voivat tarvittaessa siirtää latenssiherkimmät ja laskentaintensiivisimmät tehtävät reunapalvelimien käsiteltäväksi. Tämän avulla sitten taas puolestaan pystytään potentiaalisesti lyhentämään esimerkiksi vasteaikaa huomattavalla tavalla. Lisäksi VEC:n tapauksessa esimerkiksi sisällön pyytäjä pystyy hankkimaan tarvitsemansa sisällön välisolmuista suoraan ilman, että ydinverkkoon täytyy päästä ollenkaan. Tämän kautta puolestaan mahdollisesti pystyttäisiin vähentämään päästä päähän -latenssia. Lisäksi kaistanleveyden käytön tehokkuus verkos-

sa mahdollisesti tehostuisi. Kuitenkin kyseisen asian suhteen esiintyy vielä seuraavanlaisia haasteita ja ongelmia. Koska tallennustila on rajoitettu, jokainen välisolmuista ei välttämättä pysty tallentamaan kaikkea sisältöä välimuistiin. Näin ollen ongelmaksi muodostuukin esimerkiksi seuraavat asiat. Pohdinnan kohteena on edelleen esimerkiksi, että miten määritetään se, että mitä välimuistiin tulisi tallentaa. Lisäksi ihmetystä aiheuttaa määrittäminen sen suhteessa, että mihin välimuisteista tallennetaan ja kuinka määritetään välimuistikäytäntö. VEC:n avulla saadaan kuitenkin tulevaisuudessa potentiaalisesti mahdollisesttua erilaisia palveluita tehokkaasti. Tämä siksi, että sen avulla saadaan luultavasti yhdistettyä esimerkiksi uusia teknologioita, kuten esimerkiksi lohkoketju ja tekoäly, keskenään. (Liu ym. 2021) Täten myös VEC on siis IoV:n suhteen luultavasti potentiaalinen ratkaisun avain moniin sen haasteisiin tulevaisuudessa. Seuraavaksi vielä hieman tarkemmin VEC:n mukanaan tuomista erilaisista eduista ja tätä kautta edelleen mahdollisista ratkaisuideoista myös IoV:n suhteen.

VEC:n kautta mahdollistuu useiden erilaisten teknologioiden, kuten esimerkiksi SDN:n, NFV:n ja pilviteknologian, käyttö. VEC on osana mahdollistamassa myös autonomisten itseohjautuvien älykkäiden ajoneuvojen teknologiaa. VEC:n mahdollistamana pilviteknologialla on esimerkiksi seuraavanlaisia hyötyjä. Pilviteknologian kautta pystytään mahdollistamaan tehokkaat resurssit tallentamiselle. Lisäksi sen avulla mahdollistetaan tehokas laskentakapasiteetti. Yleensä pilviteknologia sijaitsee ikään kuin kaukana käyttäjistä, mutta VEC:n avulla asian suhteen pystytään tuomaan seuraavanlainen ratkaisu. VEC:n avulla pilviteknologian toiminnallisuus pystytään tuomaan verkon reunalle, jolloin VEC:n kautta pystytään pitämään yllä monipuolisesti erilaisia sovelluspalveluita. (Liu ym. 2021)

Ohjelmiston määrittämä verkko eli lyhennettynä SDN (engl. Software defined networking) on eräänlainen innovaatioverkkoarkkitehtuuri. Sen perusominaisuutena on se, että data- ja ohjaustaso pystytään irroittamaan toisistaan. SDN:n avulla pystytään toisin sanoen siis mahdollisesti yksinkertaistamaan verkon hallintaa. Verkkotoimintojen virtualisointi eli lyhennettynä NFV (engl. Network function virtualization) on seuraavanlainen teknologia. Sen tavoite on pyrkiä tarjoamaan uusi lähestymistapa esimerkiksi verkkopalveluiden hallintaan, käyttöönottoon ja suunnitteluun. Kyseinen teknologia tarjoaisi mahdollisia ratkaisuja seuraavan asian suhteessa. Kyseinen teknologia mahdollistaa verkkotoimintojen irroittamisen niistä fyysisistä laitteista, joissa verkkotoiminnot toimivat. Tällä puolestaan sitten pystyttäi-

siin mahdollisesti vähentämään merkittävällä tavalla erilaisia kustannuksia, kuten esimerkiksi pääoma- ja käyttökustannuksia. Lisäksi NFV:n kautta palveluiden käyttöönotosta pystytään luultavasti tekemään sekä tehokkaampaa että joustavampaa. Älykkäillä ajoneuvoilla on myös paljon omia resursseja käytettävissään muun muassa tallennusten ja laskennan tapauksessa. Tätäkin on mahdollista käyttää hyödyksi siten, että ajoneuvot pystyvät käsittelemään erilaisia tehtäviään myös paikallisesti tarvittaessa. Edelleen hyötynä tässä on se, että tätä kautta ajoneuvoverkkoilla olevaa taakkaa pystytään vähentämään. Näin ollen edelleen myös pystyttäisiin vähentämään verkon viiveitä. (Liu ym. 2021)

VEC:llä on myös monia etuja liittyen esimerkiksi vasteaikoihin, energiatehokkuuteen, tietojen varastointiin, läheisyyspalveluihin, kaistanleveyteen, kontekstitietoihin, ajoneuvon reunalaskentaan, tieturvallisuuteen, viihteeseen, liikennevalvontaan, reitin navigointiin, laskentavaltaisiin palveluihin ja tietojen yhdistämiseen ja louhintaan liittyen. Seuraavaksi vielä hieman tarkemmin näistä. Vasteaika on se toimitusaika, joka menee tietojen siirtämisessä reunapalvelimille ja takaisin. Lisäksi vasteaikaan lukeutuu myös se käsittelyaika, joka menee tietojen käsittelemiseen palvelimissa. VEC voi toimia vasteajan mielessä yhtenä ratkaisun avaimena ainakin siinä mielessä, että sen reunapalvelimet ovat lähellä ajoneuvoja ja niiden käyttäjiä. Täten eri tietojen siirtämisiin liittyviä suoritusaikoja voidaan saada huomattavasti lyhyemmiksi. Tämä olisi juuri yksi potentiaalinen ratkaisu erityisesti viiveherkissä sovelluksissa, jollainen IoV:kin on. Älyajoneuvot ja niiden mukana yleistyvät järjestelmät lisäävät räjähdysmäisellä tavalla energiankulutusta. VEC:n kautta pystytään myös potentiaalisesti tukemaan myös tätä puolta, kuten edeltäkin jo hieman tuli ilmi. Erilaisten ajoneuvoverkkojen ja niiden myötä lisääntyvien sovellusten myötä myös käsiteltävän datan määrä kasvaa räjähdysmäisesti. VEC on tämänkin asian suhteen yksi potentiaalinen keino. Sen avulla esimerkiksi pilvipalvelun sekä tallennus- että laskentaresurssit pystytään siirtämään ikään kuin verkon reunaan. Tämän kautta sitten puolestaan pystytään mahdollisesti lievittämään isoja kaistanleveysrasitteita. (Liu ym. 2021)

VEC:n myötä saataisiin hyötyjä myös tietojen varastoimiseen liittyen. Pilvessä tiedot ovat kaukana ajoneuvojen käyttäjistä, mutta VEC:n kautta tiedot pystyttäisiin tallentamaan reunapalvelimiin ajoneuvojen ja käyttäjien läheisyyteen. Tämä taas puolestaan mahdollistaa sen, että käyttäjät pääsisivät tallennettuihin tietoihin ajoissa. Lisäksi myös etäpilvellä olevaa tal-

lennustaakka pystytään lieventämään. Reunapalvelimet saadaan VEC:n avulla siis lähelle ajoneuvojen käyttäjiä. Tästä on myös se hyöty, että pystytään tarjoamaan erilaisia lähipalveluita käyttäjille. Tämän avulla voidaan myös potentiaalisesti parantaa käyttäjien käyttökokemuksia samalla kun varmistetaan myös kuitenkin liikenteen hallintakin tehokkaasti. VEC:n reunapalvelimien avulla myös pystytään todennäköisesti mahdollistamaan se, että ajoneuvojen käyttäytymiseen ja sijaintiin liittyen saadaan nimenomaan luotettavaa reaaliaikaista tietoa. Tällaista reaaliaikaisuuden mahdollista toimivuutta voidaan käyttää myös hyväksi monissa muissa asioissa, kuten esimerkiksi reaaliaikaisen sisällön ja palveluiden toimittamisessa ajoneuvojen käyttäjille. Lisäksi tällaisia reaaliaikaisia tietoja voidaan käyttää hyväksi myös esimerkiksi liikenne- ja tieturvallisuuden parantamisessa, kun erilaisia riskitietoja ja muita vastaavia, ennalta vaaran suhteen turvaavia, tietoja pystytään lähettämään teillä liikkuville reaaliaikaisesti. VEC:iä pystytään käyttämään monin tavoin hyödyksi myös esimerkiksi viihteen ja siihen liittyvien palveluiden suhteen. Ensinnäkin itseohjautuvat älyajoneuvot tulevat mahdollisesti yleistymään ja näin kuljettajille jää matkan aikana aikaa nauttia erilaisista viihdepalveluista esimerkiksi. Tällaisia viihdepalveluita pystytään todennäköisesti osittain mahdollistamaan VEC:n tarjoamien runsaiden laskenta- ja tallennusresurssien myötä. Lisäksi VEC:n avulla asioita pystytään tallentamaan välimuistiin tallentamalla ne yhteistyössä reunapalvelimien ja ajoneuvojen kesken. Tämä mahdollistaa viihdepalveluiden suhteessa todennäköisesti sen, että käyttäjät pystyvät hakemaan viihdesisältöä, esimerkiksi videoita, suoraan ilman etäpilvipalvelua. Tämä sitten puolestaan taas vähentää latenssia ja jälleen käyttäjien käyttökokemus paranee. (Liu ym. 2021)

Edelleen VEC:n ja sen reunapalvelimien avulla pystytään siis kattamaan eri viestintäalueita ja vastaanottamaan sieltä reaaliaikaista tietoa. Tätä voidaan käyttää hyödyksi paikallisten liikenneolosuhteiden analysoinnissa. Sitten taas edelleen tämän kautta voidaan esimerkiksi ohjata liikenteen sujuvuutta ja pystytään mahdollisesti ennalta ehkäisemään muun muassa liikenneruuhkien aiheutuminen. VEC:n avulla kerättyä reaaliaikaista tietoa voidaan myös käyttää hyödyksi erilaisissa navigoinnin palveluissa ja reittien analysoinneissa. VEC:n avulla pystytään siis tarjoamaan huomattavia sekä tallennus- että laskentaresursseja juuri nimenomaan esimerkiksi reaaliaikaisiin navigointijärjestelmiin. VEC:n avulla on ylipäänsä potentiaalisesti mahdollistettavissa automaatinen ajo. Tämä siksi, että VEC:n avulla on potentiaalista mahdollistaa myös erilaiset ajamisen palvelut, jo edelläkin mainituista syistä johtuen, to-

della alhaisella viiveellä ja lisäksi korkean luotettavuuden kera. VEC:n avulla erityisesti autonomisen ajon suhteessa pystytään ehkä tekemään mahdolliseksi se, että autonomiseen ajoon saadaan tehokas laskentaresurssin tuki taustalle tehtävien suorittamiseen. Edelleen hyötynä on muutenkin se, että VEC:n avulla sovelluksia voidaan siirtää reunapalvelimiin, joiden kautta sitten saadaan hyödynnettyä VEC:n tehokasta laskentaresurssia erillaisissa tilanteissa. VEC:n kautta myös kerättäisiin paljon dataa ajoneuvoihin liittyen. Jos VEC:ssä hyödynnetään syvällisesti tällaista dataa, hyötynä voi olla kenties myös se, että tällaisen hyödynnetyn tiedon kautta opitaan erilaisia asioita. Tämän kautta sitten taas puolestaan mahdollisesti voidaan oppia käyttämään opittua tietoa hyväksi esimerkiksi verkon suorituskyvyn parantamisessa tai muussa vastaavassa tiedon tehokkuuden edistämisessä. VEC:llä on kuitenkin edelleen monia haasteita ja tekijöitä, joista hieman mainittiin jo edellä, jotka kuitenkin vielä hankaloittavat senkin käyttöönottoa täysmittaisesti. (Liu ym. 2021)

Kuten edelläkin jo mainittiin, reunalaskenta myös yhteistyössä 5G:n kanssa tarjoaa mahdollisuuden käyttää laajan valikoiman erilaisia yhteyksiä ja tekniikoita samanaikaisesti ilman katkoja verkossa. Lisäksi, koska reunalaskentakehyksen perusviestintä on rakennettu 5G:n verkkoon, jolle puolestaan on ominaista alhainen latenssi ja iso datamäärä, on reunalaskenta potentiaalinen keino ratkaisuksi myös tässä suhteessa. Yleisesti ottaen, kuten jo edelläkin on tullut mainittua, reunalaskennan kautta pystytään upottamaan suuri määrä monimutkaisia laskelmia reunapalvelimiin lähemmäksi käyttäjiä. Tarkemmin sanottuna tienvarsiyksiköt eli RSU:t varustettaisiin näillä reunapalvelimilla, jotka sitten kykenisivät palvelemaan peittoalueellaan liikkuvia ajoneuvoja. Tehtävien siirtämistä voidaan tehdä sitenkin päin, että sitten kun taas puolestaan reunapalvelimien laskentakyky ylittyy, voidaan laskentatehtäviä siirtää taas takaisin pilvipalvelimelle. Kuten monesti tuli edelläkin jo esille, tämän kautta sitten mahdollisesti saadaan täytettyä tehokkaastikkin alhaisen latenssin ja kaistanleveyden tehokkuuden vaatimukset ja haasteet. Nämä edellä mainituthan ovat myös IoV:n keskeisiä haasteita ja vaatimuksia, joten mahdollista on, että reunalaskennan kautta saadaan edistettyä IoV:nkin kehitystä merkittävällä tavalla. Haasteita asian suhteen kuitenkin edelleen on. Esimerkiksi yksi iso haaste on reunapalvelimien suuresta määrästä aiheutuvat isot kustannukset.

Myös tekoälyllä on mahdollista todennäköisesti edistää reunalaskentaa siten, että tekoälyä integroidaan sen kanssa. Tekoälyn integroimisella reunalaskentaan pystytään mahdollista-

maan kenties esimerkiksi asianmukaisen reunapalvelun käyttöönotto ja joustavien resurssien ajoitus IoV:ssä. Tekoälyn integroinnin kautta pystytään mahdollisesti myös käyttämään kognitiivisia kykyjä esimerkiksi siten, että niin sanotussa reunaälykkäässä IoV-kehyksessä voitaisiin toteuttaa tehokas käsittely kriittisille sovelluksille. Lisäksi täten pystyttäisiin edelleen mahdollisesti esimerkiksi toteuttamaan alhaisen viiveen omaavan sisällön toimitus interaktiivisen viihteen tapauksessa. Lisäksi pystyttäisiin tekemään sellaisia tiedonsiirtoja, jotka olisivat tietoisia QoS-vaatimuksista. Reunalaskennan suhteen yksi ratkaisu voi olla myös se, että toteutettaisiin jonkinasteinen universaali MEC-kehys. Tällainen saatetaan tarvita, jotta reunalaskentaominaisuuksia pystytään parhaalla mahdollisella tavalla käyttämään sellaisissa ajoneuvoympäristöissä, jotka tukevat erilaisia sovellustyyppejä ja monikäyttöverkkoja. Lisäksi edelleen ajoneuvojen suuri liikkuvuuskin pystyttäisiin mahdollisesti huomioimaan samalla. Ratkaisu, erityisesti reunalaskentasovellusten työkuormituksen ja työn ajoituksen ruuhkautumisen ratkaisemiseksi, voisi olla esimerkiksi seuraava. Ratkaisu tähän voisi olla MEC:n hajauttaminen kahteen eri kehykseen nimeltään Autonomous Vehicular Edge (AVE) ja Hybrid Vehicular Edge (HVE). AVE:sta voisi olla seuraava hyöty. Sen avulla laskentakyky kenties saavutettaisiin havaitsemalla V2V -yhteyksissä lähimmät käytettävissä olevat resurssit ympäröivien ajoneuvojen sijainnin perusteella ilman minkäänlaista infrastruktuuria. Tällainen mainittu infrastruktuuri voi olla siis esimerkiksi RSU. Toisesta kehyksestä eli HVE:sta puolestaan olisi luultavasti hyötyä online-laskentaominaisuuksien suorittamisessa, sillä kyseiset laskentaominaisuudet suoritettaisiin monikäyttöverkon kautta V2I- ja V2V-yhteyksiä käyttäen. Konkreettisena hyötynä tästä olisi puolestaan se, että esimerkiksi saatavissa olevien resurssien hankinta pystyttäisiin tekemään verkossa mahdollisimman pienen odotusajan sisällä. (Osibo ym. 2021; Wu ym. 2021; Ning ym. 2021; Fadhil ja Sarhan 2020)

4.6 Koneoppiminen ja tekoäly

Koneoppimisen menetelmien kautta voidaan mahdollisesti saada ratkaistua haasteita liittyen erilaisiin dynaamisiin tie- ja ympäristöolosuhteisiin. Lisäksi myös muihin autonomisten ajoneuvojen ympäristön ja sijainnin tuntemuksen haasteisiin liittyen saatettaisiin saada ratkaisuja. IoV:n sovelluksista mahdollisesti pystytään tekemään kestäviä ja globaaleja myös siten, että käytetään tekoälyä. Tekoälyn avulla tullaan luultavasti saamaan jonkinlaisia ratkaisuja

aikaiseksi myös esimerkiksi liikenteessä tarvittavan älykkään päätöksenteon suhteen. IoV:ssa myös yksi mahdollisuus saada vältettyä esimerkiksi liikenneonnettomuuksia voi olla tekoälyn käyttäminen. Esimerkiksi IoT-teknologian ja tekoälyn mahdollistamien tekniikoiden yhteispelinä tullaan saamaan mahdollisesti aikaiseksi jonkinasteisia keinoja kontrolloida esimerkiksi auton nopeus- ja jarrutusjärjestelmää automaattisesti. (Singh ja Baljit 2021; Sleem, Noura ja Couturier 2020; Fadhil ja Sarhan 2020)

4.7 Luotettavuus, liikkuvuus, standardit ja rajoitettu verkon peittoalue

Luotettavuudessa on IoV:n kannalta kyse seuraavasta. IoV:ssa olevat erilaiset ajoneuvot, anturit ja kaikki muutkin aiheeseen liittyvät verkkolaitteet voivat mahdollisesti paikoitellen toimia heikosti eri syistä johtuen. IoV-järjestelmän tulisi kyetä toimimaan jotenkin riittävällä tavalla myös tällaisissa tilanteissa. IoV:ssa tulisi pystyä käsittelemään erilaisia viallisia kommunikaatioita tai tietoja. Esimerkiksi yksi luotettavuutta vaarantava tietoturvahyökkäyksen muoto on palvelunestohyökkäykset. IoV-järjestelmän tulisi pystyä torjumaan nämäkin. Kyse on siis toisin sanoen siitä, että IoV-teknologian on tarjottava ennen kaikkea turvallisuutta siinä oleville ajoneuvoille, sitä käyttäville kuljettajille ja muillekin käyttäjille. Toimiva taktiikka ratkaisujen osalta IoV:ssa tässä tapauksessa voisi olla se, että aina kehityksessä otettaisiin huomioon ajatus, että turvallisuus on aina tarjottava ja varmistettava ennen viihdettä. (Storck ja Duarte-Figueiredo 2020)

Yksi tärkeistä IoV:n keskeisiin haastetekijöihin liittyvistä ominaisuuksista on myös liikkuvuus, johon tulisi myös vielä saada aikaiseksi jonkin sortin toimivat ratkaisut. Liikkuvuudella tarkoitetaan IoV:n tapauksessa seuraavaa. IoV:ssa on hyvin vaikeaa pitää solmut kytkettyinä joka hetki, koska ajoneuvot ovat liikkuvia objekteja ja täten myös verkon topologia muuttuu kaiken aikaa. Sen lisäksi solmuille on myös täten hankalaa tarjota resursseja siihen, että asioita pystyttäisiin sekä lähettämään että vastaanottamaan reaaliaikaisesti. Liikkeessä olevien itseohjautuvien ajoneuvojen tapauksessa reaaliaikaisuudesta ei voi juuri poiketa, koska muuten seuraukset voivat olla kohtalokkaita. Ratkaisuna liikkuvuuteen olisi jokin sellainen keino, jolla pystyttäisiin takaamaan tarpeellisella tavalla se, että IoV-järjestelmä pystyy tarjoamaan hyvää verkon vakautta jatkuvassa liikkeessä oleville pysähtymättömille yhteyksille. (Storck ja Duarte-Figueiredo 2020)

Yksi IoV:n keskeisistä haasteista liittyy myös standardeihin. Eri puolilla maailmaa standardit vaihtelevat suuresti, mikä on ongelma IoV:n suhteessa. Erilaiset standardit tulisi ottaa huomioon, eikä niitä saisi loukata. Kaikista paras ja helpoin vaihtoehto IoV:n toteuttamisen kannalta olisi se, että siihen liittyen olisi esimerkiksi yksi yhteinen kansainvälinen standardi. Standardien vaihteluiden seurauksena erityisesti ajoneuvojen välinen tehokas V2V-viestintä ja sen toteuttaminen vaikeutuu huomattavasti. Ratkaisuna standardien suhteessa nähdään seuraava. Eri hallitusten tulisi toimia siten, että osallistettaisiin, rohkaistaisiin ja kannustettaisiin eri teollisuudenaloja yhteistyöhön teknologian kehittämisessä. Tämä voisi puolestaan nopeuttaa parhaiden käytäntöjen teknologista kehitystä ja käyttöönottoa. Lisäksi standardointi yksinkertaistuisi ja verkkojen yhteentoimivuuttaa mahdollisesti tuettaisiin avoimilla standardeilla. Tätä kautta myös edelleen tiedon jakelusta tulisi tehokkaampaa ja sujuvampaa. (Storck ja Duarte-Figueiredo 2020)

Yksi haaste on myös verkon rajoitettu peittoalue. Ajoneuvot yleisesti jakavat resurssejaan ajoneuvojen pilven, lyhennettynä VC (engl. Vehicular Cloud), kautta käyttäen joko matkapuhelinverkkoa tai jotain kiinteää infrastruktuuria, kuten esimerkiksi RSU:ita. Ongelma tässä suhteessa on kuitekin se, että ajoneuvo ei pysty julkaisemaan pyyntöään toisten ajoneuvojen kanssa silloin, jos ne jäävät verkon kantaman ulkopuolelle. Tässä suhteessa yksi ratkaisu voisikin olla mobiilivälittäjien käyttäminen palveluntarjoajina. Jokainen tällaisista mobiilivälittäjistä tallentaisi sitten aiempien ajoneuvopyyntöjen sisältämät tiedot ja paketit. Esimerkiksi linja-auto voisi toimia tällaisena liikkuvana välittäjänä. Tämä voisi toimia myös siksi, että juuri nimenomaan linja-auto kulkee ennalta määriteltyä entuudestaan tunnettua reittiä, joka kattaisi kaiken lisäksi ison osan kaupungista. Välitys esimerkiksi voisi toimia seuraavasti. Eli välittäjänä toimivaan linja-autoon lähetetään pyyntösanoma parhaan paketin löytämiseksi lähellä sijaitsevista ajoneuvoista. Linja-auto sitten taas puolestaan lähettää palveluntarjoajan tunnuksen eli ajoneuvon tunnuksen pyydettyyn ajoneuvoon. Näin saadaan sitten luotua yhteys ja tarvittavat palvelut välittyvät sinne, mihin on tarkoituskin. Siinä tapauksessa, että linja-auto ei löytäisikään niin sanottua osumapakettia, tällöin pyyntö välitettäisiin edelleen muille mahdollisille lähistöllä oleville välittäjille tai esimerkiksi RSU:ille. Ajoneuvopyyntö puolestaan perutetaan, jos käy sitten niin, että vastaavaa pakettia ei onnistuta löytämään. (Fadhil ja Sarhan 2020)

4.8 Big data

Big datalla tarkoitetaan terminä tiivistetysti seuraavaa. Sillä tarkoitetaan sellaisia massiivisia tietojoukkoja, jotka ovat rakenteeltaan suuria, monimutkaisempia ja monipuolisempia. Tällaisia tietojoukkoja on myös vaikea visualisoida, analysoida ja tallentaa muita prosesseja tai tuloksia varten. Big data on usein hyödyllistä tietoa yrityksille tai muille vastaaville organisaatioille. Ne voivat saada big datasta uusia syviä rikkaampia oivalluksia ja näin ollen myös ehkä etua kilpailijoihinsakin nähden. Tämän takia big dataan liittyvät toteutukset on myös sekä suoritettava että analysoitava yleensä mahdollisimman tarkasti.(Sagiroglu ja Sinanc 2013)

IoV:n yksi haasteistahan liittyy big dataankin, kuten edeltäkin kävi jo IoV:n haasteiden käsittelyn yhteydessä ilmi. Toisin sanoen IoV ja sitä kautta suuri määrä verkkoon yhdistettyjä autonomisia ajoneuvoja loisivat verkkoon massiivisen määrän dataa sekä tallennettavaksi että käsiteltäväksi. Esimerkiksi yksi ratkaisuidea big datan käsittelemiseksi IoV:ssa voisi olla mobiilipilvilaskenta. (Storck ja Duarte-Figueiredo 2020) On myös harkittu sellaisia keinoja, että ajoneuvot IoV:ssa toimisivat ikään kuin verkotettuina laskentakeskuksina. Eli ajoneuvot voisivat mahdollisesti auttaa läheisiä muita ajoneuvoja tietojenkäsittelyssä. Eli esimerkiksi resurssirajoitusten asettamista ja muutenkin resurssien jakamista voitaisiin toteuttaa ajoneuvojen kesken. Esimerkiksi kunkin ajoneuvon laskentaresursseja voitaisiin luultavasti käyttää esimerkiksi seuraavien reititysohjeiden laskemiseen big datassa IoV:n välityksellä. Lisäksi tienvarsiyksiköissä eli RSU:issa on yleensä moniytimisiä voimakkaita prosessoreja. Niissä on myös yleensä massiivinen tallennustila, joka toimii myös nykyaikaisissa järjestelmissä. Myös muita valtavia laskentaresursseja omaavia maalaitoksia ja niiden resursseja voidaan mahdollisesti käyttää hyödyksi myös big datan laskemisessa IoV:n kautta. Yksi keino laskennan jakamiseen voi olla ajoneuvojen ryhmittely, jossa lasketaan sitten esimerkiksi liikkuvuuden käsitteitä, kuten esimerkiksi viereisten ajoneuvojen kiihtyvyyttä ja nopeutta. (Xu ym. 2018) Yksi esimerkki tällaisesta tulikin jo edellä platooning-ratkaisun kohdalla. Autonomisten ajoneuvojen laskentakyvyn kehittämiseksi yhä enemmän big dataan liittyvä laskentatehtäviä voisi siis jakaa joustavasti ajoneuvojen, RSU:iden ja datakeskusten kesken. Tällä saataisiin luultavasti ikään kuin kehitettyä big datan arvoa IoV:n kautta syntyvien etujen kannalta. (Xu ym. 2018)

Ajoneuvot IoV:ssa tulevat sen lisäksi, että ne kuluttavat massiivisen määrän dataa, myös luomaan ja kuluttamaan valtavan määrän erityyppistä dataa. IoV:n myötä siirryttäisiin täysin uudenlaiseen big datan aikakauteen. Big datalla on IoV-yhteyksien kautta potentiaalista parantaa esimerkiksi IoV:n suorituskykyä viestintäprosessin tarkan mallintamisen ja tehokkaiden data-avusteisten IoV-protokollien suunnittelun kautta. Seuraavaksi hieman tarkemmin näistä potentiaalisista ratkaisuideoista. Esimerkiksi louhimalla sellaisia massiivisia tietoja, jotka ovat siirretty IoV:n kautta, on mahdollista saada määritetyksi seuraavaa. Tällaisella louhinnalla on mahdollista saada määritettyä tarkka IoV-viestintämalli käytännön parametrien, kuten kanavan kapasiteetin ja ominaisuuksien sekä tiedon saapumisen, arvioimiseksi. Jo aiemmin tehdyt mittauksetkin osoittavat, että pakettien toimitussuhde ja tila pystyttäisiin mahdollisesti laskemaan tiedonsiirron avulla. Lisäksi tällaisen tiedonsiirron avulla saataisiin mahdollisesti laskettua myös pakettien eri datapolkujen ajallinen korrelaatio eri viestintäkonteksteissa. Lisäksi yksi hyöty olisi se, että tulevaa datakuormitusta pystytään mahdollisesti ennustamaan big datan tehtävien saapumishetkien tallentamisen avulla. Lisäksi kyseisenlaisella tallentamisella pystytään mahdollisesti myös ennustamaan palveluaikaa, joka kuluu esimerkiksi V2V-kapasiteetin arviointiin. Tästä kyseisestä palveluajan arvioinnista on sitten taas edelleen se hyöty, että pystytään varaamaan vastaavia resursseja ennakolta, ennen kuin varsinaiset datatehtävät saapuvat. Tällaisia vastaavia resursseja voivat olla siis esimerkiksi kaistanleveys ja puskuritila. Big datan avulla IoV:n suhteen voidaan hyödyntää myös kanavadataa eli esimerkiksi kohinan tai signaalin voimakkuutta. Näitä voidaan käyttää hyödyksi esimerkiksi kanavaparametrien, kuten esimerkiksi polkuhäviön, arviointiin. Tällaisia kanavatietoja voidaan käyttää hyödyksi myös tarkkojen IoV-olosuhteiden toistamiseen, jollaisia voivat olla esimerkiksi IoV-kanava ja ajoneuvojen liikkuvuus. Tämä auttaa edelleen kustannusten vähentämisessä ja uusien V2X-protokollien kehittämisessä ja todentamisessa. Kyseisten protokollien kehityksessä ja todentamisessa auttaa erityisesti se, että kanavatietojen ja näin edelleen tarkan simuloinnin avulla, pystytään arvioimaan niiden suorituskykyä. (Zhou ym. 2020)

Lisäksi big datan päätelmiä IoV:n olosuhteista ja ominaisuuksista pystytään mahdollisesti käyttämään hyödyksi tehokkaiden dataohjattujen viestintäprotokollien suunnittelussa. Lisäksi big dataa voidaan hyödyntää myös IoV-tilatietueiden suhteessa seuraavanlaisesti. Havaittuja IoV-tilatietueita voidaan hyödyntää muun muassa kanavakapasiteetin ja liikennekuormi-

tuksen ennustamisessa. Tätä voidaan sitten edelleen hyödyntää luultavasti esimerkiksi IoV:n suorituskyvyn parantamisessa. Lisäksi saadusta big datasta voidaan käyttää IoV-yhteyksien parantamiseen erilaisia saatuja kontekstitietoja, kuten ajoneuvojen nopeuksia ja sijainteja. Tällaisten kontekstitietojen kautta voidaan mahdollisesti myös ennustaa signaalin vaihtelua, mikä voi auttaa esimerkiksi erilaisissa ajoneuvojen liikkuvuuden vuoksi aiheutuvissa kanavan muutoksissa. Sijaintietoihin perustuvaa liikkuvuuden ennustamista voidaan kenties käyttää hyväksi myös siinä, että IoV:ssa varataan tarpeeksi kaistanleveyttä. Tällä saadaan sitten puolestaan vähennettyä pakettien katoamisnopeutta. Big datan avulla IoV mahdollisesti kykenee olemaan myös tietoisempi useammista konteksteista liittyen kommunikaatioon. Lisäksi sen avulla IoV on todennäköisesti tietoisempi myös erilaisista tietotyypeistä, signaalien vaihtelusta ja kaistanleveydestä. Tätä kaikkea sitten edelleen pystyttäisiin käyttämään IoV:n mukautumiskyvyn ja resurssien käytön parantamisessa ja tehostamisessa. (Zhou ym. 2020)

Big dataankin liittyen esiintyy kuitenkin edelleen erilaisia haasteita, joka koituu vielä tällä hetkellä ongelmaksi myös IoV:n kannalta. Big datan kannalta riskejä liittyy esimerkiksi tietoturvallisuuteen ja epäjohdonmukaiseen tiedonkeruuseen liittyen. Riskinä on esimerkiksi ensinnäkin se, että kolmannelle osapuolle toimitettavat tiedot saattaa päästä pahimmassa tapauksessa tietomurron seurauksena vuotamaan esimerkiksi kilpailijoille tai asiakkaille. Riskinä on myös se, että säännöllisen tiedonkeruun sijaan tarvittaisiin tässä tapauksessa reaaliaikainen jatkuva tiedonkerääminen ja analysointi. Tämä taas puolestaan edellyttäisi merkittäviä strategisia toimia. Lisäksi siitä aiheutuisi suuret kustannukset. Lisäksi riskinä on myös se, että usein suurten tietojoukkojen keräämisessä käytetyt työkalut ovat epätarkkoja. Yksi haaste ja riski big datan suhteen on myös ulkoistettujen tietojen luottamuksellisuus, saatavuus, eheys ja yksityisyys. Haasteita aiheuttavat myös esimerkiksi erilaiset ongelmat langattomien yhteyksien suhteessa. Langattomiin yhteyksiin voi vaikuttaa haitallisesti muun muassa erilaiset infrastruktuurit, kuten sillat, tunnelit tai korkeat rakennukset. Taajuusresurssipula on yksi haaste. Haasteita tulee vielä myös ajoneuvojen suuren liikkuvuuden ja ajoneuvojen dynaamisen tiheyden suhteen, jonka seurauksena IoV-datatehtävät vaativat erilaista datan lähetysnopeutta ja suoritusviivettä. IoV:lta puuttuu myös globaali koordinointi, koska se muodostuu liityntäverkosta, joka on heterogeeninen. Ongelmaa aiheutuu myös siitä, että IoV:lle tulevaa big dataa tulee monesta eri lähteestä. Tämän vuoksi pitäisi tulevaisuudessa IoV:n kattavuutta saada parannettua ja laajennettua laajalla etenemisalueella ja korkealla signaalien-

läpäisykyvyllä, koska voi olla mahdollista, että eri tietolähteet leviävät laajoillekin alueille. Big datan ongelmana on myös se, että kuinka pystytään valitsemaan juuri oikeat ajoneuvot sekä oikeaan aikaan että oikeaan paikkaan. Tämä on ongelma siksi, että pitäisi saada kerättyä, tallennettua ja jaettua tietoja muille IoV-verkoissa oleville ajoneuvoille siten, että myös pitkän aikavälin verkonhallinta pystyttäisiin saavuttamaan. Tämän ongelman ratkaiseminen jollain keinolla saattaisi myös edistää merkittävällä tavalla IoV:lla olevia big dataan liittyviä haasteita. (Kayarga ja Kumar 2021; Zhou ym. 2020; Fadhil ja Sarhan 2020)

4.9 Tietoturvallisuus, turvallisuus ja yksityisyys

IoV tulee olemaan avoin julkinen verkko. Lisäksi se tulee sisältämään useita erilaisia integroitavia teknologioita, standardeja ja palveluita. Täten IoV on myös samaan aikaan haavoittuvainen erilaisille kyberhyökkäyksille ja tunkeutumisille. Jos tällaisia pääsee tapahtumaan IoV:ssa, seuraukset voivat olla pahoja. Voi aiheutua sekä erilaisia tietosuojavuotoja että jopa erilaisia onnettomuuksia ja muita fyysisiä vahinkoja esimerkiksi. IoV on myös hyvin riippuvainen langattomasta tietoliikenteestä esimerkiksi silloin, kun pyritään hallitsemaan liikennevirtoja. Tämäkin tekee IoV:sta alttiin erilaisille tietoturvahyökkäyksille. Kaiken tämän takia erittäin tärkeää IoV:n täysimääräisen toteuttamisen aloittamiselle on, että sille pystytään luomaan jonkinlainen tehokas yksityisyys- ja tietoturvajärjestelmä. (Storck ja Duarte-Figueiredo 2020; Fadhil ja Sarhan 2020) Tietoturvaan kohdistuvia erilaisia hyökkäyksiä ja muitakin keskeisimpiä IoV:n tietoturvavaatimuksia tulikin lueteltua jo edelle, mutta seuraavaksi vielä tarkemmin muutamia erilaisia mahdollisia ratkaisuideoita IoV:n tietoturva-asioihin liittyen.

Yleisiä taktiikoita ja lähestymistapoja IoV:n turvallisuusongelmien ratkaisemiseksi ovat esimerkiksi seuraavat. Yksi mahdollinen tapa voisi olla esimerkiksi todennus- ja avaintenhallintaprosessin käyttäminen. Tällaista prosessia voitaisiin käyttää erilaisten entiteettien, kuten esimerkiksi ajoneuvojen ja tienvarsiyksiköiden eli RSU:iden, välillä sumupalvelimien kanssa. Edistystä tietoturvan suhteen saatettaisiin saada myös käyttämällä kyseisenlaista prosessia esimerkiksi pilvipalvelimen ja sumupalvelimien välillä. Toinen yleisesti esitetty lähestymisidea tietoturva-asioiden ratkaisemisen suhteen IoV:ssa on esimerkiksi salattu data tai salattu viestintä. Tällaisen lähestymistavan eli erilaisten salaustekniikoiden käyttämisen kautta

pystyttäisiin todennäköisesti muun muassa suojaamaan reunalaitteiden tuottamaa sähköistä dataa tilanteessa, jossa sitä siirretään sumupalvelimien ja pilvipalvelimen välillä. Tällainen data voi siis olla esimerkiksi ajoneuvojen käyttäjien henkilöllisyyksiä. Tällaisessa lähestymistavassa salaustekniikoita voivat olla esimerkiksi Data Encryption Standard (DES) -algoritmi tai vaikkapa Advanced Encryption Standard (AES) -algoritmi. Säännöllinen verkon valvonta on myös yksi keino pönkittää IoV:n tietoturvan luotettavuutta seuraavanlaisissa tapauksissa. Tällaista tekniikkaa voidaan käyttää hyödyksi esimerkiksi sumujärjestelmien verkon resurssien tarkkailussa, jotta havaittaisiin kaikki mahdolliset epäilyttävät toiminnot ajoissa, ennen kuin mitään pahempia seurauksia pääsee aiheutumaan. Säännöllistä verkon valvontaa voisi tehdä myös erilaisten verkkoskannausmekanismien kautta. Tällaiset mekanismit voisivat olla joko dynaamisia, staattisia tai molempia. Tällainen laaja verkkoskannaus toimii yleensä virustorjuntaa tai esimerkiksi palomuuria hyödyntävänä ja vahvistavana keinona kaikkien epäilyttävien pakettien kiinnisaamisessa. Lisäksi langattomat suojausprotokollat voivat olla myös keino IoV:n tietoturvan parantamisen suhteen. Tällaiset protokollat voivat olla ratkaisu erityisesti suojatun tiedonsiirron toteuttamisessa sumuympäristöissä. Esimerkiksi monet IoT-laitteet on kytketty juuri nimenomaan sumuympäristöön, jossa ne lähettävät arkaluontoisiakin tietoja langattomasti. Tällaisia langattomia suojausprotokollia ovat nimeltään esimerkiksi Wi-Fi Protected Access (WPA) ja sen eri versiot, kuten WPA2 ja WPA3. Tällaiset langattomat suojausprotokollat voivat mahdollisesti toimia tehokkaana ratkaisuna myös esimerkiksi Sybil-tietoturvahyökkäysten torjunnassa. (Fadhil ja Sarhan 2020)

4.10 Muita ratkaisuideoita

Ratkaisu esimerkiksi ajoneuvon sisäisten tietojen eli lyhennettynä IVI (engl. In-Vehicle Information) soveltamiseen itseohjautuvissa autonomisissa ajoneuvoissa voisi olla esimerkiksi jonkinasteinen yhteinen IVI-standardijärjestelmä, jollainen nyt juuri nimenomaan puuttuu. Lisäksi asian suhteen saattaisi auttaa myös se, että ei käytettäisi niin paljon rajoitettuja hallintatekniikoita, vaan sallittaisiin myös enemmän avoimen lähdekoodin omaavia sovelluksia. Lisäksi erilaisten QoS:ihin liittyvien haasteiden, kuten dataviiveiden, yhteyksien katkeamisten ja rajoitetun laajakaistan, suhteen ratkaisuja voisivat kenties tuoda jonkinlaiset monitiereititysmekanismit ja sisäänpääsyn hallinta verkon istuntojen suhteen perustuen kaistanle-

veyden saavutettavuuteen. Ajoneuvojen tarkan ja turvallisen sijainnin jakamiseen IoV:ssa liittyy ongelmia, kuten paikannuksen ja sijainnin tarkkuus, yksityisyys ja varmistus. Näiden ongelmien ratkaisemiseksi tulisi saada kehitettyä esimerkiksi jokinlainen tarpeeksi turvallinen tietojen jakamismekanismi. Lisäksi läheisten autojen välille tulisi jollain keinolla saada luotua riittävä luottamus tietojen jakamiseen. Myös ajoneuvojen tarkkojen nopeuksien havaitsemisen kautta jollain keinoilla voitaisiin saada aikaiseksi edistystä myös tämän kyseisen asian suhteessa. Erilaisten liikenneonnettomuuksien välttämiseksi IoV:n kannalta ratkaisuna voisi olla käyttää IoT-teknologiaa ja tekoälyn tarjoamia tekniikoita hyödyksi jollain sellaisella toimivalla tavalla, jolla pystyttäisiin tarvittavalla tavalla kontrolloimaan autojen nopeuksia ja jarrutuksia automaattisesti. (Fadhil ja Sarhan 2020)

5 Tulokset ja pohdinta

Tässä luvussa avataan vielä tiivistetymmässä muodossa kertaalleen tutkituista lähteistä esiin nousseet tulokset sekä IoV:n haasteisiin että niihin löytyneisiin mahdollisiin ratkaisuihin liittyen. Mukana on myös hieman omaa pohdintaa.

5.1 IoV:n haasteet

Tutkitun lähdeaineiston perusteella selvisi, että IoV:n suhteen on vielä paljon erilaisia haasteita ja ongelmia, jotka estävät sen täysimittaisen toteuttamisen. Seuraavaksi tiivistys löytyneistä IoV:n keskeisimmistä haasteista. Selvisi, että IoV:n yksi suurimmista haasteista liittyy lähetysviiveeseen eli latenssiin. IoV:n tapauksessa kyse on liikkuvista ajoneuvoista, joten tarpeeksi alhainen latenssi ja sen toimivuus olisi erityisen kriittinen tekijä. Latenssin suhteen pitäisi pystyä kehittämään sellaiset keinot, joilla se täyttäisi laatuvaatimusten ja muutenkin tarpeen vaatimat kriteerit riittävällä tavalla.

Yksi IoV:n suurimmista haasteista näytti taas puolestaan liittyvän massiivisten datamäärien hallintaan eli toisin sanoen big dataan. Jos IoV otettaisiin käyttöön, käsiteltäväksi tulisi erittäin suuri määrä erilaista dataa, kun yhdistettynä olisi lisäksi massiivinen määrä erilaisia laitteita. IoV-verkkojen heterogeenisen luonteen vuoksi myös samassa yhteydessä tietojen analysoiminen, tallentaminen, integroiminen, yhdistäminen ja niihin liittyvä päätösten tekeminen ovat tällä hetkellä vielä vaikeasti toteutettavissa IoV:n suhteen. Datan hallinnan suhteen tulisi siis saada myös kehitettyä toimivat keinot tarpeen vaatimalla tavalla.

Selvisi myös, että IoV:n yksi suurimmista haasteista on sen liikkuva luonne. Ajoneuvot ovat liikkeessä, mikä sitten puolestaan taas aiheuttaa solmujen suuren liikkuvuuden. Tämä saattaa aiheuttaa erilaisia katkoksia ja solmut tulisi onnistua pitämään kytkettyinä tarpeen vaatimalla tavalla. Toisin sanoen IoV:n tapauksessa datan lähettäminen ja vastaanotto tulisi tapahtua reaaliaikaisesti. Tähänkään ei ole vielä keksittyä tarpeeksi kattavia keinoja. Lisäksi verkkoyhteyksien skaalautuvuus on myös IoV:n yksi keskeisin haaste. Liikkuvuudesta ja liikenteen vaihtelevasta tiheydestä aiheutuu vaihtelevaa kuormitusta verkkoyhteyksille ja ongelmia siis luultavasti esiintyisi tämänkin johdosta. IoV:n verkkoyhteydet tulisikin jotenkin saada niin

vankalle tasolle, että tämäkin pystyttäisiin käsittelemään tarpeen vaatimalla tavalla. Kaiken lisäksi tulisi myös saada säilytettyä tarpeeksi hyvä tiedonsiirtonopeus. Lisäksi IoV:n suurena haasteena on monenlaisia tietoturvaan ja yksityisyyteen liittyviä uhkia, jotka IoV:n toteuttamisen myötä tulisivat ongelmaksi. Näidenkin suhteen tulisi saada niin kattavat ratkaisut kehitettyä, että IoV:n luotettavuus ja turvallisuus saataisiin tarvittavalle tasolle. Yksi IoV:n haasteista on myös paljon eri alueittain eroavat standardit ja niiden huomioiminen eri toimissa. Mainittiin myös, että hyötynä standardien yhtenäistämisestä voisi olla IoV:n kehitystyön tehostuminen. Yhtenä haasteena on myös IoV:n toteuttaminen energiatehokkaasti tarpeeksi alhaisten kustannusten kera. Hyvällä energiatehokkuudella varmistettaisiin IoV:ssa sekä energian ehtymättömyys eri laitteissa ja sovelluksia että verkkoyhteyksien pitkä käyttöikä.

Yhdeksi IoV:n haasteeksi mainittiin myös IoV-teknologian sopeutumiskyky erilaisten tekijöiden kesken. IoV:n sopeutumiskykyyn voi vaikuttaa eri kulttuurien eroavaisuudet. Lisäksi IoV:n käyttöönotto, siltä vaadittavan infrastruktuurin rakentaminen ja sen sopeuttaminen eri alueiden kesken tulisi vaatimaan todella isoja kustannuksia. Muutenkin iso haaste IoV:n kannalta liittyy juuri tarpeellisen infrastruktuurin rakentamisesta aiheutuviin suuriin kustannuksiin. Myös lainsäädännön suhteen saattaisi IoV:n myötä tulla täysin uudenlaisia tilanteita pohdittavaksi. Myös erilaisia eettiseen ja moraalisen päätöksentekoon liittyviä seikkoja ja tilanteita on arvioitava IoV:n tapauksessa, joka voi olla haastavaa.

Lähteiden pohjalta kerätyn aineiston perusteella voisi todeta siis seuraavaa. Haasteita ja ongelmia näyttäisi olevan vielä aivan liikaa ratkaistavaksi, ennen kuin IoV:n konkreettinen toteuttaminen pystyttäisiin aloittamaan tarpeeksi turvallisella, luotettavalla ja toimivalla tavalla.

5.2 Ratkaisut

IoV:n haasteisiin pyrittiin löytämään lähdeaineiston pohjalta jonkinlaisia ratkaisuideoita. Löytyneestä ja kerätystä aineistosta suurin osa oli tehty lähivuosien aikana. Kerätyn aineiston pohjalta löytyi ja havaittiin seuraavanlaisia tuloksia.

5.2.1 Lohkoketju

Ensinnäkin kerätyn aineiston pohjalta havaittiin, että lohkoketju ja sen tarjoama teknologia on yksi lupaavimmista ja isoimmista ratkaisun avaimista juuri nimenomaan IoV:n toteuttamisen mahdolliselle onnistumiselle tulevaisuudessa. Kerätyn aineiston pohjalta havaittiin muutenkin, että IoV:n toteuttamisen myötä tulisi hyötyjä, mutta myös monia uudenlaisia haasteita ja uhkia. IoV olisi alttiina monille uusille uhkille, kuten tietoturvauhkille ja tietoturvahyökkäyksille. Tietoturvan ja IoV:ia käyttävien osapuolien yksityisyydenkin takaaminen ovat yhtiä IoV:n keskeisimmistä ja suurimmista haasteista. Löytyneistä tuloksista havaittiin, että lohkoketjulla on IoV:n suhteessa monia muitakin hyötyjä. Kerätystä aineistosta nousi kuitenkin esiin, että useimmiten kun lohkoketjua käytettäisiin IoV:ssa, käytettäisiin sitä juuri nimenomaan turvallisuuden parantamiseen. Kerätystä aineistosta voi havaita, että lohkoketjulle on ominaista salattujen ketjutettujen lohkorakenteiden käyttö. Tällaisen lohkorakenteen kautta kyettäisiin sitten toteuttamaan monia hyödyllisiä asioita IoV:n kannalta.

Aineistosta havaittiin, että IoV:n toteutuksen myötä ajoneuvojen välinen kommunikointi ja liikkuvan datan määrä kasvaisivat todella massiivisella tavalla. Pelkästään jonkun keskitetyn pilvipalvelun käyttäminen IoV:ssa ei näin ollen enää todennäköisesti toimisi, vaan muuttuisi tehottomaksi. Pahimmassa tapauksessa koko IoV-järjestelmä saattaisi romahtaa esimerkiksi jonkinasteisen ylikuormittumisen seurauksena. Lohkoketjun lohkorakenteen kautta saataisiin luultavasti tuotua ratkaisu tähänkin IoV:n haasteeseen. Kerätystä aineistosta havaittiin, että lohkoketjun lohkot koostuvat tallennetuista tiedoista. Näissä lohkoissa on siis aina linkit seuraaviin ja edellisiin lohkoihin. Lohkot sisältävät myös tietoja eri solmuista. Tällaisia solmuja ovat tässä tapauksessa yleensä juuri esimerkiksi ajoneuvot ja niihin liittyvät tiedot. Myös esimerkiksi tienvarsiyksiköt eli RSU:t voivat olla tällaisia solmuja. Lohkoketjun tuomana ratkaisuna onkin nyt tällaisissa tapauksissa se, että tällaiset solmut voivat olla lohkoketjussa kytkettyinä erillisiin palvelimiin. Näin ollen eri palvelimet pystyvät tallentamaan tietoja solmuista esimerkiksi yksitellenkin sekä alilohkoina että yhdistettynä pääpilvipalvelimeen. Lohkoketju tuo hajautetun ominaispiirteensä avulla tarjolle erilaisia vaihtoehtoja sen sijaan, että IoV-verkoissa olisi vain jokin yksi keskitetty organisaatio.

Lohketjun yhdeksi pääominaisuuksista osoittautui sen avulla tehtävä hajauttaminen. Lohketjun kautta olisikin mahdollista kenties toteuttaa hajautetut IoV-verkot. Sen myötä pystyt-

täisiin ehkä luomaan IoV-verkkoihin hajautettuja kokonaisuuksia, joita voivat olla esimerkiksi ajoneuvot, RSU:t ja ihmiset. Ratkaisun avaimena IoV:n kannalta tässä hajauttamisessa saattaisi olla erityisesti seuraava. Sen kautta pystyttäisiin poistamaan nykyinen IoV-verkon keskitetty päätöksenteko. Tämän myötä sitten hajautetut kokonaisuudet voisivat itsenäisesti hallita omaa toimintaansa. Positiivisena mahdollisena seurauksena IoV:n kannalta edellä mainitusta olisi myös IoV-järjestelmän yksinkertaistuminen ja tätä kautta myös sen käyttäjäkokemusten parantuminen sen tarjoamiin palveluihin liittyen. Lisäksi luultavasti IoV:ssa mahdollistuisi tehokkaat nopeat tapahtumat, reaaliaikaisuus ja älykkäät sopimukset ja niiden kautta edelleen erilaisten transaktioiden, kuten maksutapahtumien helpottuminen. Lisäksi luultavasti tiedon jakamisen luotettavuus paranisi. Myös erilaiset vakuutukset, pysäköintimaksut ja verot pystyttäisiin tekemään aikatehokkaammin.

Lohkoketjun kautta myös mahdollisesti IoV:n tietoturvallisuus ja sitä kautta myös koko IoV:n turvallisuus parantuisi. Selvisi, että lohkoketjun myötä mahdollistuu sekä synkronointi että replikaatio kaikkien sellaisten vertaissolmujen välillä, jotka ovat verkkoon kytkettyjä. Näin ollen verkon pätkimiset ja katkeamiset luultavasti vähentyisivät. Lisäksi, toisin kuin normaalissa keskitetyssä järjestelmässä luultavasti olisi, yhden solmun mahdollinen vaarantuminen ei nyt siis kaataisi koko järjestelmää kerralla. Lisäksi lohkoketjuissa käytettävät salaustekniikat myös parantaisivat luultavasti tietojen yksityisyyttä ja koko tietoturvaa.

Lohketjun kautta tulevana hyötynä olisi myös se, että pilvijärjestelmillä oleva riippuvuus tietojen tallentamisesta ja hallinnasta pystyttäisiin poistamaan. Selvisi myös, että lohkoketjun älykkään sopimuksen kautta pystyttäisiin toteuttamaan se, että ajoneuvopalveluja järjestäisivät ja ylläpitäisivätkin lohkoketjuverkoston osallistujat itse. Tästä etuna olisi sitten taas puolestaan ajoneuvopalveluihin liittyvien käyttökustannusten aleneminen. Lohkoketjun lohkorakenteen avulla pystyttäisiin myös mahdollistamaan se, että erilaiset tiedot pysyisivät muuttumattomina ja näin pystyttäisiin jälleen parantamaan tietoturvaa, kun erilaiset tietojen laittomat muokkaukset pystyttäisiin luultavasti estämään.

Selvisi myös, että lohkoketjun avulla mahdollistuisi luultavasti IoV:ssa palvelun tarjoajien ja pyytäjien välisen suoran yhteyden toteuttaminen. Näin ollen jälleen mahdollistuisi turvallinen tiedonjako RSU:iden ja ajoneuvojen välillä. Tällainen suora kommunikointi luultavasti vähentäisi myös latenssia. Lohkoketjun konsensuksen kautta pystyttäisiin myös todennäköi-

sesti saamaan ratkaisuja sellaisten heterogeenisten kokonaisuuksien yhdistämisessä, jotka eivät täysin luota toisiinsa. Lisäksi lohkoketjun älykäs sopimus saattaisi auttaa sellaisissa tilanteissa, joissa päätöksiä tehdään ilman mitään luotettavaa tahoa. Jälleen tietoturva IoV:ssa todennäköisesti paranisi edellä mainitun myötä.

Kaiken kaikkiaan siis selvisi, että lohkoketjun avulla olisi potentiaalista saada erilaisia ratkaisuja latenssin vähentämisessä, ison tallennustilan tarjoamisessa lohkoketjun rakenteen kautta, reaaliaikaisen tiedon keräämisessä, tallentamisessa, käsittelyssä hajautetusti, IoV:n suorituskyvyn parantamisessa ja IoV:n erilaisiin toimiin liittyvän automaation toteuttamisessa. Lisäksi lohkoketjurakenteen kautta luultavasti myös tietoturvaa saataisiin parannettua. Näin ollen IoV:n turvallisuus ylipäätään ja luottamus siihen kasvaisi. Lisäksi tietojen yksityisyys IoV:ssa pysyttäisiin todennäköisesti takaamaan. Myös tiedon eheys mahdollisesti parantuisi. Tietoja pystyttäisiin lisäksi tarkistamaan luultavasti hyvin jälkikäteen, mikä olisi hyvä asia erilaisten palvelujen, kuten esimerkiksi vakuutuspalveluiden vakuutuskorvausten arviointien kannalta. Lisäksi tämän johdosta myös luultavasti erilaiset asiayhteyteen liittyvät rikokset ja rikkomukset vähenisivät. Lohkoketju tarjoaa myös erilaisia kryptografisia suojauskeinoja, jotka jälleen edistäisivät tietoturvaa monelta eri kantilta. Kuten edeltäkin jo ilmeni, lohkoketjun hajautettu luonne myös parantaisi luultavasti koko IoV:n toimintaa ja suorituskykyä, kun se ei olisi enää niin altis erilaisille häiriöille. Lisäksi toiminta mahdollisesti tehostuisi, kun ei olisi enää vain yhtä hallitsevaa tahoa. Todennäköisesti myös, kun nyt mikään yksittäinen taho ei tekisi enää ainoastaan päätöksiä, vaan ne tehtäisiin yhdessä, päätöksetkin saattaisivat olla tämän myötä avoimempia, luotettavampia ja läpinäkyvämpiä.

Edellä tuli esiin lohkoketjun tarjoamat hyvät puolet, mutta edelleen haasteita ja huonojakin puolia löytyy. Vaikka lohkoketju sinällään ratkaisuja paljon tarjoaisikin, silti on riskinä, että lohkoketjun ominaisuudet eivät välttämättä toimikaan tarpeellisella tavalla IoV:ssa. Esimerkiksi tietoturvan suhteen voi silti mahdollisesti löytyä vieläkin epäkohtia, vaikka sinänsä lohkoketju keinot sen suhteen tarjoaisikin. Lisäksi IoV-verkko tulisi saada ensin ominaisuuksiltaan niin varmalle tasolla, että lohkoketjun käyttöönotto, joka muutenkin edellyttäisi suurta laskentatehoa, olisi käytännössä edes mahdollista. Lisäksi lohkoketju ei ole edes vielä teknologia, joka olisi laajalti hyväksytty käyttöönotettavaksi. Tämä taas puolestaan heikentää lohkoketjunkin luotettavuutta. Lisäksi lohkoketjun ammattilaisista on pulaa.

Kaiken näiden kerätyistä lähteistä esiin nousseiden asioiden perusteella vaikuttaisi siltä, että lohkoketju olisi erittäin lupaava, ellei jopa lupaavin teknologia IoV:n haasteiden ja erityisesti sen tietoturvaongelmien ratkaisuun. Lohkoketju jo itsessään luonteeltaan tarjoaisi erinomaisen pohjan ja monia eri ratkaisuja IoV:n tietoturvan parantamiseen. Lisäksi näyttäisi, että sen hajautetun rakenteen avulla saataisiin myös mahdollisesti ratkaisuja aikaan myös ihan yleisesti koko IoV:n suorituskyvyn ja toimintakyvyn kannalta. Eli potentiaalisia ratkaisuja tulisi aika lailla kaikkien IoV:n keskeisten haasteiden, kuten latenssin, massiivisen datan hallinnan, tietoturvan, suorituskyvyn ja reaaliaikaisuuden suhteessa. Silti ongelmia luotettavuuden ja myös kyseisten teknologioiden integroimisen suhteen muutenkin näyttäisi esiintyvän vielä hieman liikaa. Edellä esiin tulleet haastekohdat tulisi tavalla tai toisella saada ratkaistua niin luotettavasti, että täysi konkreettinen käyttöönottaminen voisi tapahtua. Lohkoketju kuitenkin muuten itsessään näyttäisi erittäin varteenotettavalta monipuoliselta pohjalta IoV:n toiminnan toteuttamiseen.

5.2.2 5G

Lähteiden perusteella selvisi, että ensinnäkin 5G:n avulla pystytään poistamaan ne rajoitukset, joita 4G:llä vielä oli. Esimerkiksi lähetysnopeus kasvaa 5G:n myötä merkittävästi. 5G tulee kasvattamaan valtavasti potentiaalia IoT:n, ITS:n ja IoV:n toteuttamisen suhteen ja avaa aivan uudenlaisia mahdollisuuksia. Tutkitun perusteella havaittiin, että 5G:n myötä luultavasti pystytään tarjoamaan mahdollisuus verkon ylläpitämiseen kaikkialla kaiken aikaa. Verkon ylläpitäminen todennäköisesti mahdollistuu myös sekä tiheästi asutetuilla alueilla että tilanteissa, joissa liikkuvuus on suurta. Lisäksi 5G:n myötä luultavasti mahdollistuu määrältään massiivisten samanaikaisten yhteyksien ylläpitäminen, joka on myös merkittävä IoV:n käyttöönoton mahdollistava tekijä. Tämä kaikki johtaa edelleen sitten myös siihen, että potentiaalista mahdollisuutta tarjotaan kaikkien verkossa olevien laitteiden yhdistämiseen. 5G:n kautta pystytään myös tarjoamaan alhainen latenssi, joten viestintäviiveet ajoneuvojen välillä sekä ajoneuvojen että muiden laitteiden välillä saadaan todennäköisesti vähenemään merkittävästi. Lisäksi myös luultavasti erilaisten IoV-järjestelmien välinen yhdistettävyys paranee. 5G parantaa myös verkon jatkuvuutta. 5G:n avulla siis kaiken kaikkiaan pystytään luultavasti tarjoamaan yhteydet sekä turvallisesti että toimivasti laajalle alueella. Tämän kaiken lisäksi

yhteydet olisivat todennäköisesti myös vielä nopeita kauttaaltaan. Tämä kaikki juuri edellä mainittu olisi IoV:n toteuttamisen onnistumisen kannalta erittäin hyvä asia, jotta verkot toimisivat katkeamattomasti ja muutenkin, liikkuvien autojen suhteen ajatellen, kaikin puolin tarpeen vaatimalla tavalla.

Lisäksi 5G:n avulla pystyttäisiin potentiaalisesti mahdollistamaan paljon myös IoV:iin kytkeytyviä erilaisia palveluita. Tällaisia voivat olla esimerkiksi erilaiset liikkuvuuden palvelut, kuten autonomisen ajamisen palvelut, erilaiset reittisuunnittelupalvelut, älykkään liikenteen palvelut ja erilaiset ajon aikaiseen viihtymiseen liittyvät palvelut. Tutkitun perusteella myös selvisi, että juuri nimenomaan 5G tekee periaatteessa mahdolliseksi V2X -viestintätyypin luomisen. Se tekisi mahdolliseksi myös muut IoV:n viestintätyypit, jotka aiemmin tässä työssä jo tulivatkin esille. 5G potentiaalisesti kaiken kaikkiaan mahdollistaisi älykkäiden kaupunkien integroitumisen ITS:n kanssa.

Tutkitun perusteella löytyi myös seuraavia 5G:n tarjoamia keinoja vastata IoV:n eri haasteisiin. Yhdeksi keinoksi, jolla pystyttäisiin ratkaisemaan ehkä sekä 5G:n integroimista IoV:n kanssa että tiedonsiirtoa, samanaikaisten yhteyksien toimivuutta ja energiatehokkuutta, olisi kenties seuraava. Selvisi, että ratkaisuna voisi olla se, että tiedonsiirto tehtäisiin ilman tiedon välittämistä verkkoinfrastruktuurin kautta ollenkaan. Tiedonsiirto tehtäisiin tällöin siis vain läheisten laitteiden välillä. Tällainen on toiselta nimeltään Device-to-Device eli D2D -teknologia. Seurauksena voisi olla luultavasti sekä käyttäjien käyttökokemuksen parantuminen IoV:ssa että IoV:n tehokkuuden kasvu esimerkiksi signaalien ja taajuuksien tapauksessa. Mainittiin, että erityisesti V2V-viestinnän tapauksessa D2D voisi olla erityisen hyödyllinen. Apuna voitaisiin luultavasti käyttää infrastruktuureita, joilla pystyttäisiin ehkä saavuttamaan 5G:ssä mahdollisesti toimivat V2V-yhteydet.

Siihen haasteeseen, että 5G:tä ei välttämättä saada ulotettua kaikille syrjäisimmille seuduille asti, ratkaisuksi ehdotettiin puolestaan ad-hoc -verkkojen käyttöä kyseisenlaisilla alueilla. Yhdeksi ratkaisuideaksi IoV-verkkojen katkeamattomuuteen ehdotettiin puolestaan tekniikkaa nimeltään Massive Multiple-Input Multiple-Output (MIMO). Näin suurten antenniryhmien käyttämisen kautta pystyttäisiin luomaan sellainen langaton verkko, jolla pystyttäisiin lähettämään ja vastaanottamaan vielä entistä enemmin tietoa. Yhdeksi keinoksi tiedonsiirtonopeuden, datakapasiteetin ja IoV-verkkojen toimivuuden parantamiseen ylipäätään mainit-

tiin kannettavat miniatyyriset tukiasemat eli toisin sanoen pienet solut. Ne vaatisivat hyvin vähän virtaa toimiakseen ja niiden siirrettävyys olisi myös hyvä. Tämä saattaisi olla yksi keino myös IoV:n liikkuvuuden ja tiheyden haasteisiin. Huonona puolena näissäkin on kuitenkin se, että niitä olisi asennettava suuri määrä eri paikkoihin. Lisäksi huono puoli on siinä, että 5G vaatii entistä suuremman soluinfrastruktuurin, jonka luominen tulisi hyvin kalliiksi.

Mainittiin myös, että 5G:n avulla olisi potentiaalisesti mahdollista luoda jonkinasteisia älykkäitä sovellutuksia, kuten älykkäitä dynaamisesti toimivia liikennevaloja, ja älykästä navigointia. Näillä sitten puolestaan saatettaisiin saada liikenneruuhkia ja sitä kautta myös ympäristön saasteita kuriin, kun liikenne ja parkkeeraaminen tulisi tehokkaammaksi. Mainittiin myös, että 5G-verkkoon on rakennettu reunalaskentakehyksen perusviestintä. Täten myös reunalaskennan suhteen 5G voisi olla jonkin asteinen mahdollistaja tulevaisuudessa ja ne voisi kenties jollain tavalla yhdistää keskenään. Tällöin esimerkiksi saattaisi mahdollistua käytettäväksi laaja valikoima erilaisia tekniikoita samanaikaisesti. Tällaisen yhdistelmän suhteen mainittiin lisäksi, että sen kautta luultavasti mahdollistuisi myös ajoneuvojen nopea sekä liittyminen että poistuminen IoV:n verkoista. Näin taas puolestaan erilaisia navigointi- tai sijaintitietoja saataisiin liikutettua tarpeen vaatimilla tavoilla ilman esimerkiksi katkoksia tai muita verkon putoamisia.

Mainittiin, että yksi haaste on 5G:n tukiasemien pienessä peittävyydessä. Tätä varten tarvittaisiin valtava määrä reunapalvelimia, joka tulee taas puolestaan kalliiksi. Tähän ratkaisuksi esitettiin tienvarsiin järjestettäviä solmupisteitä, joiden avulla ehkä pystyttäisiin auttamaan ajoneuvojen tehtävien siirtämisessä tukiasemille. Ongelmaksi tässä mainittiin kuitenkin vielä se, että tiedonsiirron pitäisi tapahtua nopeasti myös pitkän matkan päähän. Jos tähän keksittäisiin jokin toimiva ratkaisu, voitaisiin 5G-verkoilla olevien tukiasemien määrä laskea ja kustannukset laskisivat myös samalla.

5G:n myötä ratkaisunavaimia olisi myös seuraavassa. Sen avulla IoV:ssa pystyttäisiin luultavasti tukemaan yhteyksiä ajoneuvojen, RSU:iden, antureiden ja latauspisteiden välillä. 5G:n myötä myös luultavasti itseohjautuvien ajoneuvojen kehitystyö tulisi kasvamaan huomattavasti. Yksi syy tähän on juuri 5G:n myötä huomattavasti vähentyvät viestinnän viiveet. Myös tietoturvan, yksityisyyden ja muutenkin IoV:n luotettavuuden suhteen tullaan mahdollisesti saamaan huomattavaa edistystä 5G:n kautta. Toisaalta sitten kuitenkin 5G:n myötä lisään-

tyvien mahdollisuuksien ja ominaisuuksien myötä erilaiset tietoturvauhat ja tietoturvaongelmat saattaisivat myös puolestaan sen sijaan vain lisääntyä ja erilaisia uusia uhkia saattaisi ilmaantua. Haasteita on siis edelleen aivan liikaa vielä tietoturvan ja yksityisyydenkin suhteen. Selvisi, että vaikka 5G sinänsä tarjoaisikin periaatteessa erittäin potentiaalisia ratkaisuja IoV:n keskeisimpien haasteiden, kuten latenssin, kaistanleveyden ja tiedonsiirtonopeuden suhteen, haasteita tutkitun perusteella löytyy silti vielä edelleen paljon.

Tutkitun perusteella ensinnäkin yksi iso haaste 5G:n tapauksessa on yhtenäisen arkkitehtuurin puute teknisen yhteen liitettävyyden suhteen. Yksi haaste on myös paljon eri puolilla maailmaa vaihtelevat standardit. 5G:n saaminen syrjäseuduille ja siitä aiheutuvat suuret kustannukset luovat myös omat haasteensa. Lisäksi tulisi käytännössä luoda täysin uusi iso toimiva infrastruktuuri, joka tulisi olemaan sekä erittäin haastava että kallis prosessi. Myös edelleen käytössä olevat vanhemmat teknologiat, kuten 4G, luovat omat haasteensa ja saattavat ikään kuin hidastaa 5G:hen liittyvää kehitystä. Erilaisia ongelmia on vielä muun muassa laajakaistojen suuntaominaisuuksien, huonojen antennipeittojen ja muiden mahdollisten tiedonkulkua heikentävien tekijöiden suhteen. Yksi haaste 5G:n suhteen IoV:ssa on ajoneuvojen suuresti vaihteleva liikkuvuus, joka luo erilaisia tietoturvauhkia. Lisäksi tämän myötä myös resurssien järkevä kohdentaminen ja IoV-verkkojen hallinta muutenkin hankaloituu. IoV:ssa ajoneuvot olisivat muutenkin kaiken aikaa yhdistettynä. Täten, kasvavan tiedonsiirron suhteenkin, haaste tulee olemaan lisäksi siinä, että miten tiedot pystytään jakamaan tavalla, joka hyödyttää eniten kaikkia. Kuten edelläkin jo sivuttiin, 5G:n tukiasemien peittävyys on pientä. Sen takia jouduttaisiin pystyttämään paljon reunapalvelimia ja siitä sitten aiheutuisi jälleen suuria kustannuksia. Haasteita on myös edelleen big datan ja massiivisen datan hallinnan suhteen, jotka tulisi käsiteltäväksi IoV:n toteutuksen myötä. Haasteita 5G:n ja IoV:n suhteessa on siis edelleen myös kaistanleveyteen, reaaliaikaisuuteen, tiedonsiirtonopeuteen, latenssiin ja muutenkin IoV:n luotettavuuteen liittyen. Ajoneuvojen suhteen on myös vielä liian rajalliset laskennan ja tallentamisen resurssit, että 5G:tä pystyttäisiin niissä olevien palveluiden, kuten esimerkiksi viihdepalveluiden, suhteen vielä kunnolla hyödyntämään. Lisäksi, jos lähes kaikkea IoV:n myötä kasvavaa datamäärä tultaisiin tulevaisuudessa siirtämään ainoastaan 5G:n kautta, voi olla että tulevaisuudessa 5G:nkään resurssit eivät enää tulisi riittämään.

Lähteistä kerätyn perusteella voisi todeta 5G:n olevan erittäin potentiaalinen, lohkoketjun rinnalla yksi parhaimmista, mahdollistaja IoV-teknologialle kaikin puolin. Näyttäisi siltä, että lähes kaikkiin IoV:n keskeisiin haasteisiin, kuten liian suuren latenssiin, massiivisen datamäärän käsittelyyn, riittämättömään tiedonsiirtonopeuteen ja liian pieneen kaistanleveyteen, pystyttäisiin ainakin jollain tavalla vastaamaan 5G:n tarjoamien erilaisten ratkaisujen kautta. 5G:n avulla myös erittäin todennäköisesti IoV ja sen verkot toimisivat paljon tehokkaammin. 5G:n integroitumiseen IoV:n kanssa liittyy kuitenkin edelleen ongelmia siinä määrin, että ei ole vielä tarpeellista valmiutta tällaiseen integroitumiseen käytännön tasolla.

5.2.3 Ratkaisuideoita etäajoon liittyen

Selvisi, että etäajo tulisi luottamaan tulevaisuudessa todennäköisesti täysin 5G-teknologiaan ja sen mahdollistamiin ominaisuuksiin. Eli ominaisuuksiin, kuten alhainen latenssi ja suurempi kaistanleveys. 5G:n kautta mahdollistettavassa etäajossa autonomisten autojen erilaiset tunnistus-, ohjaus- ja päätöksentekotoimet siirrettäisiin pilvipalveluun. Etäajo pitäisi kuitenkin ensin saada niin täysin varmalle tasolle, että se voitaisiin konkreettisesti toteuttaa. Hyödyksi etäajosta mainitaan esimerkiksi se, että pystyttäisiin mahdollistamaan erittäin tarkka ajoneuvojen ohjattavuus, mikä sitten taas olisi luultavasti myös edelleen turvallisuutta lisäävä tekijä.

Etäajon konkreettiseen toteuttamiseen esitettiin myös erilaisia ideoita. Yhdeksi taktiikaksi mainittiin kameroiden asentaminen eripuolille ajoneuvoa, jotka sitten informoisivat tarpeen vaatimalla tavalla ajoneuvoa ympäröivistä tapahtumista. Näiden kameroiden kuvaamat videot välitettäisiin kuljettajan puolelle reaaliaikaisesti 5G:n välityksellä. Näin synkronointikin saataisiin samalla varmistettua. Yhdeksi ratkaisuksi etäajon kannalta mainittiin myös platooning -ratkaisu. Siinä autonomiset ajoneuvot ryhmittyisivät tietyllä tavalla keskenään ja kulkisivat yhtenäisenä järjestäytyneenä joukkona. Tässä joukossa sitten vaihdettaisiin tietoa ja tehtäisiin päätöksiä aina sitä mukaan, kun ryhmään joko liittyy tai siitä poistuu ajoneuvoja. Tämäkin olisi siis yksi potentiaalinen tapa tehostaa myös esimerkiksi liikennettä.

Näyttäisi siltä, että etäajoon olisi jo nyt hyviä ideoita olemassa. Vaikuttaisi myös, että etäajoa saataisiin periaatteessa aika pitkälle kenties toteutettua jo nyt. Kuitenkin on kyse asiasta,

jonka suhteen kaikki pitäisi toimia lähes täydellisesti. Näyttäisikin siltä, että tähän ei tulla pääsemään vielä luultavasti vähään aikaan, sillä etäajoa ei saada vielä toteutettua tarpeeksi turvallisesti ja luotettavasti.

5.2.4 Ratkaisuideoita liittyen saatavuuteen, tietojen eheyteen, luottamuksellisuuteen ja todennukseen

Lähdeaineiston perusteella tuli selväksi, että muun muassa ominaisuudet, kuten saatavuus, tietojen eheys, luottamuksellisuus ja todennus ovat tärkeitä IoV:n ja sen toimivuuden kannalta. Saatavuus on IoV:n kannalta tärkeä ominaisuus ennen kaikkea siksi, että kyseessä on liikkuvat objektit eli ajoneuvot. Tarvittavat tie- ja liikennetiedot täytyisi päivittyä kaiken aikaa riittävällä tavalla tai muuten ajoneuvojen tapauksessa seuraukset voivat olla pahoja esimerkiksi liikenneonnettomuuksien muodossa. Lisäksi, jos saatavuus on heikkoa tai sitä ei ole ollenkaan, voi pahimmassa tapauksessa koko IoV-ympäristö pysähtyä, jos esimerkiksi tietoturvahyökkäykset pääsevät aiheuttamaan haittaa. Saatavuuden suhteen selvisi, että yleisimpiä siihen kohdistuvia tietoturvahyökkäyksen muotoja ovat erilaiset häiriöt, DDoS ja Dos. Ratkaisuiksi saatavuuteen kohdistuvia tietoturvahyökkäyksiä vastaan ehdotettiin muun muassa seuraavia. Mainittiin, että yksi tapa voisi olla jonkinlainen paketintunnistusjärjestelmä, jossa paketti saapuisi kahteen tunnistusjärjestelmään, joissa ensin paketintunnistusmoduulilla tarkistettaisiin signaalin havaitseminen aika-alueella. Toiset monitorit sitten puolestaan taas tarkkailisivat mahdollisia impulssihäiriöitä. DoS-hyökkäysten suhteen taas ehdotettiin, että yksi mahdollinen keino voisi olla DoS-hyökkäysten havaitseminen V2V-viestinnässä tiedonlouhintaan perustuvan lähestymistavan kautta. Ehdotettiin myös, että keinona DoS-hyökkäysten ennaltaehkäisemisessä voisi olla myös jonkinlainen pakettien havaitsemisalgoritmi, joka havaitsisi haitalliset solmut.

Luottamuksellisuus on myös tärkeä ominaisuus IoV:ssa. Ajoneuvojen ja niiden käyttäjien tietojen suhteen tulisi saada varmistettua se, että kyseiset tiedot eivät päädy vääriin käsiin ja että tietyt tiedot pysyvät aina salaisina. Esimerkiksi tiettyjä tietoja, kuten ajoneuvon sijainteja, ajoreittejä ja muita vastaavia tietoja, tulisi suojella siten, että niihin ei pääse käsiksi muut kuin asianomaiset. Yhdeksi luottamuksellisuuteen kohdistuvaksi yleisimmäksi tietoturvahyökkäykseksi mainittiin salakuuntelu. Salakuuntelun torjuntaan ehdotettiin esimer-

kiksi sellaista tapaa, että tietoliikenteessä luotaisiin valepaketteja, joilla hyökkääjiä pyrittäisiin johtamaan harhaan. Toinen ehdotettu taktiikka oli pyöritettyyn häirintään (engl. rotated-jamming-based) perustuva salakuuntelujärjestelmä, jonka avulla pystyttäisiin sieppaamaan tietoja. Näin epäilyttäviä linkkejä pystyttäisiin sitten edelleen häiritsemään. Yksi tekniikka oli myös eräänlainen tien kunnon valvontajärjestelmä, jossa tieolosuhteita tarkkailtaisiin pilvipalvelimen kautta reaaliaikaisesti. Kyseisellä tekniikalla luultavasti pystyttäisiin torjumaan erilaisia yhteistoimintahyökkäyksiä ja RSU:iden kautta tapahtuvia hyökkäyksiä. Näin erilaisten arkaluontoisten tietojen paljastuminen hyökkääjille pystyttäisiin todennäköisesti estämään.

Tärkeäksi ominaisuudeksi IoV:n kannalta osoittautui myös tietojen eheys eli se, että IoV:ssa jaettavia ja jaettuja tietoja ei ole muokattu luvattomasti ja vastaanotetut tiedot ovat samoja, kuin mitä ne olivat vielä lähettämisvaiheessa. Tietoturvahyökkäys nimeltään Man-in-the-middle havaittiin yleiseksi uhaksi eheyden tapauksessa. Tämän torjuntaan ehdotettiin keinoja, kuten luottamusmallia ja pseudo-identiteettiin pohjautuvaa järjestelmää. Tällainen luottamusmalli esimerkiksi kykenisi tunnistamaan hyökkäyksiä aloittamassa olevia haitallisia solmuja. Näihin liittyviä tunnistetietoja pystyttäisiin sitten jälkeenpäin tarpeen vaatiessa perumaan. Jälkimmäisen keinon tapauksessa taas käytettäisiin, liityttäessä RSU:iden kanssa, pseudonyymiä oikean todellisen identiteetin sijasta. Näin saataisiin luultavasti paljastettua haitallisten ongelmia aiheuttavien ajoneuvojen todellinen henkilöllisyys.

Myös todennuksen havaittiin olevan olennainen ominaisuus IoV:n tietoturvan kannalta. IoV ympäristössä olevat järjestelmät, käyttäjät ja niiden henkilöllisyys tulisi jollain lailla varmistaa, ettei ongelmia pääsisi aiheutumaan. Sybil-hyökkäys mainittiin olennaiseksi tietoturvahyökkäykseksi todennuksen kannalta. Ratkaisuksi todennukseen liittyvien tietoturvaongelmien kannalta mainittiin esimerkiksi jonkinlainen hajautettu kevyt todennusjärjestelmä muun muassa V2V -viestinnän tapauksessa. Lisäksi mainittiin mekanismi, jossa käytettäisiin sellaista reititystä, joka perustuisi anonyymiin sijaintiin. Huomioon otettaisiin aikaisempi vyöhykkeen yli tapahtunut viestien vaihto. Viestien saapumiskulmaan perustuen vyöhykkeet sitten luokiteltaisiin esimerkiksi turvallisiin ja vaarallisiin.

Näistäkin ominaisuuksista havaitun perusteella voi todeta seuraavaa. Mainituista ominaisuuksista jokainen on tärkeä IoV:n toimivuuden kannalta. Näyttäisi siltä, että jokainen näis-

täkin ominaisuuksista tulisi saada ensin todella toimivalle tasolle IoV:n kannalta. Esimerkiksi näihin kytkeytyvät tietoturvauhkat pitäisi saada torjuttua niin varmasti ja tehokkaasti, että ainakin lähtökohta olisi se, että kaikki nämä ominaisuudet pystyttäisiin takaamaan IoV:ssa tarpeellisella tehokkuudella ja turvallisuudella. Lisäksi jälleen kerran on havaittavissa seuraavan kaltainen seikka. Vaikka näidenkin ominaisuuksien tietoturvan takaamisen suhteen jonkinasteisia ratkaisuideoita pystytään jo esittämään, ovat ne kuitenkin vielä liian hajanaisia ideoita vain.

5.2.5 Reunalaskenta ja VEC

Tutkitun aineiston perusteella myös reunalaskenta voisi tarjota ratkaisuja IoV:n suhteen. Poimitusta tiedosta kävi ilmi, että mobiilireunalaskenta eli MEC voisi toimia varteenotettavana mahdollistavana tekniikkana massiivisesti kasvavan datamäärän käsittelemisen tapauksessa. Reunalaskennan kautta pystyttäisiin mahdollisesti auttamaan massiivisen datan määrän suhteen siten, että tallennusta, laskentaa ja niiden kapasiteettia pystyttäisiin siirtämään välimuistiin ajoneuvojen läheisyyteen. Eli tallennusta ja laskentaa kyettäisiin siirtämään etäpilvestä verkkojen reunaan, jossa ne olisivat lähellä ajoneuvojen käyttäjiä. Tämä kenties sitten taas puolestaan mahdollistaa IoV:n kannalta tarpeeksi alhaisen latenssin. Lisäksi kaistanleveyden kulutustakin saataisiin luultavasti pienennettyä. Reunalaskenta olisi siis mahdollisesti yksi ratkaisu toimitusviiveiden minimoimiseen IoV:ssa. Selvisi myös, että MEC:n integroimisesta perinteisten ajoneuvoverkkojen kanssa on syntynyt kokonaan uusi käsite nimeltään VEC (engl. Vehicular Edge Computing). VEC:n kautta pyritään löytämään ratkaisuja viestintä-, laskenta- ja välimuistiresurssien siirtämisessä ajoneuvojen käyttäjien läheisyyteen. Edelleen VEC sitten voisi olla yksi potentiaalinen ratkaisu IoV:n kannalta. Tämä siksi, että sen avulla luultavasti saataisiin mahdollistettua suurempi kaistanleveys ja alhaisempi latenssi. Selvisi, että VEC:n kautta tämä pystyttäisiin mahdollistamaan esimerkiksi siten, että RSU:ita käytettäisiin reunapalvelimina. Niille ajoneuvot pystyisivät tarvittaessa siirtämään eniten laskentaa vaativat ja viiveherkimmät tehtävät suoritettavaksi. Lisäksi sisällön pyytäjät pystyisivät mahdollisesti hankkimaan tarvitsemansa tiedot ja sisällöt välisolmuista täysin ilman ydinverkkoon pääsyä. VEC:n avulla pystyttäisiin siis mahdollisesti rajoittamaan vasteaikoja ajoneuvojen läheisyyteen perustettavien reunapalvelimien kautta. Tietojen siirtämisen suoritusai-

koja saataisiin mahdollisesti lyhennettyä paljonkin, mikä olisi erittäin hyvä asia erityisesti IoV:n viiveherkkien sovellusten kannalta.

IoV:n myötä myös energiankulutus lisääntyisi räjähdysmäisesti. Kun VEC:n avulla sitten mahdollisesti voitaisiin siirtää pilvipalvelun resursseja verkon reunalle, kuten jo tuli ilmi, pystyttäisiin kaistanleveysrasitteita mahdollisesti vähentämään ja tätä kautta vaikuttamaan positiivisesti myös sitten edelleen tähän energiankulutuksen haasteeseen. VEC:n avulla saataisiin myös ehkä parannettua tietojen varastointia IoV:ssa, kun reunapalvelimien kautta tietoja saataisiin tallennettua lähelle ajoneuvoja ja niiden käyttäjiä. Käyttäjät mahdollisesti pääsisivät hyvissä ajoin käsiksi tietoihin ja lisäksi myös etäpilvellä olevaa kuormaa pystyttäisiin täten lieventämään. Lisäksi lähipalveluiden tarjoaminen mahdollisesti helpottuisi ja parantuisi tämän juuri edellä mainitun seurauksena. Näin myös käyttökokemukset edelleen luultavasti parantuisivat.

VEC:n avulla saataisiin myös luultavasti ehkä jollain tasolla toteutettua ajoneuvoihin liittyvän luotettavan reaaliaikaisen tiedon mahdollistaminen. Tämä mahdollistaisi sitten potentiaalisesti edelleen taas paljon asioita erilaisten IoV:ssa tarjottavien palveluiden toimivuuden ja liikenneturvallisuuden parantamisen suhteessa. Viihdepalveluiden tarjoamistakin pystyttäisiin IoV:ssa ehkä parantamaan VEC:n tarjoamien hyvien tallentamiseen ja laskemiseen liittyvien resurssien myötä. VEC:n myötä yksi mahdollistava tekijä on myös se, että tällöin tietoja pystyttäisiin tallentamaan välimuistiin ajoneuvojen ja reunapalvelimien kesken toteutetun yhteistyön kautta. Tämä sitten mahdollistaisi kenties sen, että joissain tapauksissa ei välttämättä tarvita edes etäpilvipalvelua ja näin jälleen pystyttäisiin positiivisesti vaikuttamaan esimerkiksi latenssiin.

Mainittiin myös, että VEC:n avulla pystyttäisiin tulevaisuudessa kenties mahdollistamaan erilaisten teknologioiden käyttö. Sen avulla esimerkiksi teknologiat, kuten tekoäly ja lohkoketju saataisiin mahdollisesti yhdistettyä keskenään. Lisäksi VEC:n kautta pystyttäisiin potentiaalisesti mahdollistamaan teknologioita, kuten NFV, SDN ja pilviteknologia. VEC:n kautta pilviteknologiankin toiminnallisuus saataisiin mahdollisesti tuotua verkon reunalle asti. Pilviteknologian kautta pystyttäisiin sitten edelleen todennäköisesti mahdollistamaan tehokas tietojen tallentaminen ja kyettäisiin tarjoamaan tehokas kapasiteetti laskennalle. SDN:n avulla puolestaan pystyttäisiin mahdollisesti irrottamaan verkkotoiminnot sellaisista fyysi-

sistä laitteista, joissa verkkotoiminnot toimivat. Tämän seurauksena sitten edelleen pystyttäisiin, esimerkiksi IoV:nkin tapauksessa, vähentämään erilaisia kustannuksia, kuten pääoma- ja käyttökustannuksia. NFV:n kautta pystyttäisiin taas puolestaan mahdollisesti esimerkiksi tekemään palveluiden käyttöönotosta sekä joustavampaa että tehokkaampaa. NFV:n avulla pystytään siis mahdollistamaan verkkotoimintojen irrottaminen fyysistä laitteista. Myös NFV:n avulla mahdollisesti pystyttäisiin vähentämään erinäisiä kustannuksia.

Älykkäillä ajoneuvoilla on myös omia resursseja käytettävissään. Tämä puolestaan mahdollistaa luultavasti, esimerkiksi IoV:nkin kannalta, sellaisen hyödyllisen seikan, että ajoneuvoilla olevia tehtäviä pystytään tarpeen vaatiessa käsittelemään myös paikallisesti. Täten edelleen pystytään luultavasti vastaamaan IoV:n viiveisiin liittyviin haasteisiin ainakin jollakin tavalla, kun tällaisella paikallisella käsittelyllä voidaan tarvittaessa mahdollisesti säädellä ajoneuvoverkoilla käsiteltävänä olevaa taakkaa. Selvisi myös, että koska VEC:n avulla IoV:ssa pystyttäisiin toteuttamaan ehkä alhaisempi latenssi ja tätä kautta myös parempi luotettavuus, saattaa olla, että VEC:n avulla pystyttäisiin myös toteuttamaan automaattinen ajo. Selvisi myös, että reunalaskentakehyksen perusviestintä on rakennettu 5G:n verkkoon. Tämä sitten puolestaan tarjoaa erilaisia potentiaalisia mahdollisuuksia tekniikoiden ja yhteyksien suhteen, kun reunalaskenta ja 5G mahdollisesti yhdistettäisiin.

Vaikka reunalaskenta mahdollisuuksia IoV:n suhteen tarjoaakin, ongelmia tämänkin tapauksessa vielä löytyy. Yhdeksi ongelmaksi mainittiin esimerkiksi rajoitettu tallennustila, jonka seurauksena välisolmuista ei välttämättä pystytä tallentamaan kaikkea tarvittavaa sisältöä kerralla välimuistiin asti. Ongelmia aiheutuu myös määrittelyn suhteen sekä siitä, mitä välimuistiin pitäisi aina kulloinkin tallentaa että siitä, mihin olemassa olevista välimuisteista pitäisi tallentaa. Lisäksi ihmetystä aiheuttaa vielä esimerkiksi välimuistikäytännön määrittely. Näiden ongelmien suhteen oli esitetty esimerkiksi sellaista ratkaisua, että tekoälyn kautta luotaisiin kognitiivisia kyvykkyyksiä, jotka osaisivat suorittaa asiat kulloisessakin tilanteessa oikein. Yksi iso haaste on myös se, että reunapalvelimien pystyttämisestä aiheutuisi valtavat kustannukset.

Voidaankin havaita, että reunalaskennankin keinoin olisi potentiaalisesti saavutettavissa ratkaisuja IoV:n haasteisiin, kuten latenssiin ja kaistanleveyteen liittyen. Tämä siksi, että reunalaskennan avulla erilaisia toimia ja toimintoja pystyttäisiin mahdollisesti järjestämään tar-

vittaessa lähempänä ajoneuvoja. Näin verkon taakkaa pystyttäisiin säätelemään tarpeen vaatimalla tavalla. Kuitenkin jälleen voi todeta seuraavaa. Vaikka potentiaalisia ideoita löytyy, ongelmia näyttäisi kuitenkin olevan vielä aivan liikaa erityisesti välimuistin tallentamiseen liittyvien käytäntöjen ja aiheutuvien kustannusten suhteen.

5.2.6 Koneoppiminen ja tekoäly

Selvisi lyhyesti myös, että koneoppimisen kautta on kenties tulevaisuudessa mahdollista ratkaista seuraavanlaisia haasteita. Sen avulla saadaan potentiaalisesti kehitettyä jonkinlaista ideaa dynaamisten sekä tieolosuhteiden että ympäristöön liittyvien olosuhteiden haastetekijöihin. Lisäksi koneoppimisen menetelmät saattavat olla mahdollistavia tekijöitä esimerkiksi ajoneuvojen sijainnin tuntemuksen haasteissa.

Liikenteessä tapahtuu luontaisesti erilaisia tilanteita. IoV:n suhteen tullaankin siis tarvitsemaan älykästä päätöksentekoa, joka sitten puolestaan, tutkitun perusteella, tulee potentiaalisesti olemaan mahdollista esimerkiksi juuri tekoälyn kautta. Eli autonomisen ajon kontrolloinnin, kuten nopeuden ja jarrutuksen suhteen, tekoälyllä tullaan mahdollisesti saamaan aikaiseksi ratkaisuja tulevaisuudessa. Näin ollen tekoäly tulee mahdollisesti olemaan tehokas tekijä liikenneonnettomuuksien tehokkaassa välttämisessä.

5.2.7 Luotettavuus, liikkuvuus, standardit ja rajoitettu verkon peittoalue

Tutkitun perusteella on selvinnyt, että luotettavuus on IoV:n kannalta tärkeä ominaisuus, kuten on jo edeltäkin käynyt ilmi. Luotettavuuden osalta tulisi saada varmistetuksi se, että verkkolaitteet toimisivat ilman pätkimisiä. Uutena asiana vielä, luotettavuuden suhteen, tuli jälkeenpäin ajatuksia seuraavaan liittyen. IoV:n kannalta olisi löydettävä ratkaisu myös sellaisten tapausten varalle, joissa pätkimisiä pääsee väistämättä tapahtumaan. IoV:n tulisi siis kyetä säilyttämään toimintansa riittävällä tavalla myös tällaisissa tapauksissa. Tähän ehdotettiin esimerkiksi, että toimiva lähestymistapa voisi olla seuraava. Lähestymistapana voisi olla se, että joka kerta kehitystyössä pidetään mielessä ajatus siitä, että turvallisuus on taattava aina ennen viihdettä. Näin saataisiin sitten luultavasti aikaan mahdollisimman turvallisia ja luotettavia ratkaisuja.

IoV:n keskeinen haastetekijä on myös ajoneuvoista aiheutuva suuri liikkuvuus. Liikkuvuudella tarkoitetaan IoV:n kannalta sitä, että haasteellista on pitää solmut kytkettyinä jatkuvasti jokaisena hetkenä, joka aiheutuu ajoneuvojen suuresta liikkuvuudesta. Reaaliaikaisuuden toteuttaminen eri IoV:n toiminnoissa on haastavaa suuresta liikkuvuudesta johtuen. Sitten taas toisaalta reaaliaikaisuus on välttämätön vaatimus IoV:n toiminnan kannalta, jotta ei pääse aiheutumaan liikenteessä mitään vakavia seurauksia johtuen juuri nimenomaan reaaliaikaisuuden puutteesta. Mitään sen suurempaa ratkaisua tähän ei tässä kohdin löytynyt, mutta esitettiin seuraavaa. Mainittiin, että liikkuvuuteen tulisi saada jotenkin kehitettyä ratkaisu, jolla pystyttäisiin varmistamaan hyvä verkon vakaus IoV:n pysähtymättömille korkean liikkuvuuden alla oleville verkkoyhteyksille tarpeen vaatiman tason mukaisesti.

Selvisi, että ongelma IoV:n kehitykselle ovat myös eri puolilla maailmaa suurestikin vaihtelevat standardit. Erilaiset standardit hankaloittavat IoV:n toteuttamista, kun kaikki erilaiset standardit tulisi huomioida. Yhdeksi ratkaisuksi tähän esitettiin, että voitaisiin ottaa käyttöön yksi yhteinen kansainvälinen standardi IoV:n tapauksessa. Lisäksi mainittiin, että esimerkiksi eri hallitukset voisivat kannustaa ja rohkaista eri teollisuuden aloja tekemään yhteistyötä teknologian kehitystyössä. Näin potentiaalisesti sekä teknologian kehitys saattaisi nopeutua että standardit yksinkertaistua. Yhdeksi ongelmaksi IoV:n kannalta selvisi myös verkon rajoitettu peittoalue. Ajoneuvot jakavat omia resurssejaan ajoneuvojen pilven kautta ja käyttävät yleensä matkapuhelinverkkoa tai kiinteitä infrastruktuureja. Ongelman tässä suhteessa kerrottiin aiheutuvan siitä, että ajoneuvot eivät pysty kommunikoimaan siinä kohtaa, kun joku osapuolista jää verkon kantaman ulottumattomiin. Ratkaisuksi tähän ehdotettiin sitä, että käytettäisiin palveluntarjoajina mobiilivälittäjiä, jotka aina tallentaisivat muistiin aikaisempien ajoneuvopyyntöjen sisältämät tiedot. Esimerkkinä mainittiin, että jotain tiettyä reittiä jatkuvasti kulkeva linja-auto voisi toimia kyseisenlaisena välittäjänä.

Näitä samoja asioita tulikin jo esille aieminkin eri asiayhteyksien yhteydessä. Jälleen nähdään, että kaikenlaisia ideoita löytyy. Kuitenkaan mitään sen yhtenäisempää toimivaa linjaa asioiden suhteen ei ole vielä saatu kehitettyä, jota sitten lähdettäisiin entistä paremmin jatkojalostamaan.

5.2.8 Big data

IoV:ssa verkkoon yhdistetyt autonomiset ajoneuvot loisivat erittäin suuren määrän dataa käsiteltäväksi. Lisäksi kulutuksen kohteena tulisi olemaan luultavasti myös valtava määrä nimenomaan erityyppistä dataa. Tämän seurauksena myös big data tulee haasteeksi IoV:n kannalta. Yhdeksi potentiaaliseksi ratkaisuksi big datan käsittelemisen kannalta mainittiin mobiilipilvilaskenta. Toiseksi keinoksi mainittiin ajoneuvojen toimiminen verkotettuina laskentakeskuksina IoV:ssa, jolloin ne keskinäisen yhteistyön kautta toteuttaisivat tietojenkäsittelyä ja resurssien jakamista. Jonkinlainen ajoneuvojen ryhmittely voisi mahdollisesti toimia ratkaisuna. Samassa yhteydessä mainittiin myös, että esimerkiksi sellaisia maalaitoksia, jotka omaavat suuria laskentaresursseja, voitaisiin käyttää hyödyksi myös big datan käsittelemisessä IoV:n kautta.

Selvisi myös, että tiedon louhinnan keinoin on ehkä mahdollista määrittää tarkka IoV-viestintämalli esimerkiksi tiedon saapumisen, kanavan ominaisuuksien ja kapasiteetin arvioimista varten. Selvisi myös, että tiedonsiirron avulla pystyttäisiin potentiaalisesti laskemaan sekä paketeilla oleva toimitussuhde että niiden tila. Yksi seurauksena saatavista hyödyistä saattaisi olla myös esimerkiksi se, että tuleva datakuormitus pystyttäisiin mahdollisesti ennustamaan big datan ja sen tehtävien saapumisaikojen tallennuksen kautta. Näin varattavia resurssejakin, kuten kaistanleveyttä, pystyttäisiin mahdollisesti suunnittelemaan jo ennalta. Yhdeksi ratkaisuksi mainittiin myös kanavadatan eli esimerkiksi signaalin voimakkuuden hyödyntäminen kanavaparametrien, kuten polkuhäviön, arvioimisessa. Edelleen kyseisenlaisia kanavatietoja pystyttäisiin kenties hyödyntämään myös tarkkojen IoV-olosuhteiden toistamisessa liittyen esimerkiksi ajoneuvojen liikkuvuuteen.

Lisäksi selvisi, että big dataa voitaisiin mahdollisesti käyttää hyödyksi IoV:n kannalta myös esimerkiksi seuraavin tavoin. Muun muassa big datan päätelmiä IoV:n ominaisuuksiin ja olosuhteisiin liittyen pystyttäisiin mahdollisesti hyödyntämään tehokkaiden dataohjattujen viestintäprotokollien suunnittelussa. Edelleen big dataa voidaan käyttää luultavasti hyödyksi liikenteen kuormituksen ja kanavien kapasiteettien ennustamisessa ja mahdollisesti myös IoV:n suorituskyvyn parantamisessa havaittujen IoV-tilatietueiden hyödyntämisen kautta. Myös big datan kautta saatavia erilaisia kontekstitietoja pystyttäisiin mahdollisesti hyödyntämään ajoneuvojen liikkuvuudesta aiheutuvien kanavien muutosten ennustamisessa. Lisäksi

edellä mainitun kautta mahdollisesti pystytään myös arvioimaan varattavaa kaistanleveyttä paremmin IoV:ssa.

Haasteita big dataan IoV:n suhteessa ilmeni kuitenkin edelleen seuraavanlaisia. On vielä liikaa riskejä tietoturvallisuuteen liittyen. Lisäksi tiedonkeruu on vielä liian epäjohdonmukaista. Riskinä on, että esimerkiksi tietomurron seurauksena arvokkaita tietoja vuotaisi asiakkaiden tai kilpailevien toimijoiden tietoon. Tiedonkeruun tulisi lisäksi olla reaaliaikaista ja jatkuvaa, jotta se saataisiin mahdollisesti tarvittavalle tasolle. Tämä sitten taas puolestaan edellyttäisi isoja strategisia toimia, joista sitten taas aiheutuisi isoja kustannuksia. Lisäksi isojen tietojoukkojen keräämisessä käytettävät työkalut tulisi olla tarpeeksi tarkkoja ja näiden suhteen ei ole vielä tarvittavaa varmuutta. Riski on myös ulkoistettujen tietojen yksityisyys, eheys, saatavuus ja luottamuksellisuus. Haasteita voi aiheutua myös esimerkiksi ongelmista langattomien yhteyksien ja taajuusresurssipulan suhteen. Jälleen haasteita aiheutuu myös esimerkiksi ajoneuvojen suuresta liikkuvuudesta. IoV:n kattavuutta tulisi myös saada parannettua, sillä big dataa tulisi monesta eri lähteestä. Ongelmana IoV:n ja big datan suhteen on myös se, että kuinka saataisiin valittua aina juuri oikeat ajoneuvot oikeassa ajassa ja paikassa, jotta pystyttäisiin ylläpitämään myös pitkän aikavälin verkonhallintaa.

Jälleen myös big datan suhteen voi todeta sen, että ratkaisuja ja arvioituja hyötyjä IoV:n suhteen näyttäisi olevan monia. Esimerkiksi datakuormitusta ja erilaisia IoV-olosuhteitakin, kuten sen kapasiteetteja ja myös liikenneolosuhteita, pystyttäisiin mahdollisesti arvioimaan jo ennalta, jos ratkaisut saataisiin toteutettua. Tästä olisi sitten taas mahdollisesti edelleen monia eri hyötyjä. Potentiaalisesti hyötynä olisi ehkä jopa koko IoV:n suorituskyvyn parantuminen. Jälleen kerran kuitenkin näyttäisi esiintyvän vielä sen verran ongelmia, joita ei ole täysin kyetty ratkaisemaan, että ratkaisuja ei pystytä vielä tarpeellisella varmuudella viemään toteutukseen asti.

5.2.9 Tietoturvallisuus, turvallisuus ja yksityisyys

IoV:n tietoturvallisuuden kannalta nousi vielä esiin myös seuraavanlaisia pieniä ratkaisuideoita. Ehdotettiin, että ennen kuin IoV:n toteutus voitaisiin täysimääräisesti aloittaa, pitäisi onnistua luomaan tehokas yksityisyys- ja tietoturvajärjestelmä. Lisäksi yhdeksi mahdollisek-

si keinoksi tietoturvaongelmien torjuntaan mainittiin todennus- ja avaintenhallintaprosessin käyttäminen. Kyseistä keinoa voitaisiin käyttää esimerkiksi ajoneuvojen ja RSU:iden välillä yhdessä sumupalvelimien kanssa. Salattu viestintä voisi puolestaan toimia yhtenä keinona. Säännöllistä verkon valvontaa voitaisiin mahdollisesti myös hyödyntää esimerkiksi sumujärjestelmien verkon resurssien tarkkailemiseen. Langattomat suojausprotokolla voisivat sitten taas ehkä toimia sumuympäristöissä toteutettavan tiedonsiirron toteuttamisessa esimerkiksi.

Monenlaista ideaa on, mutta jälleen kerran ratkaisut vaikuttaisivat olevan kuitenkin hajanaisia. Mitään sen suurempaa yhtenäisempää toimivaa linjaa ole löydetty, johon kannattaisi erityisesti panostaa ja kohdistaa jatkokehitystä.

6 Oma analyysi ja yhteenveto

Tutkielman perusteella selvisi, että IoV:n toteuttamista ei ole päästy konkreettisesti käytännön tasolle asti viemään vielä juuri ollenkaan, johtuen sillä vielä olevista monista haasteista ja ongelmista. IoV:n suurimpina ja keskeisimpinä haasteina näyttäisi olevan erilaiset latenssiin, tietoturvallisuuteen, kaistanleveyteen, isojen datamäärien hallintaan, skaalautuvuuteen, standardeihin, autojen suuresti vaihtelevaan liikkuvuuteen ja infrastruktuurin luomisen haastavuuteen ja kalleuteen liittyvät haasteet. Tässä tutkimuksessa havaittiin, että näihin haasteisiin löytyy monia eri ideoita mahdollisiksi ratkaisuiksi ja käytettäviksi tekniikoiksi. Lupaavimpina tekniikoina IoV:n suhteen havaittiin olevan lohkoketju ja 5G. Myös reunalaskenta näyttäisi tarjoavan potentiaalisia mahdollisuuksia IoV:n suhteen. Myös koneoppiminen ja tekoäly vaikuttaisivat tulevaisuuden suhteen lupaavilta tekniikoilta IoV:n toteuttamisen kannalta, erityisesti erilaisten älykästä ja dynaamista päätöksentekoa vaativien sovellusten ja asioiden suhteen.

Kuten edellä jo lähteistä poimittujen tulosten perusteella selvisi, pystyttäisiin lohkoketjun avulla tarjoamaan potentiaalisia ratkaisuja latenssin, isojen datamäärien käsittelyn, reaaliaikaisen tiedonkulun käsittelyn, tiedonkulun käsittelyn, suorituskyvyn, tietoturvan, yksityisyyden, vikasietoisuuden ja tietojen sekä läpinäkyvyyden että eheyden suhteen. 5G:n avulla sitten taas puolestaan saataisiin mahdollisesti toteutettua ensinnäkin V2X-viestintä ja myös paljon uudenlaisia ominaisuuksia sekä IoV:n verkkojen että palveluiden suhteen. IoV:n tavoitteena on myös tarjota mahdollisimman hyvä viihtyminen matkustajille matkan ajaksi. Esimerkiksi juuri erilaiset viihtymisen palvelut saataisiinkin potentiaalisesti mahdollistettua 5G:n kautta. Lisäksi 5G:n avulla saataisiin mahdollisesti luotua liikenteen sujuvuutta parantavia sovellutuksia, joilla saataisiin todennäköisesti tehostettua liikennettä monin eri tavoin. 5G näyttäisi tarjoavan ominaispiirteineen myös potentiaalisia mahdollisuuksia samanaikaisten verkkoyhteyksien ja isojen datamäärien hallintaan kaikkialla jatkuvasti kaiken aikaa. Näin ollen 5G voi olla mahdollinen ratkaisu myös IoV:n suuresti vaihtelevan liikkuvuuden haasteisiin. Lisäksi 5G:n avulla saataisiin IoV:n suhteen parannettua todennäköisesti verkon jatkuvuutta, kaistanleveyttä, latenssia, järjestelmien välistä yhdistettävyyttä ja verkkoyhteyksien tiedonsiirtonopeutta, turvallisuutta ja kantavuutta. Lupaavaksi tekniikaksi

osoittautui myös reunalaskenta, jonka avulla mahdollisesti pystyttäisiin vastaamaan suuren datan määrän hallintaan, latenssiin ja kaistanleveyteen liittyviin haasteisiin IoV:ssa. Tämä tapahtuu siirtämällä kuormaa etäpilveltä verkkojen reunoilla lähemmäs ajoneuvoja käyttäjineen.

Näiden kaikkien edellä mainittujen teknologioiden integroimiseen IoV:n kanssa liittyy kuitenkin edelleen paljon erilaisia haasteita ja ongelmia liittyen tietoturvaan, laskentatehoon, energiankulutukseen, isojen datamäärien hallintaan, tallennustiloihin, tekniseen yhteen liitettävyyteen, standardeihin, infrastruktuurin luomiseen, kustannuksiin, syrjäisimpiin alueisiin, resurssien käyttöön, rajoituksiin, kohdentamiseen ja verkon vakauteen. Tutkimuksen perusteella ilmeni myös, edellä mainittujen tekniikoiden ohella, erilaisia minimaalisempia hajanaisia ratkaisuideoita liittyen tärkeisiin ominaisuuksiin IoV:n toimivuuden kannalta. Tällaisia olivat ominaisuudet liittyen saatavuuteen, luotettavuuteen, tietojen eheyteen, todennukseen, liikkuvuuteen, standardeihin, tietoturvallisuuteen, yksityisyyteen, rajoitettuun verkon peittoalueeseen ja etäajon toteuttamiseen.

Tämän tutkimuksen perusteella IoV:n haasteiden suhteen ratkaisuja näyttäisikin tekniikoiden ja ideoiden puolesta löytyvän jo melko kattavasti. Tutkimuksen perusteella vaikuttaisikin siltä, että tekniikan puolesta IoV:ia olisi mahdollista periaatteessa lähteä jopa toteuttamaan konkreettisesti ihan käytännön tasolle asti monilta osin jo tällä hetkellä. Kuitenkin IoV:n suhteen löytyy vielä aivan liikaa kaikenlaisia aukkoja, haasteita ja ongelmia aina eettisiin ja moraalisiin asioihin asti, jotka kaikki tulisi jollain tavalla huomioida. Monia tekniikoita on, kuten tässä tutkimuksessa erityisesti esimerkiksi lohkoketju, 5G ja reunalaskenta, joilla olisi potentiaalista lähteä sinänsä IoV:n ongelmia ratkaisemaan. Kuitenkin, kuten tuli edellä tutkimuksessa todettua, on näilläkin tekniikoilla jokaisella vielä aivan liikaa omiakin ongelmakohtia, jotka tulisi saada ratkaistua jollain tavalla. Ongelma näyttäisi olevan myös monesti siinä, että IoV:n toteuttamista edistävien ratkaisujen toteuttaminen tulisi monesti todella kalliiksi. Esimerkiksi IoV:n toteutukseen vaadittavan infrastruktuurin luominen vaatisi, kuten edellä jo ilmeni, suuria kustannuksia ja olisi lisäksi erittäin haastavaa toteuttaa.

Kuten edellä tutkimuksessa myös osoittautui, erityisen haastavaa IoV:n toteuttamisesta näyttäisi tekevän myös sen liikkuva vaihteleva luonne, joka aiheutuu autojen suuresti vaihtelevasta liikkumisesta ja määrästä. Tämä sitten aiheuttaa verkkoihin ongelmia, kuten katkoksia

ja pätkimisiä. Lisäksi erityisen haastavan IoV:n toteuttamisesta näyttäisi tekevän myös juuri nimenomaan autot. Kaikki pitäisi saada toimimaan lähes täydellisen varmasti. Minkäänlaisia esimerkiksi suurempia verkkojen katkoksia ei saisi esiintyä tai muuten seuraukset voivat olla tässä tapauksessa todella vakavia esimerkiksi kohtalokkaiden liikenneonnettomuuksien muodossa. Lähes kaikki ongelmakohdat ja haasteet tulisi siis saada ratkaistua ja korjattua niin varmasti, että voidaan olla varmoja siitä, että kaikki toimii siten kuten pitääkin.

Ongelma näyttäisi olevan myös osaltaan seuraavassa. IoV:n suhteen näyttäisi olevan esitetty myös erittäin paljon erilaisia pienempiä ratkaisuideoita sen eri osa-alueisiin liittyen. Tutkimuksen perusteella tuli siis havaittua, että ratkaisuideat ja ratkaisuehdotukset ovat monesti vielä, vaikka niitä paljon erilaisia löytyykin, hyvin hajanaisia. Voidaankin todeta, että olisi hyvä että IoV:n suhteen löytyisi vielä näidenkin tapauksessa yhtenäisempi linja ja ideat alkaisivat vastata yhä enemmän toisiaan. Näin voitaisiin saada kenties enemmän keskitettyä voimavaroja ja ajatuksia aina joihinkin tiettyihin, jo toimivaksi todettuihin, ideoihin ja näin saada kasvatettua niiden toimivuutta ja luotettavuutta. Kuten Sakshi ym. (2021) tekstissään totesi, tulisi ehkä kehittää jonkinlaiset yhtenäiset standardit ja ohjenuorat IoV:n kehitystyölle, jotta se yhtenäistyisi vielä enemmin ja näin ollen edelleen mahdollisesti tehostuisi. Toisaalta hyötynä standardien puuttumisestakin on se, että tulee enemmin monipuolisempia laaja-alaisempia ideoita. Vielä kiteytettynä edellisesti seuraavaa. IoV:n pelikenttä tulisi siis jollain tasolla saada yhtenäisemmäksi kuin mitä se nyt on. Täten kehitystyö lähtisi kulkemaan kenties vielä tehokkaammin. Tällä hetkellä näyttäisi enemmänkin olevan paljon yksittäisiä pienempiä hajanaisia ratkaisuideoita siellä täällä. Ideat vaikuttaisivat olevan vielä liian hajanaisia keskenään ja yhtenäisempää linjaa pitäisi löytää.

Yhteenvetona kaikesta tutkitusta voisikin todeta seuraavaa. Tekniikan puolesta IoV:n toteuttaminen vaikuttaisi olevan nyt jo osittain mahdollista ja paljon erilaisia ideoita ratkaisuiksi näyttäisi löytyvän. Ratkaisuehdotukset ja ratkaisuideatkin ovat vielä kuitenkin liian hajanaisia keskenään eikä tarpeeksi yhtenäistä linjaa näyttäisi vielä löytyvän maksimaalisen kehitystyön mahdollistamiseksi. Myös sekä näillä mahdollistavilla tekniikoilla että myös IoV:lla yleensäkin on vielä aivan liikaa erilaisia haasteita, aukkoja ja ongelmia. Nämä tulisi ensin saada ratkaistua niin perusteellisella, kattavalla ja varmalla tavalla, että IoV:n toteuttaminen voitaisiin toteuttaa täysimääräisesti tarpeeksi luotettavasti, turvallisesti ja toimivasti. Jatko-

tutkimusaiheiden suhteen voisi todeta seuraavaa. Tässä tutkimuksessa koneoppimisen ja tekoälyn tutkiminen, IoV:n ratkaisukeinoina, jäivät vielä verrattain erittäin vähäiseksi. Tämä voisi olla yksi osa-alue, johon voisi syventyä vielä perusteellisemmin. Lisäksi yleisesti voisi keskittyä tutkimaan jatkossa vielä tarkemmin erityisesti, IoV:n kannalta potentiaalisten, tekniikoiden, kuten 5G:n ja lohkoketjun, haasteita. Niiden suhteen voisi sitten myös yrittää mahdollisesti jatkokehittää jonkinlaisia ratkaisuideoita. Yksi vaihtoehto on myös se, että yrittää kehitellä täysin uudenlaisia ideoita ratkaisuiksi IoV:n suhteen. Eli yrittäisi kehitellä kenties jotain jopa vielä toimivampaakin, kuin jo aiemmin esille tulleet teknologiat.

Lähteet

Abbas, Sohail, Abu T. Manar, Afaf Ahmed, Faheem Khan, Shabir Ahmad ja Kim Do-Hyeun. 2021. *Blockchain-Based Authentication in Internet of Vehicles: A Survey* [kielellä English]. 23. Copyright - © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License; Last updated - 2021-12-09. https://www.proquest.com/scholarly-journals/blockchain-based-authentication-internet-vehicles/docview/2608140665/se-2.

Arena, Fabio, Giovanni Pau ja Alessandro Severino. 2020. *An Overview on the Current Status and Future Perspectives of Smart Cars* [kielellä English]. 7. Copyright - © 2020. This work is licensed under http://creativecommons.org/licenses/by/3.0/ (the "License"). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License; Last updated - 2021-02-14. https://www.proquest.com/scholarly-journals/overview-on-current-status-future-perspectives/docview/2419905703/se-2.

Baruah, Barnana, ja Subhasish Dhal. 2020. *A Secure and Privacy-Preserved Road Condition Monitoring System.* https://doi.org/10.1109/COMSNETS48256.2020.9027482.

Darwish, Tasneem S. J., ja Kamalrulnizam Abu Bakar. 2018. *Fog Based Intelligent Transportation Big Data Analytics in The Internet of Vehicles Environment: Motivations, Architecture, Challenges, and Critical Issues.* https://doi.org/10.1109/ACCESS.2018.2815989.

El Madani, Samira, Saad Motahhir ja Abdelaziz El Ghzizal. 2022. "Internet of vehicles: concept, process, security aspects and solutions". *Multimedia Tools and Applications,* 1–25.

Elfatih, Nada M., Mohammad Kamrul Hasan, Zeinab Kamal, Deepa Gupta, Rashid A. Saeed, Elmustafa Sayed Ali ja Md. Sarwar Hosain. 2022. *Internet of vehicle's resource management in 5G networks using AI technologies: Current status and trends.* 5. https://doi.org/https://doi.org/10.1049/cmu2.12315. eprint: https://ietresearch.onlinelibrary.wiley.com/doi/pdf/10.1049/cmu2.12315. https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/cmu2.12315.

Elhadja, Benalia, Bitam Salim ja Mellouk Abdelhamid. 2020. *Data dissemination for Internet of vehicle based on 5G communications: A survey.* 5. https://doi.org/https://doi.org/10.1002/ett.3881. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/ett.3881. https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3881.

Fadhil, Jawaher Abdulwahab, ja Qusay Idrees Sarhan. 2020. *Internet of Vehicles (IoV): A Survey of Challenges and Solutions.* https://doi.org/10.1109/ACIT50332.2020.9300095.

Guerrero-Ibanez, J., J. Contreras-Castillo ja S. Zeadally. 2021. *Deep learning support for intelligent transportation systems.* 3. https://doi.org/https://doi.org/10.1002/ett.4169. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/ett.4169. https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4169.

Guevara, Leonardo, ja Fernando Auat Cheein. 2020. *The Role of 5G Technologies: Challenges in Smart Cities and Intelligent Transportation Systems.* 16. https://doi.org/10.3390/su12166469. https://www.mdpi.com/2071-1050/12/16/6469.

Ji, Baofeng, Xueru Zhang, Shahid Mumtaz, Congzheng Han, Chunguo Li, Hong Wen ja Dan Wang. 2020. *Survey on the Internet of Vehicles: Network Architectures and Applications.* 1. https://doi.org/10.1109/MCOMSTD.001.1900053.

Kaiwartya, O., A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. -. Lin ja X. Liu. 2016. *Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects* [kielellä English]. Cited By :364. www.scopus.com.

Kayarga, Tanuja, ja Anand Kumar. 2021. *A Study on Various Technologies to Solve the Routing Problem in Internet of Vehicles (IoV).* Heinäkuu. https://doi.org/10.1007/s11277-021-08220-w.

Khan, John A., ja MD Minhaz Chowdhury. 2021. *Security Analysis of 5G Network.* https://doi.org/10.1109/EIT51626.2021.9491923.

Laghari, Asif Ali, Kaishan Wu, Rashid Ali Laghari, Mureed Ali ja Abdullah Ayub Khan. 2021. *A review and state of art of Internet of Things (IoT).* Springer.

Li, Tan, Congduan Li, Jingjing Luo ja Linqi Song. 2020. *Wireless recommendations for Internet of vehicles: Recent advances, challenges, and opportunities.* 1. https://doi.org/10.23919/ICN.2020.0005.

Liu, Lei, Qingqi Pei, Sabita Maharjan ja Yan Zhang. 2021. *Vehicular Edge Computing and Networking: A Survey.* Kesäkuu. https://doi.org/10.1007/s11036-020-01624-1.

Mollah, Muhammad Baqer, Jun Zhao, Dusit Niyato, Yong Liang Guan, Chau Yuen, Sumei Sun, Kwok-Yan Lam ja Leong Hai Koh. 2021. *Blockchain for the Internet of Vehicles Towards Intelligent Transportation Systems: A Survey.* 6. https://doi.org/10.1109/JIOT.2020.3028368.

Ning, Zhaolong, Kaiyuan Zhang, Xiaojie Wang, Lei Guo, Xiping Hu, Jun Huang, Bin Hu ja Ricky Y. K. Kwok. 2021. *Intelligent Edge Computing in Internet of Vehicles: A Joint Computation Offloading and Caching Solution.* 4. https://doi.org/10.1109/TITS.2020.2997832.

Osibo, Benjamin K., Chengbo Zhang, Changsen Xia, Guanzhe Zhao ja Zilong Jin. 2021. *Security and Privacy in 5G Internet of Vehicles (IoV) Environment* [kielellä English]. 2. Copyright - © 2021. This work is licensed under https://creativecommons.org/licenses/by/4.0/ (the "License"). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License; Last updated - 2021-12-03. ISBN: 25790099. https://www.proquest.com/scholarly-journals/security-privacy-5g-internet-vehicles-iov/docview/2557141921/se-2.

Qiu, J, Y Chen, X Zhang, Q Liu, W Li, Y Pei ja L Liu. 2019. *Standardization Evolution and Typical Solutions of IoV.* https://doi.org/10.1109/WOCC.2019.8770607.

Queiroz, A., E. Oliveira, M. Barbosa ja K. Dias. 2020. *A Survey on Blockchain and Edge Computing applied to the Internet of Vehicles* [kielellä English]. Cited By :4. www.scopus.com.

Sagiroglu, Seref, ja Duygu Sinanc. 2013. *Big data: A review.* https://doi.org/10.1109/CTS.2013.6567202.

Sakshi, Garg, Mehrotra Deepti, Hari M. Pandey ja Pandey Sujata. 2021. *Accessible review of internet of vehicle models for intelligent transportation and research gaps for potential future directions.* 2. Maaliskuu.

Singh, Sehajbir, ja Singh S. Baljit. 2021. *Autonomous cars: Recent developments, challenges, and possible solutions* [kielellä English]. 1. Copyright - © 2021. This work is published under http://creativecommons.org/licenses/by/3.0/ (the “License”). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License; Last updated - 2021-12-21. Tammikuu. ISBN: 17578981. https://www.proquest.com / scholarly - journals / autonomous - cars - recent - developments - challenges / docview / 2601103874/se-2.

Sleem, L., H. N. Noura ja R. Couturier. 2020. *Towards a secure ITS: Overview, challenges and solutions* [kielellä English]. Cited By :1. www.scopus.com.

Storck, Carlos Renato, ja Fátima Duarte-Figueiredo. 2020. *A Survey of 5G Technology Evolution, Standards, and Infrastructure Associated With Vehicle-to-Everything Communications by Internet of Vehicles.* https://doi.org/10.1109/ACCESS.2020.3004779.

Tripathi, Gautami, Mohd Abdul Ahad ja Mithileysh Sathiyanarayanan. 2019. *The Role of Blockchain in Internet of Vehicles (IoV): Issues, Challenges and Opportunities.* https://doi.org/10.1109/IC3I46837.2019.9055613.

Wu, Lan, Juan Xu, Lei Shi, Yi Shi ja Wenwen Zhou. 2021. *Optimize the Communication Cost of 5G Internet of Vehicles through Coherent Beamforming Technology* [kielellä English]. Copyright - Copyright © 2021 Lan Wu et al. This work is licensed under http://creativecommons.org/licenses/by/4.0/ (the “License”). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License; Last updated - 2021-05-30. ISBN: 1530-8669. https://www.proquest.com/scholarly-journals/optimize-communication-cost-5g-internet-vehicles/docview/2534430690/se-2.

Wu, Xiaotong, Xiaolong Xu ja Muhammad Bilal. 2021. *Towards Privacy Protection Composition Framework on Internet of Vehicles.* https://doi.org/10.1109/MCE.2021.3092303.

Xu, Wenchao, Haibo Zhou, Nan Cheng, Feng Lyu, Weisen Shi, Jiayin Chen ja Xuemin Shen. 2018. *Internet of vehicles in big data era.* 1. https://doi.org/10.1109/JAS.2017.7510736.

Yang, Yang, ja Kun Hua. 2019. *Emerging Technologies for 5G-Enabled Vehicular Networks.* https://doi.org/10.1109/ACCESS.2019.2954466.

Yin, Xiuwen, Jianqi Liu, Xiaochun Cheng ja Xiaoming Xiong. 2021. *Large-Size Data Distribution in IoV Based on 5G/6G Compatible Heterogeneous Network.* https://doi.org/10.1109/TITS.2021.3118701.

Zhou, Haibo, Wenchao Xu, Jiacheng Chen ja Wei Wang. 2020. *Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities.* 2. https://doi.org/10.1109/JPROC.2019.2961937.