Tampereen yliopisto

Sanna Rikkonen

AJONEUVOJEN KYBERUHAT JA NIIDEN TORJUMINEN

Informaatioteknologian ja viestinnän tiedekunta
Diplomityö
Marraskuu 2020

TIIVISTELMÄ

Sanna Rikkonen: Ajoneuvojen kyberuhat ja niiden torjuminen
Diplomityö
Tampereen yliopisto
Tietotekniikka, DI
Marraskuu 2020

Diplomityö tehtiin kartoittamaan vallitsevaa tilannetta ajoneuvoihin kohdistuvien kyberturvallisuusuhkien osalta. Työtä ohjasivat tutkimuskysymykset:

1. Mitkä ovat modernien ajoneuvojen merkittävimmät kyberuhat?
2. Mitä voidaan tehdä ajoneuvojen kyberturvallisuuden parantamiseksi?

Tutkimus tehtiin kirjallisuuskartoituksena. Enimmäkseen tietoa haettiin Andor ja Google Scholar -hakupalveluiden avulla tieteellisesti hyväksytyistä artikkeleista, mutta tietotokantahakuja täydentämään käytettiin julkisesti internetistä löytyviä uutisia ja videoita aiheeseen liittyen. Tiedonhaussa hyödynnettiin helmenkasvatus-menetelmää.

Modernien ajoneuvojen nopean kehityksen myötä ajoneuvojen haavoittuvat komponentit lisääntyvät vauhdilla. Lähes kaikkia ajoneuvon toimintoja ohjataan nykyään ohjelmallisesti ja siellä missä on elektroniikkaa, on myös potentiaalisia haavoittuvuuksia. Ohjelmallisen ohjauksen lisäksi ajoneuvojen verkottuminen on lisääntynyt merkittävästi. Useat ajoneuvot ovat suoraan yhteydessä internetiin ja hankkivat tietoa ympäristöstään erilaisten sensoreiden avulla. Ajoneuvojen turvallisuuskriittisten komponenttien suojaaminen kyberhyökkäyksiltä on erittäin tärkeää.

Sähköautot ovat vähintään yhtä alttiita kyberhyökkäyksille kuin muut verkottuneet ajoneuvot. Sen lisäksi ne yleistyessään tuovat mukanaan potentiaalisen uhan sähköverkolle. Autonomisten ajoneuvojen tuloa odotetaan, mutta pelkästään positiivisia odotukset eivät ole. Ajoneuvoverkko VANET (engl. Vehicular Ad hoc Network) on suunniteltu lisäämään liikenneturvallisuutta ja mukavuutta. Ajoneuvojen kommunikointi toistensa ja liikenneinfrastruktuurin kanssa tuo sujuvuutta liikenteeseen. Halu saada uusia elämää helpottavia ratkaisuja nopeasti käyttöön nostaa houkutusta unohtaa tietoturva.

Ajoneuvojen tietoteknisessä rakenteessa on paljon komponentteja, jotka palvelevat hyvin alkuperäisessä tarkoituksessaan. Näitä komponentteja ei kuitenkaan ole suunniteltu ajatellen ajoneuvojen olevan osa maailmanlaajuista tietoteknistä verkkoa. Jotta ajoneuvot olisivat turvallisia, pitäisi haavoittuvuuksien paikkaaminen aloittaa näistä perimmäisistä rakenteista. Lisäksi uusien rajapintojen lisääminen pitäisi aina tehdä tarkasti suunnitellen ja testaten. On vaarallista luottaa, että käyttäjä ymmärtäisi riskin esimerkiksi matkapuhelimen kytkemisessä ajoneuvoon.

Työ osoitti, että riskialttiita kohteita on paljon ja haavoittuvuuksia tulee koko ajan lisää. Suurin vastuu asiasta huolehtimisesta on tietenkin ajoneuvovalmistajilla, mutta on toimintamalleja, joilla käyttäjä voi omalta osaltaan tilannetta helpottaa. Tärkeintä on tiedostaa, että ajoneuvot ovat nykyään lähes täysin tietokoneita ja ne ovat alttiita kyberhyökkäyksille.

Avainsanat: Auton kyberturvallisuus, kyberhyökkäys ajoneuvoon, älykäs ajoneuvo, VANET, CAN, ECU.

ABSTRACT

Sanna Rikkonen: Threats to vehicular cybersecurity and their countermeasures
Master's thesis
Tampere University
Information Technology, MSc
November 2020

The aim of this master's thesis was to survey the current situation regarding cyber threats to vehicles. Main questions leading the research were:

1. What are the biggest cyber threats to modern vehicles?
2. How can the cybersecurity of vehicles be improved?

This study was conducted as a literature review. Information was mainly searched from scientific literature through Andor and Google Scholar search services, but public sources from internet were also used to extend the search. Method used was pearl growing.

Because of the fast development in the vehicle electronics, the number of vulnerable components in modern vehicles is increasing rapidly. Almost all functions in a vehicle are electronically controlled, and where there is electronics, there is potential for vulnerabilities. Apart from electronic components, the connectivity of vehicles has increased significantly. A large number of vehicles are directly connected to the internet and are also communicating with their surroundings with sensors. Protecting the safety critical components from cyberattacks is crucial.

Electric vehicles are at least as exposed to cyberattacks as more traditional connected vehicles. In addition, electric vehicles introduce potential threat to electricity grid. Autonomic vehicles are long awaited, but not only with positive expectations. Vehicle network VANET (Vehicular Ad hoc Network) is designed to bring more traffic safety and comfort. Vehicles communicating with each other and with infrastructure makes traffic more fluent. However, desire to deploy new life-easing solutions quickly increases the risk of ignoring data security.

In-vehicle network structure consists of several components that are great for what they are originally designed for. However, these components are not designed to be used in worldwide network of connected vehicles. For vehicles to be safe, patching of the vulnerabilities should start from these main structures. New connections should always be added only after thorough planning and testing. It is dangerous to rely on users' awareness of the risk that comes e.g. from connecting a mobile phone to a vehicle.

This research showed that several risks exist and the number of vulnerabilities is rising. The main responsibility lies with manufacturers, but there are measures that users can take to ease the situation on their part. Most important thing is to acknowledge that vehicles nowadays are mostly computers and thus vulnerable to cyberattacks.

Keywords: Automotive cybersecurity, vehicle cyberattacks, intelligent vehicle, VANET, CAN, ECU.

ALKUSANAT

Työn aiheen mielenkiintoisuus meinasi aiheutua sen suurimmaksi kompastuskiveksi, kun uppouduin lukemaan aiheesta ja etsimään aina uutta tietoa jatkoksi löytämälleni. Asioiden muistiin merkitseminen meinasi unohtua kokonaan. Olen silti erittäin tyytyväinen, että juuri tämä valikoitui aiheekseni ja työn tekeminen on ollut mielenkiintoista ja silmiä avaavaa.

Haluan kiittää ohjaajiani Marko Heleniusta ja Christina Lassfolkia tuesta työn tekemisessä. Erityiskiitos Christinalle positiivisesta patistamisesta ja miellyttävistä palavereista työn parissa. Kiitos myös Topi Tuukkaselle juuri minulle sopivan aiheen löytämisestä ja kannustuksesta työn edistämisessä. Erikseen nimettyjen henkilöiden lisäksi haluan osoittaa kiitokseni kaikille läheisilleni niin töissä kuin kotona. Kiitos kun olette olleet tukena.

Hyvinkäällä, 4.11.2020.

SISÄLLYSLUETTELO

KUVALUETTELO

TAULUKKOLUETTELO

LYHENTEET JA MERKINNÄT

ABS	engl. Anti-lock Braking System, lukkiutumaton jarrujärjestelmä
ACC	engl. Adaptive Cruise Control, adaptiivinen vakionopeudensäädin
ACK	engl. ACKnowledgement, vastaanottokuittaus
ADAS	engl. Advanced Driver Assistance System, ajoavustinjärjestelmä
ADS	engl. Automated Driving System, automaattiajojärjestelmä
CAN	engl. Controller Area Network, CAN-protokolla
CAN-FD	engl. CAN Flexible Data-Rate, CAN joustavalla tiedonsiirtonopeudella
CARB	engl. California Air Resource Board, Kalifornian osavaltion ilmanlaadusta vastaava viranomainen
CSMA/CA	engl. Carrier Sense Multiple Access with Collision Avoidance, siirtotien varausmenetelmä
DSRC	engl. Dedicated Short Range Communication, lyhyen kantaman tiedonsiirto
ECM	engl. Engine Control Unit, moottorinohjausyksikkö
ECU	engl. Electronic Control Unit, elektroninen ohjausyksikkö
EDR	engl. Event Data Recorder, tallennin
EPA	engl. Environmental Protection Agency, ympäristönsuojeluvirasto
HVAC	engl. Heating, ventilation and air conditioning, ilmastointi
IDS	engl. Intrusion Detection System, tunkeutumisenhavaitsemisjärjestelmä
IoT	engl. Internet of Things, esineiden internet
IPS	engl. Intrusion Prevention System, tunkeutumisenestojärjestelmä
ITS	engl. Intelligent Transport System, älykäs liikennejärjestelmä
JIT	engl. Just In Time, juuri ajallaan; ajoneuvon reaaliaikaisen huollon käsite.
JVM	engl. Java Virtual Machine, Java virtuaalikone
LF	engl. Low Frequency, taajuusalue
LiDAR	engl. Light Detection and Ranging, optinen tutka
LIN	engl. Local Interconnect Network, kommunikointiväyläprotokolla
LTE	engl. Long-Term Evolution, neljännen sukupolven langaton tiedonsiirtotekniikka
MANET	engl. Mobile Ad hoc Network, mobiililaitteiden dynaaminen verkko
MOST	engl. Media Oriented System Transport, kommunikointiväyläprotokolla
NHTSA	engl. National Highway Traffic Safety Administration, Yhdysvaltain liittovaltion liikenneturvallisuusvirasto
NIST	engl. National Institute of Standards and Technology, yhdysvaltalainen kauppaministeriön alainen virasto
OBD	engl. On Board Diagnostics, ajoneuvon itsediagnosointi
OBU	engl. On Board Unit, sisäinen yksikkö
OSI model	engl. Open System Interconnection Reference Model, viitteellinen tietoverkkomalli
PKES	engl. Passive Keyless Entry and Start, avaimeton avaus ja käynnistys
RFID	engl. Radio-Frequency identification, radiotaajuinen etätunnistus
RSU	engl. Road Side Unit, tienvarsiyksikkö
TDM	engl. Time Division Multiplexing, aikajakokanavointi
TDMA	engl. Time Division Multiple Access, aikajakoinen moniliittymä
UHF	engl. Ultra High Frequency, radioaaltojen taajuusalue
VANET	engl. Vehicular Ad hoc Network, ajoneuvojen dynaaminen verkko

V2I	engl. Vehicle to Infrastucture, ajoneuvojen ja infrastruktuurin välinen kommunikaatio
V2P	engl. Vehicle to Pedestrians, ajoneuvojen ja jalankulkijoiden välinen kommunikaatio
V2V	engl. Vehicle to Vehicle ajoneuvojen keskinäinen kommunikaatio
V2X	engl. Vehicle to Everything ajoneuvojen kommunikaatio kaiken kanssa
WLAN	engl. Wireless Local Area Network, langaton lähiverkko

1. JOHDANTO

Ensimmäinen polttomoottoriauto valmistui vuonna 1806. Ensimmäisen version polttoaineena toimi polttokaasu, vuonna 1885 valmistui ensimmäinen bensiinikäyttöinen auto. Tämän modernin auton kehittäjänä pidetään saksalaista insinööriä, Karl Benziä. Benz oli suurin autovalmistaja, 572 valmistetulla autolla vuonna 1899. Autot olivat todella kalliita ja vain kaikkein rikkaimmilla, kuten kuninkailla, oli varaa niitä ostaa. Tavallisen kansan saataville autot tulivat vuonna 1914 Henry Fordin - Ford Model T:n - myötä. Tämän jälkeen autot alkoivat yleistyä tuotantokulujen laskiessa. [1] Tuolloin kaikki toiminnot olivat mekaanisia, eikä ajoneuvojen tietoturvallisuudesta tarvinnut olla huolissaan. Kun elektroniikkaa sitten alettiin käyttää, elektroninen ohjaus on yleistynyt ripeää tahtia.

Toisen maailmansodan jälkeen, 1950-luvulla, suuret autonvalmistajat ryhtyivät kehittämään toinen toistaan suurempia ja näyttävämpiä autoja. Samoihin aikoihin alkoi ajoneuvoihin tulla mukaan elektroniikkaa, kun ensimmäinen täystransistoriautoradio esiteltiin vuonna 1955. Vuonna 1960 Plymouth Valiantissa otettiin käyttöön vaihtovirtageneraattori. Vuonna 1963 Pontiac, ensimmäisenä autonvalmistajana, otti käyttöön vaihtoehtoisen elektronisen sytytyksen. Lukkiutumattomat jarrut toivat merkittävän lisäyksen ajoneuvoelektroniikkaan 1971. Ensimmäiset elektroniset moottorinohjausyksiköt (ECM, engl. Engine Control Modul) tulivat kuvaan 1979, mutta ensimmäisissä malleissa elektroniikkaa oli kuitenkin vielä hyvin maltillisesti. Kyseinen tekniikka kehittyi nopeasti ja parin seuraavan vuoden aikana elektroninen moottorinohjaus alkoi vallata alaa. Turvatyyny konseptina on kehitetty jo 1950-luvulla, mutta vasta 1980-luvun alussa turvatyynyihin tuli elektroninen ohjaus. Vaihteiston hallinta muuttui elektroniseksi 1980-luvun lopulla. GPS-navigointi tuli autonvalmistajien käyttöön jo 1980-luvun alussa, mutta vasta vuonna 1990 Mazda esitteli ensimmäisenä autoon integroidun GPS-navigointijärjestelmän. Peruutuskameran esitteli ensimmäisenä Toyota vuonna 1991. [2] Ajonvakautusjärjestelmän otti ensimmäisenä tuotantoon Mercedes vuonna 1995 ja se lähti yleistymään nopeasti [3].

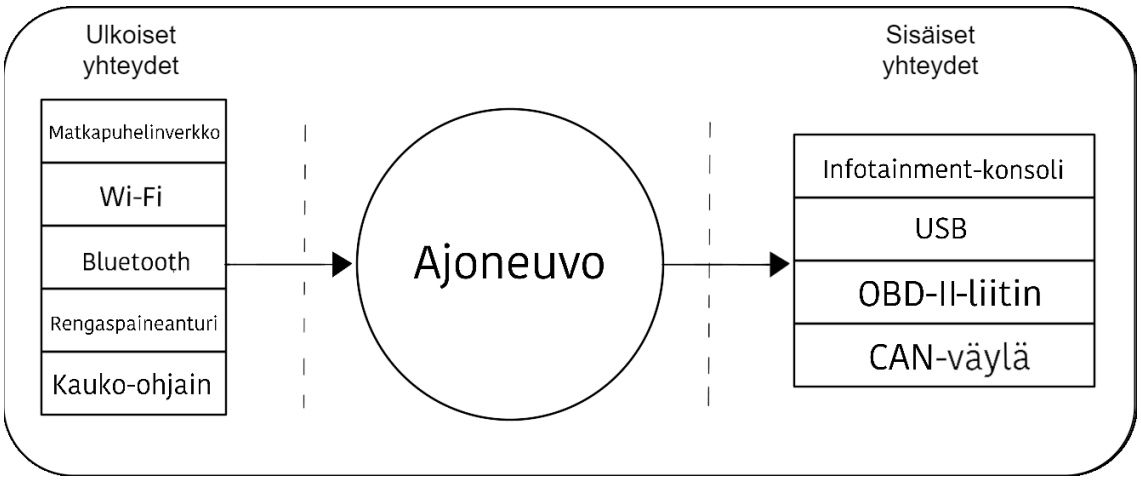
Nykyään ajoneuvoissa lähes kaikki toiminnot ovat elektronisesti ohjattuja. Modernit autot ovat lähinnä pyörillä kulkevia tietokoneita. Hyvin vähän on jäljellä yhtäläisyyksiä ensimmäisten autojen kanssa. Ottaen huomioon, että pyrkimys autonomisten autojen maailmaan on ollut esillä jo pitkään, elektroniikan ja ohjelmakoodin määrä ajoneuvoissa näyttäisi olevan kasvamassa tulevina vuosina. Esineiden internetin (IoT, engl. Internet of

Things) yleistyessä, myös ajoneuvoissa tulee olemaan entistä enemmän ominaisuuksia, jotka tarvitsevat internet-yhteyttä.

Tällä hetkellä pyrkimyksenä näyttäisi olevan täysin autonomiset ajoneuvot. Henkilökohtaisia ajoneuvoja ei välttämättä tarvittaisi, vaan ajoneuvon voisi tarvittaessa tilata paikalle, itselleen sopivilla varusteilla. Tällainen skenaario vaikuttaisi jopa mahdolliselta muutaman vuoden kuluessa, tosin ihan lähitulevaisuudessa se ei tule toteutumaan. Matkalla täyteen autonomiaan on vielä useita välivaiheita ja paljon ongelmia ratkottavaksi. Kyydin jakamispalvelut, kuten Uber ja Lyft, ovat jo suosittuja ja näiden lisäksi yhteiskäyttöiset autot alkavat yleistyä [4]. Ajoneuvojen tulevaisuuteen vaikuttaa myös ilmastonmuutos. Ympäristön kannalta sillä, mistä ajoneuvot tulevaisuudessa saavat energiansa, on suuri merkitys. Vielä ei ole päästy yksimielisyyteen siitä, mikä olisi ympäristön kannalta paras ratkaisu ja eri vaihtoehtojen tutkimista jatketaan [5]. Sähköautot ovat yleistyneet kovaa vauhtia ja niissä elektronisen ohjauksen merkitys korostuu entisestään. Tästä hyvänä esimerkkinä Tesla, jossa kaikki toiminnot ovat elektronisesti säädeltyjä. Teslakaan ei ole vielä kykenevä toimimaan täysin autonomisesti, eikä se selviäisi kaikista tilanteista itsenäisesti, mutta siihen ollaan toimitusjohtajan Elon Muskin mukaan pääsemässä lähitulevaisuudessa [6].

Uusien ominaisuuksien lisääminen ajoneuvoihin tekee niistä älykkäämpiä ja parantaa ajokokemusta. Kuitenkaan ajoneuvon sisäisen verkon turvallisuuskriittisen luonteen vuoksi ominaisuuksien lisäämisestä aiheutuvaa turvallisuusuhkaa ei voi sivuuttaa. Moderneissa ajoneuvoissa on useita komponentteja, jotka ovat alttiita hyökkäyksille. [7] Näitä komponentteja on esitetty kuvassa 1 jaoteltuina ajoneuvon sisäisiin ja ulkoisiin yhteyksiin. Yhteyden ajoneuvon ulkopuolelta mahdollistavat matkapuhelinverkko, Wi-Fi, Bluetooth, rengaspaineanturi sekä lukituksen kauko-ohjain. Ajoneuvon kanssa kosketuksiin pääseminen vaativia komponentteja taas ovat tietoviihdepalveluista vastaava infotainment-järjestelmä, USB- ja OBD-liitin (engl. On Board Diagnostics) sekä CAN-väylä (engl. Controller Area Network). Edellä mainittujen yhteiskäyttöisten ajoneuvojen yleistyminen lisää osaltaan ajoneuvojen haavoittuvuutta, kun useilla ihmisillä on pääsy ajoneuvojen fyysisiin rajapintoihin. Jotta turvallisuutta ja sujuvuutta parantamaan tarkoitetut

ominaisuudet eivät kääntyisi itseään vastaan, on haavoittuvuuksiin tutustumiselle tarvetta.



Kuva 1. *Ajoneuvon hyökkäykselle alttiita komponentteja. Perustuu lähteeseen [7].*

Tietotekniikan määrä ajoneuvoissa kasvaa nopeasti uusien turvallisuus-, mukavuus- ja viihdesovellusten myötä [8,9]. Turvallisuutta lisäämään suunnitellut sovellukset voivat kuitenkin pahimmassa tapauksessa lisätä riskejä, mikäli sovelluksen ja koko järjestelmän tietoturvassa on aukkoja.

1.1 Tutkimusongelma

Työn tarkoituksena oli tehdä kirjallisuuskartoitus ajoneuvojen kyberturvallisuudesta. Tämä tehtiin etsimällä vastauksia tutkimuskysymyksiin:

1. Mitkä ovat modernien ajoneuvojen merkittävimmät kyberuhat?
2. Mitä voidaan tehdä ajoneuvojen kyberturvallisuuden parantamiseksi?

Tässä työssä keskitytään maalla liikkuviin moottoriajoneuvoihin; henkilöautoihin sekä linja- ja kuorma-autoihin. Pääpaino on henkilöautoissa, niiden merkittävän viimeaikaisen kehityksen vuoksi. Vastaavia kyberuhkia ja torjunta keinoja tulee vastaan myös suurempien ajoneuvojen yhteydessä, mutta linja- ja kuorma-autoissa niiden suuri koko aiheuttaa omat lisähuolensa.

Yhteneväisyyksistä johtuen pakettiautot on niputettu yhteen henkilöautojen kanssa, eikä pakettiautoja varsinaisesti käsitellä omana ryhmänään. Kaksipyöräiset ajoneuvot on myös jätetty yksilöllisen tarkastelun ulkopuolelle. Kuitenkin niiltä osin kuin esimerkiksi modernien moottoripyörien ominaisuudet vastaavat ajoneuvojen ominaisuuksia, riskit ovat myös vastaavia.

Työssä käsitellään lyhyesti myös autonomisia ajoneuvoja sekä saattueajoa, mutta niiden teknisiin ominaisuuksiin ei perehdytä syvällisesti. Työn ulkopuolelle on rajattu lentokoneet, työkoneet, junat, laivat ja sotilasajoneuvot, niiden erityispiirteiden ja erityisesti lentokoneiden ja sotilasajoneuvojen osalta tiedon rajatun saatavuuden vuoksi.

Työn lähteiksi on valittu ensisijaisesti alle kymmenen vuotta vanhoja tutkimuksia, sillä kuten muutoin tekniikassa, myös ajoneuvojen tekniikassa kehitys on nopeaa. Mukana on kuitenkin myös joitakin kymmenen vuoden takaisia ja vanhempia julkaisuja, sillä autokanta uusiutuu hitaasti. Kaikkiin ongelmiin ei ole löydetty aukottomia ratkaisuja vuosien varrella, eikä uusia, turvallisempia ratkaisuja välttämättä pystytä integroimaan jo liikenteessä olevaan ajoneuvoon.

1.2 Tutkimusmenetelmä

Tutkimus toteutettiin kirjallisuuskartoituksena etsimällä julkaisuja tietokannoista ajoneuvojen ja niiden osien kyberturvallisuusnäkökulmasta. Tietokantojen ulkopuolisia hakuja käytettiin täydentämään kokonaisuutta.

Kirjallisuuskartoitus toteutettiin helmenkasvatus-menetelmällä [10,11]. Käytettyä tutkimusmenetelmää ja helmenkasvatus-metodia kuvataan tarkemmin luvussa 2.

1.3 Aiempi tutkimus

Ajoneuvojen kyberuhista löytyy paljon tietoa internetistä. Suurin osa materiaalista on kuitenkin englanninkielistä. Tällä laajuudella tehtyä koostetta ajoneuvojen kohtaamista kyberuhista ja niiden mahdollisista vastatoimista ei suomenkielellä nähdäkseni ole tehty.

Pääosa ajoneuvojen kyberturvallisuutta käsittelevästä materiaalista lähestyy aihetta jonkin tietyn ominaisuuden, kuten autonomisen ajamisen tai ajoneuvojen välisen kommunikaation, näkökulmasta. Kokonaisvaltaisempia katsauksia löytyy myös ja niitä on koottu lukuun 3.1. Lisäksi luvussa reflektoidaan tätä kartoitusta olemassa oleviin tutkimuksiin.

1.4 Tulokset

Tutkimuksessa selvisi, että kyberhyökkäykset ovat todellinen uhka ajoneuvoille. Liikenneturvallisuuden parantamiseksi lisätyt ominaisuudet ajoneuvoissa saattavat pahimmillaan kääntyä tarkoitustaan vastaan. Uudet ominaisuudet vaativat uusia yhteyksiä ja näin ollen kasvattavat potentiaalisten haavoittuvuuksien määrää.

Ajoneuvojen kyberturvallisuuden eteen on onneksi tehty paljon työtä, mutta lisää tutkimusta aiheesta tarvitaan jatkossakin. Jotta kyberturvallisuutta pystytään parantamaan,

tulee ajoneuvo- ja komponenttivalmistajien tunnistaa haavoittuvuuksia ja tehdä korjauksia niiden paikkaamiseksi. Lisäksi käyttäjien tulee pysyä valppaana ja muistaa omassa toiminnassaan, etteivät ajoneuvot ole immuuneja kyberhyökkäyksille.

1.5 Työn rakenne

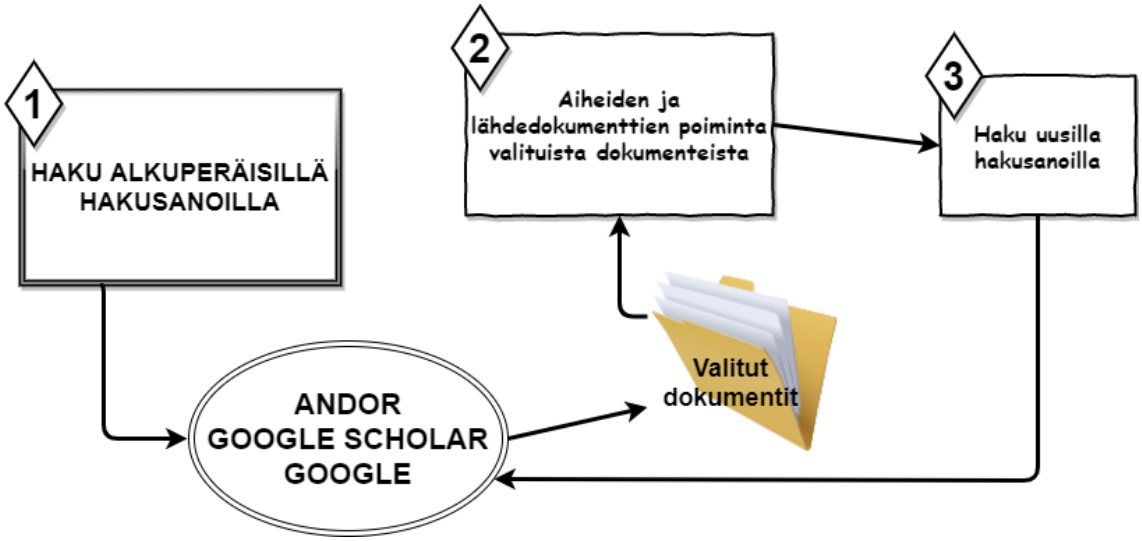
Luvussa 2 käydään läpi käytetty tutkimusmenetelmä ja luvussa 3 tehdään katsaus aiempaan kirjallisuuteen aiheesta. Luku 4 avaa keskeisimpiä käsitteitä aiheen ympäriltä. Luvussa 5 tutustutaan älykkäisiin ajoneuvoihin ja niiden haavoittuvuuksia käsitellään tarkemmin luvussa 6.

Ajoneuvotyyppikohtaisia eroja ja yhtäläisyyksiä, sekä niiden vaikutuksia ajoneuvon riskiin joutua kyberhyökkäyksen kohteeksi, käsitellään luvussa 7. Lukuun 8 puolestaan on koottu toimia, joilla ajoneuvojen kyberturvallisuutta voidaan kohentaa. Lopuksi luvussa 9 käsitellään tutkimuksen tuloksia ja luku 10 on yhteenveto koko työstä.

2. MENETELMÄT

Työ tehtiin kirjallisuuskartoituksena etsimällä julkaisuja tietokannoista ja tutustumalla internetistä löytyneisiin uutisartikkeleihin ajoneuvojen hakkeroinnista. Erilaisia hakusanoja kertyi jo ohjaajan opastamana toistakymmentä ja lista piteni dokumentteja läpikäytäessä. Kirjallisuuslähteiden lisäksi tietoa aiheesta ja ideoita uusista hakusanoista kertyi keskusteluista aiheesta kiinnostuneiden ihmisten kanssa.

Varsinaiseksi metodiksi valikoitui niin kutsuttu helmenkasvatus-menetelmä. Tässä metodissa haetaan ensin julkaisuja ennalta valituilla hakusanoilla ja tutustutaan löytyneiden kiinnostavien julkaisujen lähdeluetteloihin [10,11]. Lähdeluettelosta poimitaan jälleen kiinnostavat lähteet ja jatketaan samalla tavalla eteenpäin. Kirjallisuuden hakeminen tapahtui kuvan 2 mukaisesti. Lisäksi tutustuttiin tieteellisiin julkaisuihin, joissa oli viitattu aiemmin löydettyihin julkaisuihin.



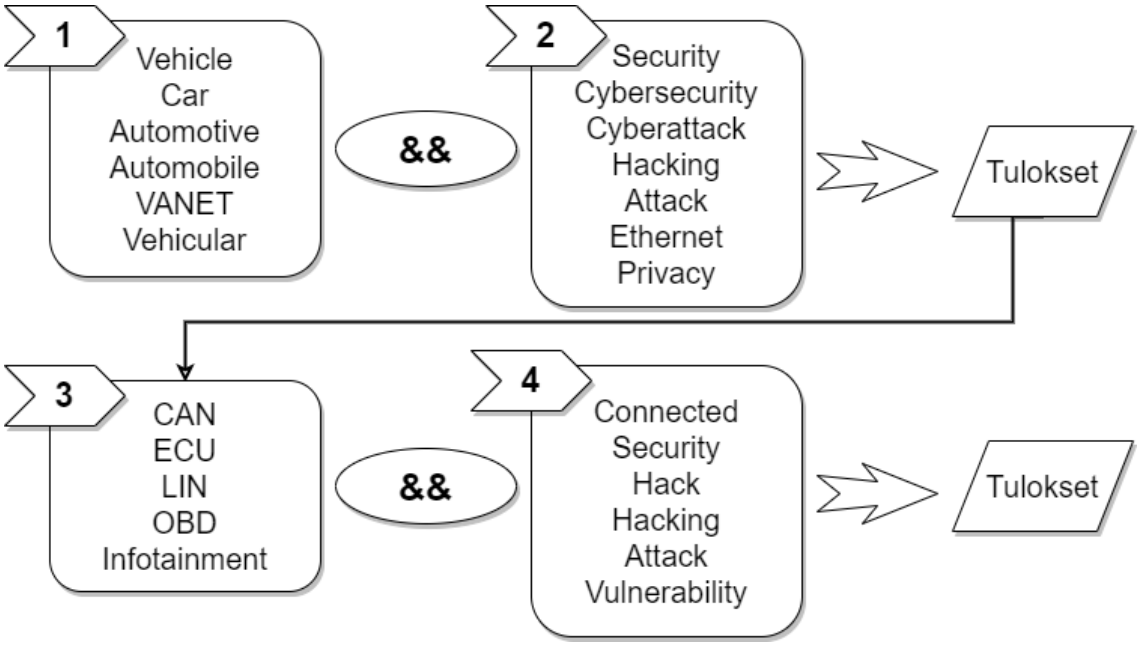
Kuva 2. *Työssä käytetyn kirjallisuuden haun periaatekuva. Hakupalveluina käytössä Andor, Google Scholar ja Google.*

Helmenkasvatus valikoitui käytettäväksi menetelmäksi, koska se soveltui hyvin ajantasaisen tiedon etsimiseen tutkimuksen aihealueesta. Systemaattiseen kirjallisuuskartoitukseen verrattuna helmenkasvatuksen etuna on mahdollisuus seurata parhaiten etsittyyn tietoon osuvia lähteitä. Näin ollen helmenkasvatuksella on systemaattista kirjallisuuskartoitusta helpompi löytää ajantasaista ja teknistä tietoa vähän tutkitusta aihepiiristä.

Tärkeimmät hakusanat, kuten esimerkiksi *automotive*, *vehicular*, *cybersecurity* ja *security*, seurasivat mukana prosessin edetessä. Jotkin hakusanat, kuten *privacy* ja *ethernet*,

jäivät aikaa myöden pois, sillä tulokset sisältyivät suurelta osin jo muiden hakujen tuloksiin. Kuvaan 3 on koottu tärkeimmät hakusanat jaoteltuina numeroituihin ryhmiin.

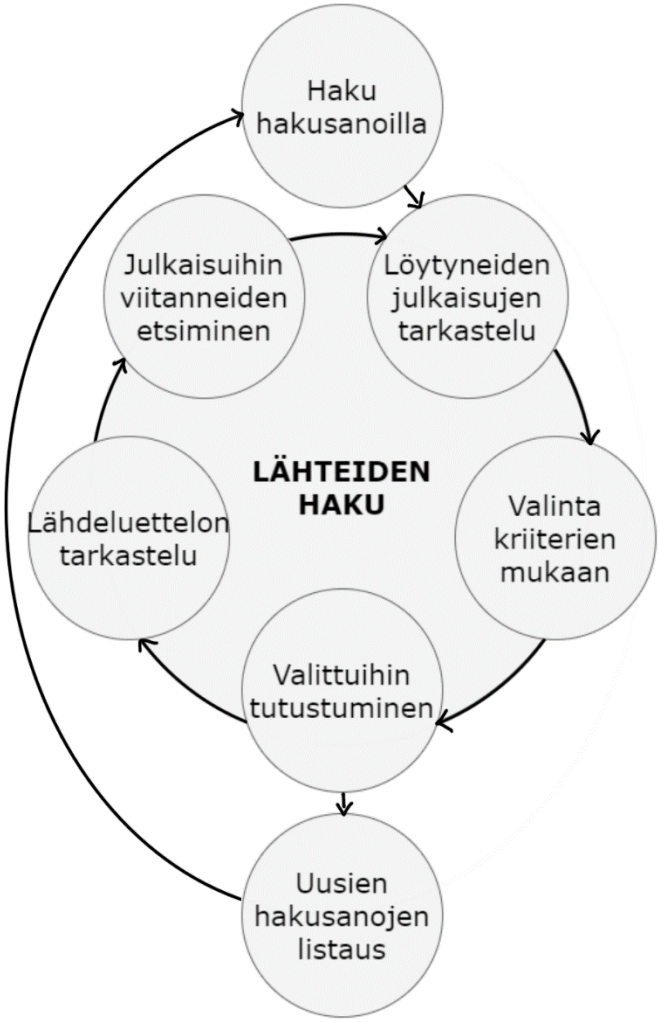
Ensimmäisillä kierroksilla materiaalia haettiin yhdistämällä ryhmän yksi hakusanat ryhmän kaksi hakusanoihin käyttämällä JA-operaattoria (&&). Näillä hakusanayhdistelmillä löytyneestä materiaalista kävi ilmi, että ryhmän kolme hakusanoja tarvitaan myös. Seuraavat hakukierrokset tehtiin yhdistämällä ryhmän kolme hakusanat ryhmän neljä sanoihin jälleen JA-operaattorilla. Ryhmät yksi ja kolme sisältävät tutkittua järjestelmää kuvaavia sanoja. Ryhmät kaksi ja neljä puolestaan kuvaavat tilannetta, josta tietoa etsittiin. Kaikki käytetyt hakusanat on listattu liitteeseen A.



Kuva 3. *Tärkeimmät hakusanayhdistelmä: Ryhmät 1 ja 2 yhdistettiin JA-operaattorilla. Tuloksista poimitut hakusanat ryhmiin 3 ja 4 yhdistettiin jälleen JA-operaattorilla.*

Yksi hakukierros koostui hakusanaparilla, tai yksittäisellä hakusanalla suoritetusta hausta. Tämä prosessi on esitetty kuvassa 4. Haun tuloksia tarkastelemalla valittiin kriteerien mukaiset hakutulokset lähempään tarkasteluun. Tässä tarkastelussa hakutulosten sisältöön tutustumisen ja uusien hakusanojen poimimisen lisäksi käytiin läpi julkaisun lähdeluettelo, josta poimittiin talteen kriteereihin sopivat lähteet.

Lisäksi tutustuttiin julkaisuihin, joissa oli viitattu alkuperäiseen hakutulokseen. Valitut lähteet ja viitanneet julkaisut päätyivät omalle tarkastelukierrokselleen. Tällaista tarkastelukierrosta voidaan kutsua hakukierroksen alikierrokseksi. Hakutuloksesta poimitut uudet hakusanat kirjattiin ylös, odottamaan omaa hakukierrostaan. Esimerkiksi hakusanaparilla *'vehicle AND cyberattack*' suoritettu haku tuotti useita hakutuloksia.



Kuva 4. *Hakukierros. Jokainen hakusanaparilla, tai yksittäisellä hakusanalla, suoritettu hakukierros sisälsi alikierroksia, joissa tutkittiin valittujen julkaisujen lähdejulkaisuja sekä julkaisuja, joissa näihin valittuihin oli viitattu.*

Edellä mainittujen hakujen lisäksi suoritettiin muutamia tietokantojen ulkopuolelle kohdistuvia täydentäviä hakuja. Täten esimerkiksi Googlen kautta haettiin kiinnostavimpia nostoja aiheen ympäriltä sekä vastauksia yksittäisiin kysymyksiin. Ajatuksia hakuihin ja tutkittaviin kohteisiin saatiin lisäksi keskusteluista aiheesta kiinnostuneiden ihmisten kanssa.

Käytetyistä lähteistä 61 prosenttia oli tieteellisiä julkaisuja. Tieteellisiksi julkaisuiksi luokiteltiin tieteellisten tietokantojen lehtiartikkelit, konferenssijulkaisut ja kirjat. Lisäksi standardit luokiteltiin tässä tutkimuksessa tieteellisiksi lähteiksi, koska niiden luotettavuus vastaa tieteellistä lähdettä. Muut lähteet luokiteltiin ei-tieteellisiksi. Ei-tieteellisiksi viitteiksi päätyi eniten verkkosivuja, mutta mukana oli myös sanoma- ja aikakausilehtiartikkeleita, raportteja sekä YouTube-videoita. Verkkosivuissa suurin edustus oli viranomaisten ja haettujen järjestelmien valmistajien sivuilla. Käytettyjen lähdetyyppien prosenttiosuudet on koottu taulukkoon 1.

Taulukko 1. *Käytettyjen lähteiden jakauma.*

Tieteelliset julkaisut (osuus käytetyistä lähteistä 60%)	***Osuus tieteellisistä julkaisuista %***
Lehtiartikkeli	59%
Konferenssijulkaisu	17%
Kirja	14%
Standardi	9%
Ei-tieteelliset lähteet (osuus käytetyistä 40%)	***Osuus ei-tieteellisistä lähteistä %***
Verkkosivu	63%
Sanomalehtiartikkeli	14%
Raportti	7%
Aikakausilehtiartikkeli	7%
Muut	9%

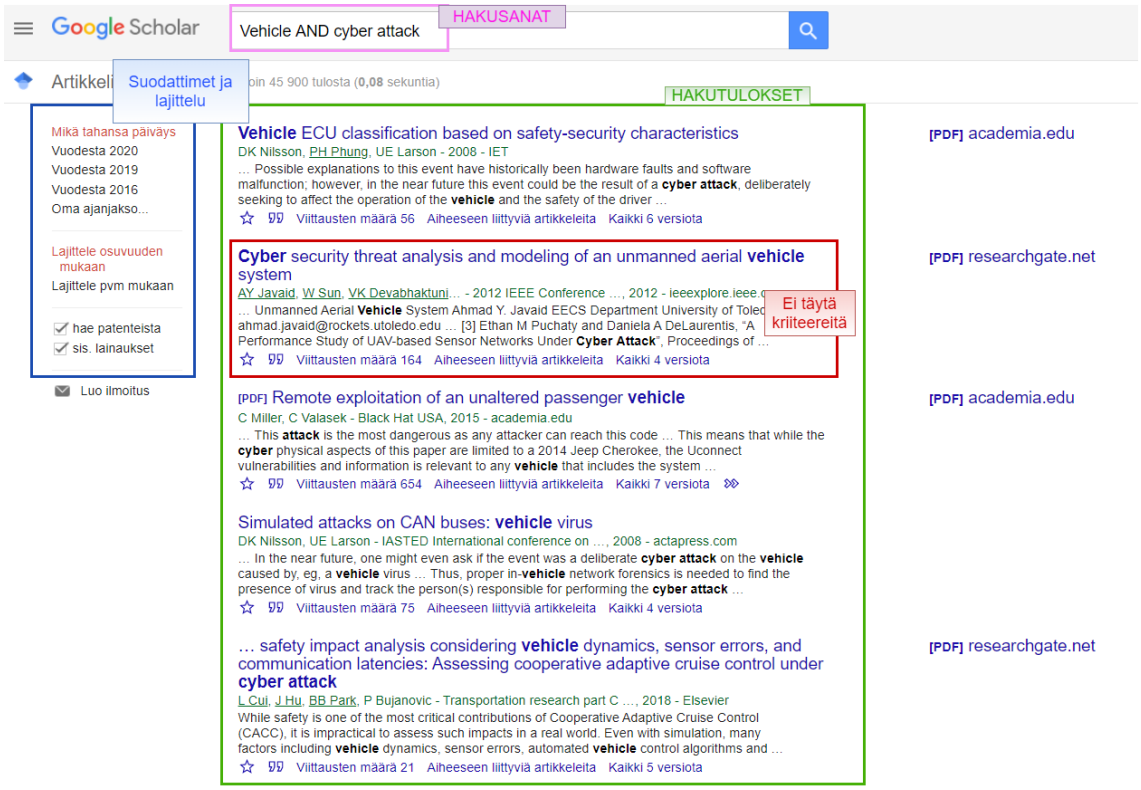
2.1 Tietokannat

Tietokantahaut suoritettiin enimmäkseen Andor [12] ja Google Scholar [13] hakupalveluiden avulla. Andor on Tampereen yliopiston hakupalvelu, joka hakee tuloksia 409 tietokannasta. Google Scholar puolestaan on Googlen palvelu, joka kohdistaa haut tieteellisiin julkaisuihin. Myös joitakin suoria hakuja IEEE Xplore -kirjastoon [14] tehtiin.

Hakutuloksista ensimmäisellä kierroksella valikoitui tutustuttavaksi laajasti artikkeleita ja kirjoja, jotka käsittelivät maalla liikkuvien ajoneuvojen turvallisuutta ja tietoteknistä rakennetta. Lentäviä, raiteilla, maan alla, avaruudessa ja vedessä liikkuvia kulkuneuvoja käsittelevät artikkelit karsiutuivat aiemmin kuvattujen tutkimusta rajaavien kriteerien mukaan pois.

Kuvassa 5 on esimerkkihaku Google Scholar -hakupalvelusta. Hakusanat on merkitty kuvaan vaaleanpunaisella suorakulmiolla ja keskellä on vihreällä kehystettynä hakutulokset. Lisäksi kuvaan on merkitty sinisellä hakutulosten suodattamiseen ja lajitteluun

tarkoitetut työkalut. Yksi hakutulos poikkesi kriteereistä ja se on merkitty kuvaan punaisella.



Kuva 5. *Kuvakaappaus Google Scholar -hakupalvelusta.*

Hakutuloksia kertyi paljon, eivätkä kaikki tulokset päätyneet tarkempaan tarkasteluun. Tuloksista suurimman painoarvon saivat alle kymmenen vuotta vanhat julkaisut. Kaikkein uusimmat julkaisut olivat kiinnostavia ajantasaisuutensa vuoksi, mutta liikenteessä olevien ajoneuvojen laajan ikäjakauman johdosta vanhempiakaan tuloksia ei sivuutettu.

Suurin osa hauista tehtiin ilman aikarajausta ja järjestettynä osuvuuden mukaan. Tilanteissa, joissa hakutuloksia oli paljon ja hakusanoihin nähden relevanteimmat painottuivat kymmenen vuoden takaisiin, tulosten uudelleen järjestämisestä julkaisuvuoden mukaan oli apua. Tällä tavoin saatiin esiin hakukohteen ajantasainen tilanne. Varsinaista aikarajausta käytettiin vain, kun etsinnässä oli viimeisin tieto, jonkin spesifin kohteen osalta. Tällöin käytössä oli rajaus viimeisen viiden vuoden aikaisiin julkaisuihin.

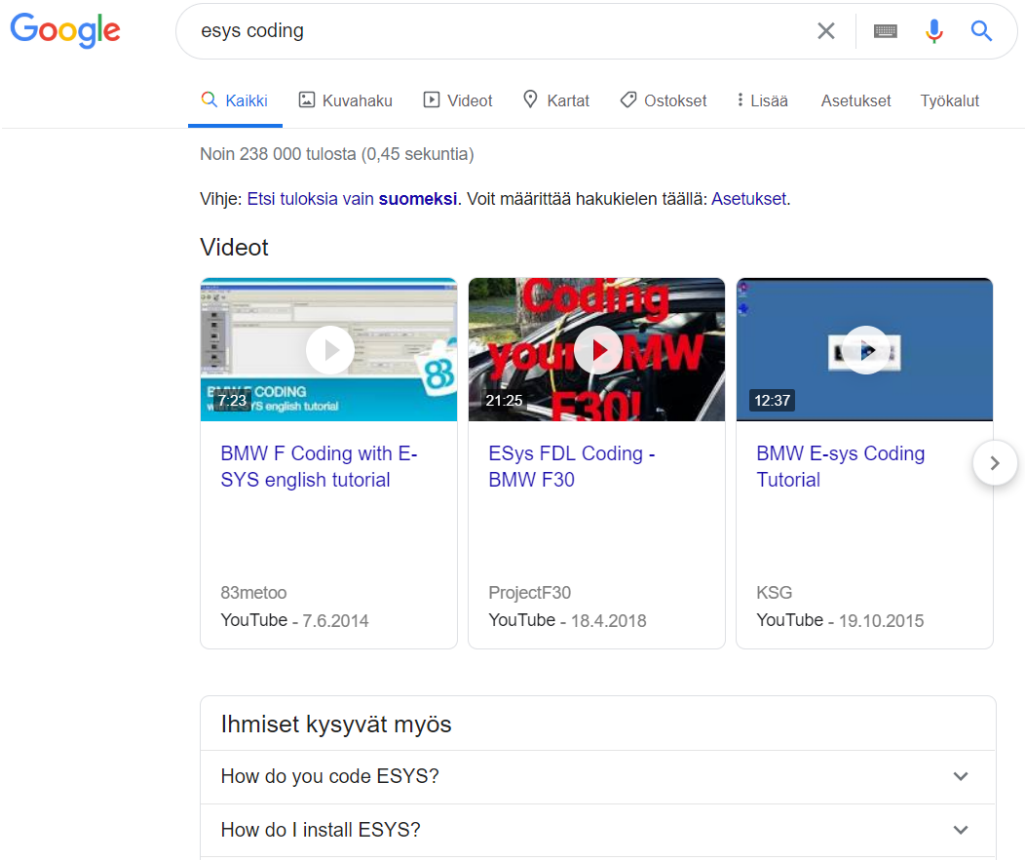
2.2 Google-haut

Google-hakujen hakutuloksille tehtiin seulontaa myös lähdetyypin mukaan. Keskustelupalstoihin osoittavat hakutulokset eivät jääneet huomiotta, mutta varsinaisina lähteinä

niitä ei käytetty. Keskustelupalstoilta löytyi näkökulmia ja uusia hakukohteita, joihin etsittiin tietoa luotettavammista lähteistä. Aikakausilehtien ja videoiden kaltaisten hakutulosten osalta tiedon löytyminen useasta eri mediasta nosti niiden luotettavuutta lähteenä.

Google-hakuja käytettiin lisänä täydentämään tieteellisten lähteiden tuloksia esimerkiksi teknisistä yksityiskohdista ja tuoreimmista löydöksistä, joita ei tieteellisissä lähteissä käsitelty. Teknisten ratkaisujen kohdalla tiedon luotettavuus oli varmistettavissa esimerkiksi käyttämällä useita lähteitä tai järjestelmien virallisia internetsivuja.

Erityisesti ajoneuvon tee-se-itse-koodaamiseen hakutuloksia kertyi eniten Google-hauilla. Kuvasta 6 näkyy, että ajoneuvon koodaukseen kohdistuvan haun tulokset sisälsivät ohjevideoita aiheesta.



Kuva 6. *Google-haku ajoneuvon koodauksesta.*

Myös onnistuneista hakkerihyökkäyksistä ja löytyneistä haavoittuvuuksista ymmärrettävästi uutisoidaan paljon. Toisaalta autonvalmistajien intresseissä on pitää tieto onnistuneista hyökkäyksistä piilossa, jotta ne eivät vaikuttaisi yhtiön maineeseen. Autonomiset ja sähköajoneuvot ovat myös viime aikoina olleet paljon käsiteltyjä aiheita.

3. AIEMPI TUTKIMUS

Tässä luvussa käsitellään samasta aiheesta aiemmin tehtyjä tutkimuksia ja verrataan niiden lähtökohtia, havaintoja ja tuloksia suhteessa tähän tutkimukseen. Luvun tarkoituksena on antaa kuva siitä, miten tämä tutkimus sijoittuu suhteessa muuhun aiheesta tehtyyn tutkimukseen. Ensisijaisesti haussa oli ajoneuvojen kyberturvallisuutta laajasti käsittelevät tutkimukset, jotka on toteutettu kirjallisuuskartoituksena. Nämä vastaavat tämän työn toteutusta ja tavoitteita parhaiten.

Haun rajaukset pohjautuvat yhtä lailla tämän työn rajauksiin, joten käsittelyyn otettiin vain maalla liikkuvien ajoneuvojen kyberturvallisuutta käsitteleviä tutkimuksia. Rajaamalla haku julkaisuvuoden mukaan korkeintaan kymmenen vuotta vanhoihin julkaisuihin, saatiin hakutulokset rajattua tämän työn kanssa vertautuviin tutkimuksiin.

Aiemman tutkimuksen löytämiseksi tehtiin hakuja Andor, Google Scholar ja Finna.fi-hakupalveluiden avulla. Käytössä oli seuraavat hakusanayhdistelmät:

- (vehicle OR automobile OR automotive) AND (cyber OR security OR vulnerability) AND (survey OR review OR overview OR study)
- (ajoneuvo OR auto) AND (kyber OR turvallisuus OR haavoittuvuus) AND (tutkimus OR selvitys OR katsaus)

Ajoneuvojen kyberturvallisuus on pinnalla oleva aihe. Tästä syystä on ymmärrettävää, että aihetta käsittelevää materiaalia, erityisesti viimeisen kymmenen vuoden ajalta, löytyy paljon. Suurin osa artikkeleista käsittelee kyberturvallisuutta kuitenkin jonkin tietyn osa-alueen, kuten ajoneuvoverkko VANETin, autonomisten ajoneuvojen tai CAN-väylän, näkökulmasta. CAN-väylän turvallisuutta käsittelevät tutkimukset sivuavat väylän yleisyydestä ja laajuudesta johtuen myös muita ajoneuvon haavoittuvia komponentteja.

Kokonaisvaltaisemmin ajoneuvojen kyberturvallisuutta tarkastelevia tutkimuksia löytyi enimmäkseen englanninkielellä. Suomenkielisiä lähinnä eri tasoisia opinnäytetöitä, löytyi kokonaisuudessaan alle kymmenen ja niistä vain yksi insinöörityö [15] käsitteli ajoneuvojen tietoturvaa kokonaisuutena. Toinen suomenkielinen kandidaatintyö [16] perehtyi CAN-väylän tietoturvaan.

Molemmat mainitut, kirjallisuuskartoituksena toteutetut, suomenkieliset opinnäytteet [15,16] nostavat esiin tärkeitä asioita ajoneuvojen tietoturvallisuudesta. Insinööri- ja kandidaatintyön laajuuden takia tutkimukset eivät kuitenkaan pysty käsittelemään laajaa ai-

hetta syvällisesti. Muut suomenkieliset ajoneuvojen kyberturvallisuuskategoriaan menevät hakutulokset olivat enimmäkseen aiheeltaan rajattuja. Autonomisten ajoneuvojen kyberturvallisuutta eri näkökulmista tarkastelevia tutkimuksia oli näistä kolme [17-19].

Englanninkielinen tutkimus aiheesta jakautuu pääosin kahteen ryhmään. Osa tutkimuksista on toteutettu kokeellisesti, kun taas osa on tämän työn tavoin kirjallisuuskartoituksia. Kokeellisesti toteutetut tutkimukset ovat suppeampia, sillä testattavia kohteita on paljon, eivätkä kaikki ajoneuvot ole alttiita samoille uhille. Vuonna 2014 Miller ja Valasek julkaisivat kuitenkin tutkimuksensa [20], jonka he olivat toteuttaneet testaamalla useita eri haavoittuvuuksia 21 eri mallisessa autossa.

3.1 Kirjallisuuskartoitukset

Tässä luvussa käsitellään parhaiten aihealueeltaan ja tutkimusmenetelmältään tätä työtä vastaavat hakutulokset. Sivuosumat, jotka pitävät sisällään kokeellisella tutkimuksella tuotetut alkuperäisartikkelit ja rajatun aihealueen kirjallisuuskartoitukset, käsitellään luvussa 3.2.

Alla olevaan taulukkoon 2 on koottu löydetyt kirjallisuuskartoitukset, jotka käsittelevät ajoneuvojen kyberturvallisuutta sekä sisäisten, että ulkoisten yhteyksien osalta. Tällaisia tutkimuksia löytyi yhteensä 14. Tutkimukset ovat taulukoituina tuoreimmasta vanhimpaan. Taulukkoon on koottu lisäksi kunkin tutkimuksen merkittävimmät vahvuudet ja heikkoudet.

Seuraavissa aliluvuissa esitellään taulukoitujen tutkimusten sisältöä, alkaen tuoreimmista tutkimuksista ja päätyen 2010-luvun alkupuoliskon tutkimuksiin. Lisäksi reflektoidaan tätä työtä löydettyihin aiempiin tutkimuksiin.

Taulukko 2. *Kirjallisuuskartoitukset taulukoituna.*

Kirjoittajat	Otsikko	Vahvuudet	Heikkoudet
Dibaei *et al*. *(2019)*	*An overview of attacks and defences on intelligent connected vehicles*	•Vastaavat tutkimusmenetelmät •Ajantasainen	•Paino olemassa olevilla suojausmekanismeilla
Kennedy *et al.* *(2019)*	*Automotive cybersecurity: Assessing a new platform for cybercrime and malicious hacking*	•Ajantasainen	•Paino valmistajien vastuulla •Tutkimusmenetelmiä ei käsitellä
Sommer *et al.* *(2019)*	*Survey and classification of automotive security attacks*	•Hyökkäyksiä käsitellään laajasti •Ajantasainen	•Paino luokittelumallin kuvauksessa
Hu & Luo *(2018)*	*Review of secure communication approaches for in-vehicle network*	•Esittelee 4 puutetta ajoneuvojen sisäisessä kommunikaatiossa	•Eri ajoneuvotyyppejä ei käsitellä
Jadhav & Kshirsagar *(2018)*	*A survey on security in automotive networks*	•Ytimekäs kuvaus käytetyistä protokollista ja turvallisuusongelmista	•VANETia ei käsitellä •Eri ajoneuvoyyppejä ei käsitellä
Jadoon *et al.* *(2018)*	*Lightweight cryptographic techniques for automotive cybersecurity*	•VANETia kuvattu laajasti •Sisäisiä yhteyksiä käsitellään	•Eri ajoneuvotyyppejä ei käsitellä •Paino salaustekniikoissa
Le *et al. (2018)*	*Security and privacy for innovative automotive applications: A survey*	•Laaja kartoitus uhista •Sisäiset ja ulkoiset yhteydet kuvataan	•Sähköajoneuvoja ei käsitellä
Tervo (2018)	*Ajoneuvoteknisten järjestelmien tietoturvallisuusselvitys*	•Suomenkielinen •Kerroksittainen suojaus •Samankaltainen tutkimusmenetelmä	•Raskasta kalustoa ei käsitellä
Bertolino *et al.* *(2017)*	*A tour of secure software engineering solutions for connected vehicles*	•Motiiveja hyökkäyksille	•Eri ajoneuvotyyppejä ei käsitellä •Paino turvallisissa ohjelmistoratkaisuissa
Zou *et al. (2017)*	*Research on information security framework of intelligent connected vehicle*	•Kyberhyökkäysten kategoriointi	•Kartoituksena suppea
Much (2016)	*Automotive security: Challenges, standards, and solutions*	•Uusien ominaisuuksien haasteet •Kerroksittainen suojaus	•Ajoneuvojen tietoteknistä rakennetta ei kuvata •Sähköajoneuvoja ja raskasta kalustoa ei käsitellä •Paino standardeissa
Saed *et al.* *(2014)*	*Security concepts and issues in intra-inter vehicle communication network*	•Tahattomat "hyökkäykset"	•Kartoituksena suppea •Sähkö- ja autonomisia ajoneuvoja ei käsitellä
Kleberger *(2012)*	*A structured approach to securing the connected car*	•Ajoneuvon ja huoltoliikkeen kommunikoinnin riskit	•Hyökkäyksiä käsitellään lähinnä sisäisien yhteyksien osalta •Verrattain vanha - moni asia muuttunut
Onishi *(2012)*	*Paradigm change of vehicle cyber security*	•Analysoi kyberuhkia ja tarjoaa ratkaisumalleja	•Verrattain vanha - moni asia muuttunut

3.1.1 Tutkimukset 2019

Tutkimuksessaan [21] Dibaei *et al*. esittelivät kattavasti uusimman teknologian ajoneuvojen tietoteknisen rakenteen, niihin kohdistuvia tietoturvauhkia ja mahdollisia ratkaisuja suojautumiseen. Dibaei *et al.* nostavat keskiöön tiedonsiirron ja etenkin langattoman viestinnän uhat ajoneuvoympäristössä. Pääpaino tutkimuksella on kuitenkin olemassa olevissa suojausmekanismeissa ja parannusten etsimisessä tulevaisuuden varalle. Tutkimusmenetelmältään Dibaei *et al*. tutkimus vastaa tätä tutkimusta. Käytetyt hakusanat ovat osittain poikkeavia erilaisen painotuksen takia. VANETia, sähkö- ja autonomisia ajoneuvoja sekä niiden tuomia haasteita turvallisuudelle käsitellään työssä. Raskasta kalustoa ei erikseen nosteta esiin, mutta suojautumismekanismit ovat monin paikoin yhteneviä henkilöautojen kanssa.

Vuodelta 2019 osuvia tutkimuksia löytyi edellä mainitun Dibaei *et al.* tutkimuksen lisäksi kaksi. Sommer *et al*. luokittelevat työssään [22] ajoneuvoihin kohdistuneita hyökkäyksiä tarkoitukseen kehittämänsä luokittelujärjestelmän mukaan. Kennedy *et al.* [23] puolestaan lähestyvät ajoneuvojen kyberturvallisuutta ajoneuvo- ja osavalmistajien vastuun näkökulmasta. Siinä missä Sommer *et al*. kuvaavat kattavasti hyökkäyksiä, Kennedy *et al*. painottavat enemmän vastuukysymyksiä.

Sommer *et al*. [22] toteavat aiempien kyberuhkaluokitusten olevan epäsopivia ajoneuvojen uhkien luokitteluun. Tästä syystä tutkimuksessa esitetään ajoneuvoille sopiva luokittelumalli, jota voidaan hyödyntää tulevien hyökkäysten tunnistamiseen. Vaikka työn ensisijaisena tarkoituksena on luoda luokittelumalli, työssä kuvataan luokittelumallin mukaisesti 162 tunnettua hyökkäystä. Sommer *et al*. tutkimus on päämärältään erilainen kuin tämä tutkimus, mutta työn seikkaperäisyyden vuoksi hyökkäyksiä käsitellään laajasti. Tutkimuksen luonteen takia sähköajoneuvoja tai raskasta kalustoa ei kuitenkaan käsitellä erikseen.

Kennedy *et al*. pohtivat [23] myös sitä, miksi todellisia pahantahtoisia hyökkäyksiä ei vielä ole raportoitu. Kaikki raportoidut hyökkäykset ovat olleet tutkijoiden tekemiä ja niiden tarkoituksena on ollut tuoda esiin haavoittuvuuksia. Yksittäistä syytä tälle ei anneta, mutta tutkijat pitävät mahdollisena, että merkittäviin hyökkäyksiin kykenevien hakkereiden määrä on vielä riittämätön. Toinen mahdollinen selitys on se, että samankaltaisia verkottuneita ajoneuvoja on liikenteessä toistaiseksi vielä niin pieni määrä, ettei niitä ole koettu kannattavaksi kohteeksi. Työssä käsitellään yleisemmin tietojärjestelmien kohtaamia kyberuhkia ja suhteutetaan niitä ajoneuvojen ympäristöön. Lisäksi puhtaasti ajoneuvojen kyberturvallisuuden sijaan työssä painotetaan erityisesti valmistajien vastuuta turvallisuuden parantamisessa.

3.1.2 Tutkimukset 2018

Vuonna 2018 julkaistuja, ajoneuvojen kyberturvallisuutta kokonaisuutena tarkastelevia, tutkimuksia löytyi viisi. Näihin lukeutuu yksi suomenkielinen tutkimus [15]. Laajassa kirjallisuuskartoituksessaan Le *et al.* [24] kuvaavat ajoneuvon tietoteknisen järjestelmäarkkitehtuurin ja esittelevät haavoittuvuuksien lisäksi hyökkääjien kykyjä sekä hyökkäysten mahdollisia vaikutuksia. Hu ja Luo [25] tarjoavat koosteen tutkimuksista, jotka käsittelevät tämän hetken turvallisia kommunikointimenetelmiä ja listaavat turvallisuusvaatimuksia, jotka tulisi huomioida uusia ominaisuuksia lisättäessä. Jadoon *et al.* [26] puolestaan tarkastelevat olemassa olevia salausratkaisuja ja esittelevät ohessa useita kyberhyökkäyksiä. [27] taas nostavat esiin merkittävimpien tietoturvaperiaatteiden noudattamisen tärkeyden kaikkein osavalmistajien kohdalla.

Tervo [15] nostaa työssään esiin havainnon, että ajoneuvovalmistajat luottavat tietoturvan kohdalla fyysiseen suojaukseen. Tutkimuksessa tuodaan esiin myös tämän ajattelumallin heikkous. Ajoneuvon rakenteen antama suoja ei toimi, mikäli esimerkiksi alihankkijan toimittamassa järjestelmässä on haavoittuvuus, joka avaa pääsyn ajoneuvon väyliin. Toisena merkittävänä uhkana Tervo nostaa langattomien järjestelmien haavoittuvuudet, jotka mahdollistavat hyökkäykset etäyhteydellä. Ratkaisuksi näihin ongelmiin työssä esitetään standardointia sekä suojausjärjestelmiä ajoneuvon tietoteknisiin rakenteisiin. Tutkimusmenetelmää ei ole kuvattu tarkasti, mutta pääpiirteet menetelmässä ovat samat kuin tässä työssä; kirjallisuushakuja tietokannoista ja internetistä. Autonomisia ajoneuvoja käsitellään työssä eri uhkaskenaarioiden yhteydessä. Sähköajoneuvot ja kyydinjakamispalvelut jäävät selvästi pienemmälle huomiolle. Raskasta kalustoa ei työssä käsitellä lainkaan.

Le *et al*. [24] tutkimus on laaja kartoitus turvallisuuden ja yksityisyyden haasteista ajoneuvojen käyttämissä sovelluksissa ja niiden alustoissa. Tutkimuksessa kuvataan ajoneuvojen tietotekninen arkkitehtuuri ja ulkoiset yhteydet. Riskianalyysissä käsitellään hyökkääjien kykyjä, haavoittuvuuksia ja hyökkäyksiä niin ajoneuvojen sisäisissä väylissä kuin ulkoisissa yhteyksissä, kuten VANETissa. Tutkimuksesta tuodaan esiin, että potentiaalisia hyökkääjiä on laajasti erilaisilla taidoilla ja motiiveilla. Myös raskaiden ajoneuvojen kaluston hallintaa käsitellään mahdollisena haavoittuvuuskohtana. Näiden lisäksi tutkimuksessa kartoitetaan olemassa olevia suojausmekanismeja kyberhyökkäyksiä vastaan.

Hun ja Luon [25] työ on kirjallisuuskartoitus ajoneuvojen turvallisiin kommunikointimenetelmiin. Lisäksi ajoneuvojen tietotekninen rakenne on kuvattu. Tutkijat nostavat esiin neljä merkittävintä puutetta ajoneuvojen sisäisessä viestinvälityksessä. Ne ovat 1) au-

tentikoinnin puute, 2) broadcast jakelu, 3) pakettien tärkeysjärjestyksen määrittely tunnisteen mukaan ja 4) aikaleimojen puuttuminen. Lisäksi käsitellään turvallisia kommunikointitapoja ja niiden teknisiä vaatimuksia. Näiden perusteella ehdotetaan myös mahdollisia ratkaisuja tulevaisuudessa. Koska aihetta lähestytään enemmän turvallisen kommunikaation näkökulmasta, kuin haavoittuvuuksia etsien, erilaisia ajoneuvotyyppejä ei käsitellä erikseen. Autonomiset ajoneuvot ja niitä koskevat uhat on mainittu.

Jadoon *et al*. [26] lähestyvät ajoneuvojen kyberturvallisuutta salaustekniikoiden näkökulmasta. Perinteisessä verkossa käytetyt salaustekniikat ovat liian hitaita ja kankeita ajoneuvojen vaatimuksille, siksi ajoneuvojen käyttöön tarvitaan kevennettyjä salausratkaisuja. Erityisesti esittelyssä on VANETin ominaisuudet, mutta kirjallisuudesta löytyneitä haavoittuvuuksia käsiteltäessä myös ajoneuvon sisäiset kommunikointiväylät tulevat käsitellyksi. Samoin salaustekniikat koskevat myös sisäisiä väyliä, vaikka tutkimuksessa painotetaan erityisesti VANETin mukana tulevia turvallisuusuhkia. Autonomisia ajoneuvoja, sähköajoneuvoja tai raskasta kalustoa ei käsitellä.

Jadhav ja Kshirsagar [27] tarjoavat katsauksen ajoneuvojen sisäisiin ja ulkoisiin kommunikointiprotokolliin sekä yleiskuvan käytetyistä standardeista ja ajoneuvojen verkkojen turvallisuusongelmista. Tutkimus on lyhyt ja ytimekäs kuvaus käytetyistä protokollista, mahdollisista hyökkäystavoista ja suojautumiskeinoista. Työn painotus on ohjausyksiköissä ja protokollissa. Ajoneuvotyyppejä ei ole eritelty vaan aihetta käsitellään yhteisten ongelmien osalta. Infotainment ja Bluetooth mainitaan vain osana ohjausyksiköiden käyttötapoja, eikä älylaitteiden liittämisen turvallisuusriskejä nosteta sellaisenaan esiin. Ongelmia käsitellään vain väylien turvallisuuden osalta. Lisäksi VANET jää käsittelyn ulkopuolelle.

3.1.3 Tutkimukset 2016-2017

Vuodelta 2017 on Zou *et al*. julkaisu [28], joka kuvailee älykkäiden ajoneuvojen tietoteknisiä piirteitä ja esittelee niiden tietoturvaan keskittyviä tutkimuksia. Samalta vuodelta on Bertolino *et al*. artikkeli [29], joka koostaa ajoneuvojen kommunikointiin liittyvät merkittävimmät turvallisuusuhat ja käsittelee myös hyökkäyksien mahdollisia motiiveja. Much [30] on julkaissut vuonna 2016 artikkelinsa[30], jossa aihetta lähestytään ajoneuvovalmistajien kohtaamien turvallisuushaasteiden kautta.

Zou *et al*. [28] esitelevät verkottuneen ajoneuvon teknologiaa sekä Yhdysvaltojen, Kiinan, Japanin ja Euroopan viranomaisten kyberturvallisuustutkimuksen tilannetta. Lisäksi työssä on kuvattu ajoneuvoihin kohdistuvien kyberhyökkäysten viitekehys, jossa hyökkäykset on jaettu kolmeen kategoriaan. Ensimmäiseen kategoriaan kuuluvat hyökkäyk-

set, jotka vaativat fyysisen pääsyn ajoneuvon rajapintoihin, kuten OBD-väylään. Seuraavaan kategoriaan menevät lyhyen kantaman hyökkäykset, jotka eivät vaadi fyysistä pääsyä, mutta etäisyys on rajallinen. Tällaisia ovat esimerkiksi Bluetoothin avulla toteutettavat hyökkäykset. Viimeisessä kategoriassa ovat pitkän kantaman hyökkäykset, joita voidaan toteuttaa internet-yhteyden välityksellä kuinka etäältä tahansa. Kirjallisuuskartoituksena työ on suppea, alle kymmenellä lähteellä. Lähestymiskulma on kuitenkin mielenkiintoinen ja muista vastaavista poikkeava, sillä aihetta tutkitaan nimenomaan viranomaisten tekemän tutkimuksen kautta.

Bertolino *et al*. [29] käsittelevät ajoneuvojen kommunikaation turvallisuusuhkia. Tutkimuksessa käsitellään löydöksiä aiemmasta kirjallisuudesta ja sen lisäksi esitellään standardeja, joiden tarkoitus on tukea turvallisuutta. Työssä esitellään myös olemassa olevia tekniikoita ja työkaluja suunnittelulähtöiselle turvallisuudelle ja tuodaan esiin niiden ongelmia ajoneuvoissa. Lisäksi luetellaan mahdollisia motiiveja hyökkäyksille, kuten terrorismi, kokeilevat hakkerit ja omista kokeiluista aiheutuvat vikatilanteet. Työn päätarkoitus on esitellä turvallisia ohjelmistoratkaisuja ajoneuvojen kommunikaatioon ja näin ollen painotus on ratkaisuilla. Kirjallisuudesta löytyneitä haavoittuvuuksia käytetään lähinnä työn motivaation esittelyyn. Tästä syystä haavoittuvat kohteet esitellään vain pintapuolisesti. Sähköajoneuvoja, raskasta kalustoa tai autonomisia ajoneuvoja ei käsitellä erikseen. Autonomisista ajoneuvoista mainitaan useiden tutkimusten käsittelevän niiden riskiä joutua kyberhyökkäyksen kohteeksi.

Much [30] esittelee ajoneuvovalmistajien kohtaamia turvallisuusongelmia ja ratkaisuja niihin. Tutkimuksessa nostetaan esiin uusien ominaisuuksien taipumus tuoda mukanaan uusia hyökkäyspintoja. Tärkeimmäksi ratkaisumalliksi tarjotaan kerroksittaista suojautumista, jossa eri kerrokset vastaavat suojautumisesta itselleen parhaalla tavalla. Jokainen kerros täydentää edeltävää suojausta. Työssä huomautetaan, että verkottuneen autonomisilla ominaisuuksilla varustetun ajoneuvon suunnittelussa ei voida keskittyä pelkästään turvallisuuteen, vaan myös saatavuus, luotettavuus, luottamuksellisuus, eheys ja ylläpidettävyys on turvattava. Tähän tulisi pyrkiä, vaikka välillä nämä ominaisuudet ovat ristiriidassa keskenään. Ajoneuvojen tietoteknistä rakennetta tai älylaitteiden tuomia haasteita ei tutkimuksessa kuvata. Tutkimuksessa painotetaan olemassa olevia standardeja ja kuvaillaan löydettyjä hyökkäyspintoja. Aiemmissa tutkimuksissa löytyneistä haavoittuvuuksista nostetaan esimerkkeinä muutamia esiin. Sähköajoneuvoja tai raskasta kalustoa ei tutkimuksessa käsitellä.

3.1.4 Tutkimukset 2010-luvun alusta

Aiemmat, 2010-luvun alkupuolen julkaisut, painottuivat enimmäkseen ajoneuvon sisäisiin verkkoihin. Kokonaisuutta laajasti tarkastelevia julkaisuja löytyi kolme. Saed *et al*. [31] esittelevät ajoneuvojen viestinnän uhkia ja mahdollisia suojautumistoimia. Onishi [32] arvioi älykkäiden ajoneuvojen mukanaan tuomia riskejä ja analysoi aiheutuneita ongelmia. Kleberger [33] esittelee turvallisuusmekanismeja verkottuneille ajoneuvoille.

Saed *et al*. [31] kartoittavat haavoittuvuuksia, joita on aiemmin yritetty hyödyntää. Sekä ajoneuvon sisäisiä väyliä, että ulkoisia yhteyksiä käsitellään. Lisäksi esitellään keinoja suojautua hyökkäyksiltä jatkossa. Todennäköisenä skenaariona hakkeroinnille pidetään telematiikan tai langattomien viestintäkanavien hyödyntämistä. Ongelmana esiin nostetaan myös taipumus tuotteita suunniteltaessa huomioida vain hyvien ihmisten riski tehdä jotakin vahingossa väärin. Tältä suojautuminen ei kuitenkaan riitä suojautumaan hakkereilta, jotka etsivät heikkouksia. Suojautumiseksi tarjotaan esimerkiksi viestin osapuolten autentikoimista ja haavoittuvuuksien tunnistamista. Kirjallisuuskartoituksena tutkimus on suppea, sillä käytettyjä lähteitä on alle 20. Sähkö- ja autonomisia ajoneuvoja ei tutkimuksessa käsitellä. Samoin ulkopuolelle on jätetty raskaat ajoneuvot. VANETia ei tutkimuksessa ole nimetty, mutta saman kaltaista ajoneuvojen välistä kommunikaatiota käsitellään.

Onishi [32] arvioi älykkäiden ajoneuvojen kyberturvallisuusuhkia riskinarviointityökalun avulla. Kirjoittaja myös analysoi aiheutuneita ongelmia ja tarjoaa ratkaisumalleja. Ongelmia haittaohjelmien torjumisessa, verrattuna tietokoneisiin, tuottaa ohjelmistopäivitysten hitaus ja ajoneuvojen pitkä käyttöikä. Lisäksi ongelmaksi on nostettu ajoneuvojen tietojärjestelmien laskentatehon heikkous verrattuna hakkereiden tietokoneisiin. Kolmanneksi on esitetty sertifikaattien varmistamisen vaikeutta, sillä ajoneuvot eivät ole jatkuvasti yhteydessä internetiin. Tutkimus on vuodelta 2012, joten tämä ongelma on jo osittain vanhentunut ja tulee poistumaan autokannan uusiutuessa ja infrastruktuurin kehittyessä. Tutkimuksessa on käsitelty mobiililaitteiden liittämisestä aiheutuvaa riskiä. Suojautumiskeinoksi on ehdotettu esimerkiksi viihdepalveluiden erottamista turvallisuuskriittisistä toiminnoista. Tämä on moderneissa ajoneuvoissa jo käytössä niiltä osin kuin mahdollista.

Klebergerin tutkimus [33] on jaettu kahteen osaan. Molemmat osat koostuvat kahdesta julkaisusta. Ensimmäinen osa kuvaa verkottuneen ajoneuvon sisäistä rakennetta. Tämän osan ensimmäisessä julkaisussa [34] tarkastellaan ajoneuvojen sisäisiä verkkoja turvallisuuden näkökulmasta. Toinen julkaisu [35] määrittelee turvallisuuden asemaa verkottuneissa ajoneuvoissa. Työn toisessa osassa tutkittiin ajoneuvon ja huoltoliikkeen

välisen kommunikaation riskejä. Toisen osan ensimmäinen julkaisu [36] analysoi huoltoliikkeiden kybertuvallisuutta verkottuneiden ajoneuvojen palvelussa. Välittömimmäksi uhaksi havaittiin autentikoinnin puuttuminen kommunikaatiossa. Viimeisessä julkaisussa [37] käsitellään ajoneuvojen suojaamista luvattomalta etädiagnosoinnilta. Työn ensisijaisena tarkoituksena on etsiä ratkaisuja tekemään ajoneuvojen kommunikoinnista turvallisempaa. Kartoitus haavoittuvuuksista keskittyy enimmäkseen ajoneuvojen sisäisiin verkkoihin. Työ on vuodelta 2012, joten moni asia on jo ehtinyt muuttua julkaisun jälkeen.

3.1.5 Yhtäläisyydet ja erot

Yhtä lukuun ottamatta kaikki käsitellyt kirjallisuuskartoitukset kuvaavat tutkimusmenetelmää vain mainitsemalla aiempaan tutkimukseen kohdistuneesta kartoituksesta. Näiden kohdalla tutkimusmenetelmien yhtäläisyyksiä on vaikea arvioida syvällisesti. Dibaei *et al*. [21] kuvaavat työssään myös tutkimusmenetelmän, joka on hyvin lähellä tämän työn menetelmää.

Raskas kalusto ja sähköajoneuvot jäävät pienelle huomiolle kaikissa tutkimuksissa, jos niitä ylipäätään mainitaan. Autonomisia ajoneuvoja ja VANETia, vähintään niiden osia, käsitellään jo selvästi useammin. Älylaitteet ovat osana uhkakuvaa, etenkin uudemmissa julkaisuissa, mutta pääosin vain matkapuhelinten osalta. Matkapuhelimen ja infotainment-paneelin yhdistämisen mahdollistavia sovelluksia ja niiden uhkia ei käsitellä missään löydetyistä tutkimuksista. Lisäksi ajoneuvojen koodaaminen ja siitä aiheutuvat uhat on jätetty tutkimuksissa ulkopuolelle. Itsediagnosointia ja OBD-väylää itsessään kuitenkin käsitellään haavoittuvana kohteena. Ratkaisut turvallisuuden parantamiselle ovat lähes kaikilla saman suuntaisia. Selkeästi eniten nostetaan esiin tarvetta salaukselle ja autentikoinnille. Toinen usein esitetty keino on kerroksittainen suojaus. Teknisiä ratkaisumalleja käsitellään kaikissa mainituissa tutkimuksissa, mutta ajoneuvon käyttäjän roolia turvallisuuden parantamisessa ei juuri huomioida.

Taulukkoon 3 on koottu aihepiireittäin tutkimusmenetelmään ja itse tutkimuksen sisältöön liittyviä ominaisuuksia sekä arvioitu näitä, asteikolla nollasta viiteen, kunkin kirjallisuuskartoituksen osalta. Tutkimuksen tekemiseen liittyvissä asioissa vertailukohtana on vastaavuus tämän työn kanssa. Asiasisältöä on arvioitu niin ikään suhteessa tähän tutkimukseen, mutta lähtökohtana käsittelyn laajuus, joka joidenkin asioiden kohdalta on laajempaa kuin tässä työssä ja toisten kohdalla taas suppeampaa. Taulukossa esitetyt arvosanat eivät kuvaa tutkimusten laatua, ainoastaan sitä miten käytetyt menetelmät ja tutkitut asiat vastaavat tämän tutkimuksen menetelmiä ja päämääriä.

Tutkimuksen toteutusosien kohdalta arvosana viisi tarkoittaa menetelmien, hakusanojen ja ajantasaisuuden olevan hyvin lähellä tätä tutkimusta. Arvosana nolla vastaavasti tarkoittaa, että tutkimus eroaa tästä tutkimuksesta merkittävästi tai menetelmiä ja hakusanoja ei ole esitelty. Käsiteltyjen aiheiden kohdalla arviointtiperusteena käytettiin käsittelyn laajuutta. Tämän tutkimuksen, jota peilataan aiempiin tutkimuksiin, osalta arviot määrittyivät niin, että arvosanan viisi saivat tässä työssä painotetut asiakokonaisuudet. Asiat, joita painotettiin vähemmän, saivat pienempiä arvosanoja. Aiempia tutkimuksia verrattiin tähän työhön niin, että täydet viisi pistettä sai tämän työn tarkimman käsittelyn laajuisesta tai sen ylittävästä tarkastelusta. Näin ollen taulukosta ei voi tarkkaan päätellä kuinka laajasti asiaa on käsitelty. Asioita, joita tämä tutkimus ei käsittele, ei ole listattu taulukossa. Taulukon tarkoituksena on verrata tämän ja aiempien tutkimusten vastaavuutta, ei arvioida niiden laatua.

Arviot perustuvat aiempiin muistiinpanoihin, jotka on tehty tutkimuksia luettaessa. Tämän lisäksi tutkimuksista etsittiin haulla asiasanoja kattamaan kohdat, joita ei muistiinpanoissa ollut käsitelty. Taulukon 3 loppuun on laskettu keskiarvo kunkin tutkimuksen kattavuudesta. Keskiarvosta on nähtävissä, että juuri samoja asioita tämän tutkimuksen kanssa ei aiemmissa tutkimuksissa ole painotettu.

Taulukko 3. *Kirjallisuuskartoitukset pisteytettynä. Tutkimuksen tekemiseen liittyvissä kohdissa vertailukohtana tämä tutkimus. Asiasisällön osalta arviointi käsittelyn laajuuden mukaan, suhteutettuna tähän tutkimukseen. *Tämä tutkimus.*

	Rikkonen (2020)*	Le et al. (2018)	Dibaei et al. (2019)	Tervo (2018)	Bertolino et al. (2017)	Hu & Luo (2018)	Sommer et al. (2019)	Jadhav & Kshirsagar (2018)	Kleberger (2012)	Onishi (2012)	Kennedy et al. (2019)	Jadoon et al. (2018)	Much (2016)	Saed et al. (2014)	Zou et al. (2017)
Kirjallisuuskartoituksen laajuus	5	5	5	2	3	5	5	2	5	2	3	5	3	1	1
Ajantasaisuus	5	5	5	5	4	5	5	5	1	1	5	5	3	2	4
Hakusanat	5	0	3	0	0	0	0	0	0	0	0	0	0	0	0
Tutkimusmenetelmä	5	1	5	2	1	1	1	1	1	1	1	1	1	1	1
Yhtenevä painotus	5	4	2	4	2	3	2	2	3	4	2	2	2	3	2
CIA	5	5	5	5	5	5	5	5	5	0	0	5	5	0	0
Sähkö- ja autonomisia ajoneuvoja	4	3	4	3	0	1	2	0	0	0	3	0	0	0	0
Raskas kalusto	5	3	0	0	0	0	0	0	0	0	0	0	0	0	0
Haavoittuvuudet	5	5	5	4	2	3	5	4	4	5	2	5	3	5	3
Hyökkäykset	5	5	5	4	4	3	5	4	3	5	3	4	3	5	3
Hyökkäyksen vaikutus/motiivi	5	5	3	3	5	0	5	1	3	2	2	0	0	0	0
Haittaohjelmat	5	2	5	5	2	2	2	2	1	5	4	2	0	1	0
Vahingot	2	0	0	5	4	0	0	0	0	0	1	0	0	5	0
Tietotekninen rakenne	5	5	5	5	2	5	1	3	5	1	1	0	0	1	1
Väylät	4	5	5	5	2	5	1	4	4	1	1	0	1	2	2
Ohjausyksiköt	5	5	5	5	3	5	2	5	4	1	2	0	2	2	2
Standardit	4	5	5	5	5	4	3	4	0	2	3	1	5	0	0
Sisäiset yhteydet	5	5	5	5	5	3	3	4	5	3	3	3	4	5	5
Ulkoiset yhteydet	5	5	4	4	5	3	3	4	2	3	2	4	4	4	5
VANET	5	5	4	0	5	0	0	0	2	1	0	5	0	0	0
Infotainment	5	4	5	0	1	2	1	1	0	2	1	0	0	0	0
Bluetooth	5	5	2	1	2	0	5	1	0	4	0	0	0	1	5
Älylaitteet	5	5	4	2	1	2	3	1	3	4	3	1	0	0	2
Itsediagnosointi	5	3	4	1	0	0	3	0	0	2	1	0	0	1	0
DIY koodaaminen	5	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Ratkaisut	4	5	5	5	5	5	3	5	5	5	4	4	5	5	3
Salausratkaisut	2	5	5	4	3	5	1	3	3	4	0	5	4	0	0
Suojausmekanismit	4	5	5	5	4	5	3	5	5	5	4	3	5	5	3
Ajoneuvon käyttäjän rooli	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Keskiarvo	**5**	**4**	**4**	**3**	**3**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**1**

3.2 Rajatun aihealueen kirjallisuuskartoitukset ja alkuperäisartikkelit

Rajatuista tutkimuskohteista ja -tavoista huolimatta muutamat julkaisut ansaitsevat tulla mainituksi. Alla luetellut työt lähestyvät aihetta eri tavoin kuin tässä työssä, mutta ovat sisällöltään kiinnostavia.

Tutkimuksissaan [38-42] Avatefipour ja Malik, Bozdal *et al*., Oyler ja Saiedian, Ring *et al*. ja Zhong *et al*. keskittyvät CAN-väylän turvallisuuteen. Kaikki mainitut tutkimukset käsittelevät laajasti CAN-väylän haavoittuvuuksia ja esittelevät kirjallisuudesta löytyneitä ratkaisuja, kuten salausta ja tunkeutumisenestojärjestelmiä. Kirjallisuustutkimuksen lisäksi Ring *et al.* [41] tekivät myös omaa tutkimusta CAN-väylään.

Laajemmin ajoneuvon sisäisien väylien turvallisuutta käsittelee Zeng *et al*. [43]. Lisäksi tutkijat esittävät vastatoimiksi uhille salausta ja autentikointia. Ajoneuvon sisäiseen verkkoon ovat keskittyneet kirjallisuustutkimuksissaan [44,45] myös Chockalingam ja Lallie sekä Studnia *et al.*, mutta ulkoisiakin yhteyksiä sivutaan.

Kokeellisia tutkimuksia Millerin ja Valasekin [20] työn lisäksi löytyi kolme. Yan kuvaa julkaisussaan [46] tutkimusta, joka toteutettiin kahden vuoden ajanjaksolla, vuosina 2014 ja 2015. Tutkimuksessa käytettiin yli 80 tarkastuspistettä haavoittuvuuksien havaitsemiseksi. Hoppe *et al*. [47] puolestaan testasivat erilaisia hyökkäyksiä CAN-väylään. Tutkijat esittävät työssään myös mahdollisia torjuntakeinoja. Koscher *et al*. [48] tutkivat vuosimallin 2009 ajoneuvojen kyberturvallisuusongelmia sekä laboratorio-olosuhteissa, että tien päällä. Lisäksi he demonstroivat järjestelmien heikkouksia.

4. KESKEISET KÄSITTEET JA HYÖKKÄYSTAVAT

Tässä luvussa esitellään tutkimuksen kannalta keskeisimmät käsitteet. Lisäksi kuvataan hyökkäysmekanismeja, joita voidaan hyödyntää ajoneuvojen tietojärjestelmiä vastaan.

Hyökkäykset tarkoittavat tämän työn kontekstissa ajoneuvon tietotekniikkaan kohdistuvia luvattomia toimia, joilla pyritään vaikuttamaan ajoneuvon toimintaan, mahdollistamaan myöhempi vaikuttaminen tai saamaan haltuun tietoja. Hyökkääjällä puolestaan tarkoitetaan hyökkäyksen toteuttajaa. Periaatteessa mainittuja luvattomia toimia on mahdollista aiheuttaa tahattomasti, mutta puhuttaessa hyökkäyksestä tai hyökkääjästä viitataan tässä työssä kuitenkin tahallisiin toimiin.

Kyberuhilla tarkoitetaan digitaalisesta tietojärjestelmästä muodostuvaan toimintaympäristöön kohdistuvia, mahdollisesti toteutuvia, haitallisia tapahtumia. Kyberuhat voivat toteutuneiden tietoturvauhkien lisäksi aiheutua myös turvallisuutta vaarantavista teoista digitaalisessa viestintäympäristössä. [49]

4.1 Luottamuksellisuus – Eheys – Saatavuus

Ajoneuvoihin, kuten muihinkin tietoteknisiin kokonaisuuksiin, voidaan kohdistaa useita erilaisia hyökkäyksiä riippuen halutusta vaikutuksesta. Yleisin tapa jaotella uhat on jakaa ne kolmeen eri luokkaan sen mukaan, mihin tietoturvan osa-alueeseen uhka kohdistuu. Tästä jaottelusta käytetään nimitystä CIA-triadi, joka tulee englannin kielen sanoista luottamuksellisuus (engl. confidentiality), eheys (engl. integrity) ja saatavuus (engl. availability). [50]

Luottamuksellisuudella tarkoitetaan sitä, että tieto on vain sen käyttöön oikeutettujen saatavilla, eikä tietoa paljasteta muille. Tiedon eheys kuvaa sitä, ettei tietoa ole muutettu luvatta tai vahingossa ja kaikki muutokset voidaan todentaa. Saatavuus puolestaan ilmentää tiedon hyödynnettävyyttä halutulla tavalla ja haluttuna ajankohtana. [49]

Luottamuksellisuutta vastaan kohdistetussa hyökkäyksessä pyritään saamaan selville tietoa, joka ei ole tarkoitettu ulkopuolisille. Tätä tietoa voidaan joko hyödyntää sellaisenaan, esimerkiksi haluttaessa selvittää, missä jokin tietty ajoneuvo on matkalla tai hyödyntää sitä jatkohyökkäyksessä. Eheydellä taas viitataan tiedon muuttumattomuuteen, tarkemmin sanottuna siihen, ettei mikään luvaton taho muuta tietoa. Yksinkertaisena esimerkkinä auton datan eheyteen kohdistuvana hyökkäyksenä voidaan pitää tilannetta, jossa hyökkääjä omalta päätelaitteeltaan tunkeutuu auton verkkoon ja syöttämällä omaa

dataansa, esimerkiksi nostaa autoradion äänen voimakkuutta. Saatavuuteen kohdistuvalla hyökkäyksellä pyritään estämään jonkin palvelun käyttö tai tiedon saanti ja tällä tavoin aiheuttamaan toiselle haittaa. Esimerkiksi auton käynnistymisen estäminen loukkaa saatavuutta.

Identiteetin väärennyksellä (engl. spoofing identity) tarkoitetaan esiintymistä oikeutettuna käyttäjänä ja sillä tähdätään aiheuttamaan haittaa järjestelmään. Tietojen peukaloinnilla (engl. tampering with data) tarkoitetaan tiedon oikeudetonta muuttamista ja pyrkimyksenä on vaikuttaa tuleviin toimintoihin. Samaan pyritään myös käyttöoikeuksien korottamisella (engl. elevation of priviledge), jossa siis haavoittuvuutta hyödyntämällä hankitaan korkeammat käyttöoikeudet, kuin käyttäjälle on tarkoitettu [51]. [50]

Identiteetin väärennyksellä, peukaloinnilla ja käyttöoikeuksien korottamisella voidaan vaikuttaa tiedon eheyteen, mutta pyrkimyksenä saattaa olla myös luottamuksellisuuden rikkominen, johon pyritään myös tietojen paljastamisella (engl. information disclosure). Tiedon paljastamisella tarkoitetaan tiedon saattamista luvattomasti ulkopuolisten haltuun. Urkinnalla (engl. phishing) pyritään samankaltaiseen lopputulokseen, mutta terminä urkinta viittaa enemmän siihen, että hyökkääjä hankkii itselleen pääsyn tietoon. Palvelunestolla (DoS, engl. Denial of Service) pyritään heikentämään saatavuutta epäämällä käyttöoikeudet tai estämällä suoraan palvelun toiminta. [50]

Kaikkia näitä hyökkäystyyppejä voidaan kohdistaa ajoneuvoon. Luottamukselliseksi tarkoitettua tietoa järjestelmästä urkkimalla voidaan saada jo tarvittava hyöty, vaikka saatua tietoa ei käytettäisi enää uudelleen ajoneuvoon kohdistuvaan hyökkäykseen. Esimerkiksi kiinnostavaa toimitusta, kuten arvotavaraa tai aseita, kuljettavan kuorma-auton paikkatieto yms. saattaa olla arvokasta dataa jo itsessään. Luvuissa 4.2, 4.3 ja 4.4 esitellään lyhyesti merkittävimpiä hyökkäystapoja, jotka soveltuvat ajoneuvojen luottamuksellisuuden, eheyden ja saatavuuden rikkomiseen.

4.2 Palvelunestohyökkäys

Palvelunestohyökkäys on yksi tunnetuimpia hyökkäystyyppejä. Palvelunestohyökkäys voidaan toteuttaa monin eri tavoin ja se pitää sisällään useita erilaisia hyökkäyksiä. Palvelunestohyökkäyksiä ovat kaikki hyökkäykset, joiden seurauksena palvelun käyttö estyy tai merkittävästi hidastuu. Hyökkäyksen pyrkimyksenä on rikkoa tiedon saatavuus oikeutetuilta käyttäjiltä. Palvelu voi estyä myös tahattomasti, jolloin teolla ei ole pyritty vaikuttamaan tiedon saatavuuteen, mutta vaikutukset ovat silti samat.

Yleisin tapa toteuttaa palvelunestohyökkäys, on tukkia palvelu toistuvilla pyynnöillä, jolloin palvelu ei pysty enää käsittelemään saamiaan pyyntöjä. Tämä hukuttamishyökkäys

(engl. flooding attack) perustuu kohdejärjestelmän ylikuormittamiseen. Kapasiteetin loppuessa, kohde ei pysty enää tuottamaan palvelua. Hyökkäyksen kohteena voi olla jokin ohjelma, käyttöjärjestelmä tai vain yksi komponentti. Vaihtoehtoisesti ylikuormitus voidaan suunnata jollekin kriittiselle resurssille, kuten reitittimelle tai verkkosivulle. Palvelunesto voidaan toteuttaa myös epäämällä käyttäjältä pääsy tarvitsemaansa resurssiin. [50]

Ajoneuvoon suunnattuna palvelunestohyökkäys voi johtaa mihin vain lievän kiusan ja hengenvaarallisen onnettomuuden välillä. Mikäli hyökkäys olisi suunnattu esimerkiksi ajoneuvon äänentoistojärjestelmään niin, että ääneen voimakkuuden säätäminen estyy, hengenvaaraa ei synny. Toisaalta jos hyökkäys kohdistetaan esimerkiksi jarruihin tai ohjaukseen, ovat hyökkäyksen vaikutukset huomattavasti dramaattisemmat. Adaptiiviseen vakionopeuden säätimeen kohdennettuna palvelunestohyökkäys aiheuttaa potentiaalisen vaaratilanteen, mutta kuljettajalla on mahdollisuus välttää onnettomuus reagoimalla itse tilanteeseen. Täysin autonomisen auton kohdalla samaa mahdollisuutta ei ole, koska kuljettajaa ei ole.

4.3 Välistävetohyökkäys

Välistävetohyökkäyksellä (MiTM, engl. Man in The Middle) tarkoitetaan salakuunteluun perustuvaa hyökkäystä. Hyökkääjä kierrättää, suoraan kahden pisteen välillä kulkevaksi tarkoitetun, viestiliikenteen itsensä kautta. Viestin alkuperäiset osapuolet luulevat kuitenkin edelleen kommunikoivansa suoraan toisilleen.

Hyökkääjä voi tarkoituksestaan riippuen joko vain salakuunnella dataliikennettä ja antaa datan jatkaa matkaa muuttumattomana alkuperäiseen määränpäähänsä tai muuttaa viestiä matkalla omiin tarkoituksiinsa sopivaksi. Eri variaatioiden takia MiTM-hyökkäys voi kohdistua kaikkiin CIA-triadin osiin.

4.4 Kiristyshaittaohjelma

Kiristyshaittaohjelma (engl. ransomware) on haittaohjelma, joka tyypillisesti salaa tiedot laitteella käyttäjän saamattomiin. Haittaohjelma vaatii maksua vastineeksi salauksen purkamisesta ja näin alkuperäisen datan vapauttamisesta.

Kiristyshaittaohjelmat ovat yleistyneet viime vuosina. Tämä johtunee siitä, että kiristyshaittaohjelma tuo suoran ansaintamahdollisuuden hyökkääjälle. Tämän kaltaisten hyökkäysten odotetaan tulevaisuudessa kohdistuvan myös ajoneuvoihin. San Franciscon metro ja bussiliikennettä palveleva tietojärjestelmä on jo joutunut tällaisen hyökkäyksen kohteeksi. Tämä hyökkäys toi ilmi kuljetusalan haavoittuvuuden kiristyshaittaohjelmille ja nosti kiinnostusta aiheeseen alalla. [52]

5. ÄLYKÄS AJONEUVO – HYÖDYLLINEN JA HAASTEELLINEN

Älykkäällä ajoneuvolla tarkoitetaan vähintään osittain ohjelmallisesti ohjattua ajoneuvoa, jolla on kyky kuljettajan avustamiseen ja jopa itsenäiseen ajamiseen. Älykäs ajoneuvo toimii osana älykästä liikennejärjestelmää (ITS, engl. Intelligent Transportation System) [53] tuoden positiivisia vaikutuksia liikenteen turvallisuuteen, taloudellisuuteen ja ympäristövaikutuksiin. [54]

Tulevaisuudessa ajoa avustavien järjestelmien on teoriassa mahdollista poistaa kolarit liikenteestä lähes kokonaan. Tämä koskee erityisesti ihmisten tekemistä virheistä aiheutuvia kolareita. Ajoneuvoihin yhdistettynä kyberturvallisuus näyttelee vielä suuremman roolin. Kaikki ajoneuvon turvallisuuteen vaikuttavat ominaisuudet pitäisi voida suojata kyberhyökkäyksiltä tehokkaasti. [55] Potentiaalista hyökkäyspintaa kasvattaa autonvalmistajien kokemuksen puute ohjelmistointensiivisistä ja voimakkaasti toisiinsa verkottuneista ajoneuvoista, sekä paine saada tuotteet markkinoille nopeasti. [56].

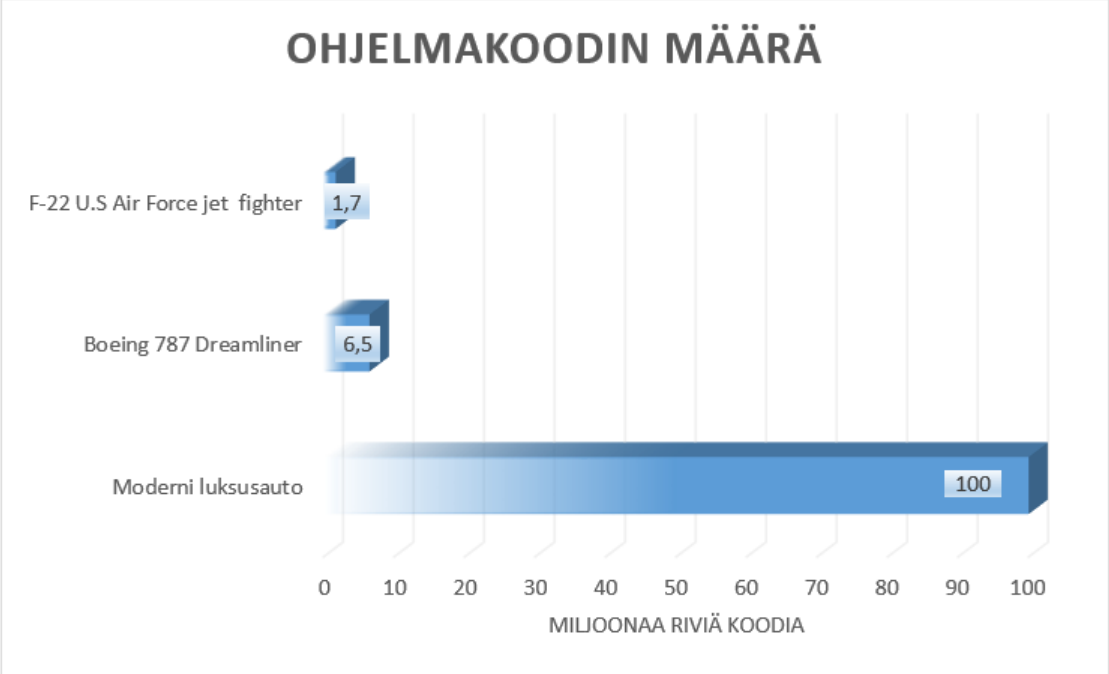
Toistaiseksi ajoneuvoihin kohdistetut hyökkäykset eivät vielä ole olleet arkipäiväisiä ja enimmäkseen vaarassa ovat tavalla tai toisella massasta poikkeavat ajoneuvot, herättäessään hyökkääjien mielenkiinnon. Kuitenkaan tilanne ei varmasti tule pysymään tällaisena elektroniikan, ja sitä myötä haavoittuvuuksien, lisääntyessä koko ajan. Yleisesti suurin huoli vaikuttaa kohdistuvan autonomisten ajoneuvojen tulemiseen ja niiden kykyyn toimia turvallisesti harkintaa vaativissa tilanteissa. Liikenteessä kuitenkin on jo suuri määrä internetiin kytkettyjä ajoneuvoja, joiden altistumisesta kyberhyökkäyksille ei ole varmuutta [52].

Hashem ja Ni [57] kuvaavat ajoneuvojen nykytilaa, vertaamalla liikenteessä liikkumista haiden kanssa uimiseen. Nykypäivän ohjelmallisesti ohjatut ajoneuvot toimivat osana laajasti verkottunutta maailmaa. Tätä kokonaisuutta ajateltaessa Hashem ja Ni neuvovat korvaamaan sanat ’ohjelmisto’ sanalla ’hakkeroitavissa’ ja ’verkottunut’ sanalla ’suojaton’. Hakkeroitavissa olevan, suojaamattoman auton vertaaminen haiden kanssa uimiseen tuntuu loogiselta.

Niin perinteisissä autoissa, kuin nykypäivän metsäkoneissa ja muissa vastaavissa, erilaisia toimintoja vaativissa laitteissa on tietotekniikkaa valtavissa määrin. Juuri mikään ei enää toimi mekaanisesti, vaan kaikkea vähintään ohjataan tietoteknisesti ajoneuvon sisäisen verkon kautta. Kun ajoneuvo kytkeytyy ulkopuoliseen verkkoon, tai ajoneuvon

verkkoon kytketään ulkopuolinen laite, avautuu mahdollisuus säädellä ajoneuvon toimintaa ulkopuolelta. Tietenkin myös tietojen urkinta ajoneuvosta mahdollistuu samalla. Lähes kaikissa uudemmissa ajoneuvoissa on jonkinlainen infotainment-järjestelmä, johon voi kytkeä USB-tikun tai mobiililaitteen suoraan esimerkiksi Bluetooth-yhteydellä.

Moderneissa ajoneuvoissa koodirivien määrä on moninkertainen verrattuna mm. lentokoneisiin, kuten kuvasta 7 näkyy. Koodin suuri määrä selittyy sillä, että lähes kaikkia toimintoja ohjataan ohjelmallisesti, takaluukun avauksesta lähtien. Tätä koodimäärää ajetaan noin 100 elektronisen ohjausyksikön sisällä. Nämä ohjausyksiköt muodostavat verkon ajoneuvon eri osien välillä. Kuvan tilanne on yli kymmenen vuoden takainen, vuodelta 2009. Koodirivien, ja samalla elektronisten ohjausyksiköiden (ECU, engl. Electronic Control Unit), määrä jatkaa kasvuaan uusien ominaisuuksien lisääntyessä. [58]



Kuva 7. *Koodirivien määrä lentokoneissa vs. autoissa, vuonna 2009. Perustuu lähteeseen [58].*

Ohjelmakoodin määrän odotetaan myös jatkavan kasvamistaan uusien turvallisuusjärjestelmien kehittämisen myötä. Vaikka elektronisilla järjestelmillä pystytään tuomaan lisää turvallisuusominaisuuksia, ohjelmakoodin lisääntyessä kasvaa myös potentiaalisten kyberhaavoittuvuuksien määrä. [59]

5.1 Ajoneuvojen tietotekninen rakenne

Aikaisemmin jokainen uusi elektroninen toiminto lisättiin omana elektronisena ohjausyksikkönään. Tämän seurauksena ajoneuvon sisäinen verkko kasvoi ja komplisoitui. Kaikkien toimintojen ollessa omissa hiekkalaatikoissaan, verkosta tuli monimutkainen kokoelma erilaisia protokollia. Tämän ongelman ratkaisemiseksi kehitettiin kommunikointiväyliä ohjausyksiköiden välille. Väylät mahdollistivat tiedon jakamisen ohjausyksiköiden välillä ja samalla kehittyneempien ominaisuuksien käyttöönoton. Esimerkiksi lukkiutumaton jarrujärjestelmä ABS (engl. anti-lock braking system) pystyy keskustelemaan turvavyöjärjestelmän kanssa ja näin turvavyöt voidaan kiristää ennen varsinaista kolaria. [8]

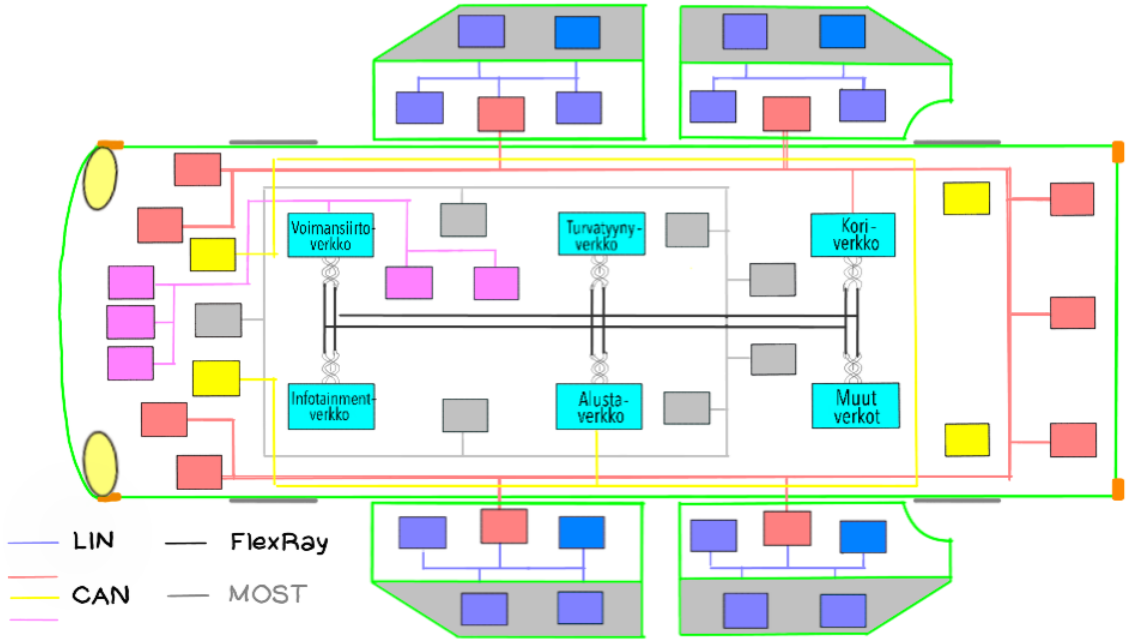
Elektroninen ohjausyksikkö on sulautettu järjestelmä, joka kontrolloi yhtä tai useampaa elektronista järjestelmää ajoneuvossa. Ohjausyksiköt saavat dataa ajoneuvon sensoreilta. Datan pohjalta ohjausyksiköt jakavat käskyjä ajoneuvon elektronisille järjestelmille. Elektroniset ohjausyksiköt voidaan luokitella niiden roolin perusteella. Moderneissa ajoneuvoissa on tyypillisesti erilliset elektroniset ohjausyksiköt voimansiirto-, turvallisuus-, mukavuus-, infotainment- ja telematiikkajärjestelmille. Voimansiirron ohjausyksiköt huolehtivat moottorin ja vaihteiston toiminnasta. Turvallisuudesta vastaavat ohjausyksiköt puolestaan huolehtivat mm. adaptiivisen vakionopeuden säätimen ja turvatyynyjen toiminnasta. Aktiivijousituksen ja ilmastoinnin toiminta kuuluu mukavuusjärjestelmille. Infotainment- ja telematiikkajärjestelmien ohjausyksiköt hallitsevat ääni- video- ja mobiilikommunikointijärjestelmiä. [60]

Elektroniset ohjausyksiköt ovat vastuussa kaikesta ajoneuvon toiminnasta. Ne kattavat yksinkertaiset tehtävät, kuten jarruvalojen sytyttämisen, mutta myös turvallisuuskriittiset tehtävät, kuten autonominen jarruttaminen. [60]

Elektronisten ohjausyksiköiden määrä ajoneuvojen verkossa jatkaa kasvuaan huolimatta ajoneuvovalmistajien pyrkimyksestä keskittää tietotekniikkaa. Nykyisissä autoissa, voi olla jopa 150 elektronista ohjausyksikköä. Tulevaisuudessa ohjausyksiköiden määrää tulee eniten lisäämään erilaiset ajoavustinjärjestelmät (ADAS, engl. Advanced Driver Assistance System) sekä hybridi- ja sähköajoneuvojen edellyttämät ohjausjärjestelmät. [61]

Ajoneuvon verkko sisältää useita kommunikointiprotokollia. Tyypillinen ajoneuvon verkkotopologia on kuvan 8 mukainen. Yleisin käytetyistä protokollista on CAN. Kuvan tapauksessa CAN-väyliä on kolme - voimansiirrolle, korille ja alustalle. CAN-väylien lisäksi tyypillisesti käytössä ovat LIN (engl. Local Interconnect Network) ja FlexRay. LIN-väylä on kuvassa violetilla merkitsemässä ovissa tapahtuvaa viestintää, mm. lukituksen oh-

jausta. FlexRay keskellä huolehtii laitteistojen välisestä viestinnästä. Näiden lisäksi infotainment-järjestelmän ohjausyksiköiden viestintä hoituu MOST-protokollan (engl. Media Oriented System Transport) avulla, kuvassa harmaalla. [62]

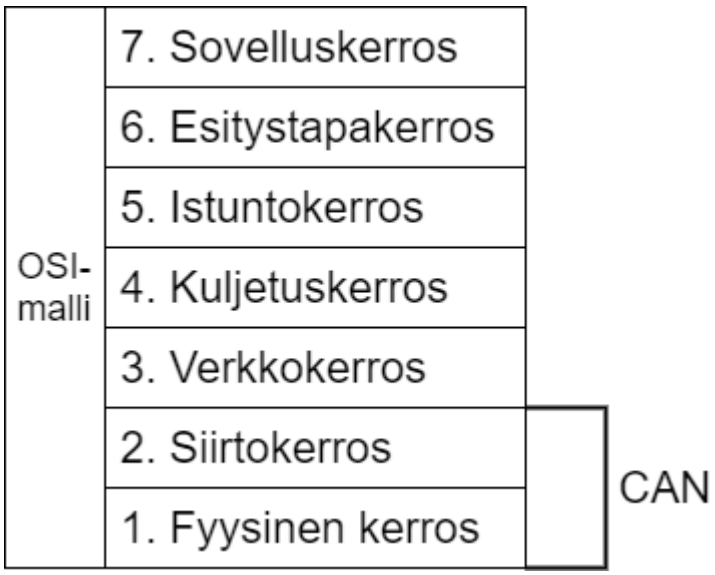


Kuva 8. *Ajoneuvon verkkotopologia. Perustuu lähteeseen [62]*

CAN-väylä on CAN-protokollaan perustuva kommunikointiväylä, jota käytetään ajoneuvoissa, mahdollistamaan sujuva ja luotettava kommunikointi verkon solmujen, eli noodien välillä. Tällaisia noodeja ovat esimerkiksi erilaiset sensorit, ohjaimet ja hallintalaitteet. [63,64] CAN-teknologian kehitti Bosch GmbH 1980-luvun alkupuolella. Ensimmäiset versiot olivat lähinnä ajoneuvojen käytössä, mutta nykyään CAN-väylää käytetään lisäksi laajalti mm. teollisuusautomaatiossa. [63]

Tiedonsiirtoon tarvittavia toiminnallisuuksia kuvaa viitteellinen OSI-malli (engl. Open System Interconnection Reference Model) [65]. CAN-protokolla määrittelee OSI-mallin kaksi alimmaista kerrosta, fyysisen ja siirtokerroksen (kuva 9). Useimmat järjestelmät tarvitsevat kuitenkin myös joitain ylemmistä OSI-mallin kerroksista. Tähän tarpeeseen on kehitetty ylempien kerrosten protokollia, kuten SAE J1939 ja CANopen. [63] SAE J1939 on kokoelma standardeja [66], jotka määrittelevät miten elektroniset ohjausyksiköt kommunikoivat keskenään esimerkiksi raskaan kaluston sisäisissä verkoissa [64]. CANopen puolestaan on protokollaperhe sulautettuun verkonrakennukseen. Sitä käytetään

mm. teollisuus- ja rakennusautomaatiossa sekä erikoisajoneuvo- ja työkonesovelluksissa [67].



Kuva 9. *CAN-protokolla määrittää OSI-mallin kaksi alinta kerrosta. Perustuu lähteeseen [63]*

CAN-väylä näyttäisi tulevaisuudessakin pysyvän tärkeänä osana ajoneuvojen verkkoa, mutta muutoksia siihen on tulossa. Laitteiden suuren määrän ja niiden toimintojen kompleksisuuden vuoksi nykyinen CAN on vaarassa ylikuormittua. Kasvavaan kaistan tarpeeseen on kehitetty CAN-FD (CAN Flexible Data-Rate) [68-70]. CAN-FD on paranneltu versio CAN-väylästä, joka tukee suurempaa kaistanleveyttä ja hyötykuormaa [71].

LIN-väylä on halvempi vaihtoehto CAN-väylälle. Sitä käytetään nykyaikaisissa ajoneuvoissa täydentämään CAN-väylää. LIN-väylä on heikompi kuin CAN-väylä nopeudessa ja vikasietoisuudessa. Usein LIN-väylää käytetään yhdyskäytävänä CAN-väylille. LIN-protokolla mahdollistaa yhden päälaitteen ja 16 sivulaitteen toiminnan korkeintaan 40 metrin mittaisella väylällä. Tämä riittää, koska ajoneuvoissa harvoin käytetään yli kymmentä noodia. [72]

Tyypillisiä käyttökohteita LIN-väylälle ajoneuvon verkossa ovat muun muassa ohjauspyörään integroitu ohjaus ilmastoinnille, pyyhkijöille ja radiolle. Lisäksi ilmastoinnin moottori ja ohjauspaneeli, sekä ovissa peilien, ikkunoiden ja lukituksen ohjaus kuuluvat myös tyypillisiin sovelluskohteisiin. [72]

FlexRay-verkkoa käytetään nopeaa tiedonsiirtoa vaativissa voimansiirto- ja turvallisuuslaitteistoissa. FlexRay on kehitetty ratkomaan CAN-väylän kaistanleveys- ja nopeusrajoitteita. Sen ei kuitenkaan uskota korvaavan kokonaan CAN- ja LIN-väylien käyttöä. [73]

MOST on kuituoptiikkaan perustuva nopea verkkoteknologia ajoneuvon sisäisille multimediapalveluille [60,74]. MOST-verkkoon voi liittää jopa 64 MOST-laitetta. Verkko on suunniteltu niin, että uusien laitteiden liittäminen ja poistaminen on yksinkertaista. Laitteet toimivat verkossa heti liittämisen jälkeen. [74] MOST-verkkoa käyttävät lähes kaikki ajoneuvovalmistajat ympäri maailman [60].

Edellä esitetyt väyläprotokollat on koottu taulukkoon 4. Taulukosta näkyy protokollien erot mm. nopeudessa ja pääsynvalvontaratkaisuissa.

Taulukko 4. *Väyläprotokollien ominaisuuksia. Perustuu lähteeseen [75]*

	LIN	***CAN***	***FlexRay***	***MOST***
Tiedonsiirtonopeus	20Kbps	1Mbps	10Mbps	24Mbps
Pääsynvalvonta	Pollaus	CSMA/CA	TDMA	TDM CSMA/CA
Fyysinen kerros	Yksijohdin	Kaksijohdin	Kaksijohdin, optinen kuitu	Kaksijohdin, optinen kuitu
Arkkitehtuuri	Yksi päälaite, tyypillisesti 2-10 sivulaitetta	Useita päälaitteita, tyypillisesti 10-30 noodia	Useita päälaitteita, jopa 64 noodia	Useita päälaitteita, jopa 64 noodia
Viestin kuljetus	Synkroninen	Asynkroninen	Synkroninen ja asynkroninen	Synkroninen ja asynkroninen
Viestin identifiointi	Tunniste	Tunniste	Aikaväli	-
Käyttö	Aliverkko	Ohjelmisto, reaaliaikainen	Laitteisto, reaaliaikainen	Multimedia
Viive	Jatkuva	Kuormasta riippuva	Jatkuva	Tietovirta

5.2 Autonomiset ajoneuvot

Autonomiset ajoneuvot ovat olleet tuloillaan liikenteeseen jo usean vuoden ajan. Suomessakin on ollut jo muutamia kokeiluja. Suomalainen robotiikka- ja ohjelmistoyritys, Sensible4, voitti jopa ’Dubai Self-Driving Transport’ -kilpailun startup kategorian vuonna 2019 [76]. Kesäkuussa 2019 Volvo ja Uber julkistivat tuotantovalmiin autonomisen autonsa, Volvo XC90 [77,78]. Kuitenkaan tämän Volvon ja Uberin yhteisprojektin testaus

ei sujunut ongelmitta, koska testiajossa ollut auto osui jalankulkijaan, joka menehtyi vammoihinsa. Autossa oli ollut turmahetkellä myös kuljettaja, joka oli onnettomuuden sattuessa keskittynyt puhelimeensa [77]. Automaattinen hätäjarrujärjestelmä olisi voinut pelastaa jalankulkijan hengen tekemällä hätäjarrutuksen tai varoittamalla kuljettajaa havaitessaan tiellä esteen. Hätäjarrujärjestelmä oli kuitenkin tapaturmahetkellä ollut kytkettynä pois päältä, joten tätä apua ei ollut käytettävissä [79,80].

Vuodesta 2016 alkaen singaporelaisen yliopiston kampusalueella on toiminut kuljettajaton taksi, jonka voi tilata älypuhelinsovelluksella. Etelä-Korea on rakentanut jopa kokonaisen kaupungin, nimeltään K-City, autonomisten ajoneuvojen testausta varten [81]. [82] Vuoden 2016 loppuun mennessä tässä kaupungissa oli testattu 11 autonomista autoa ja ajettuja kilometrejä oli kertynyt 260 000. Vuoden 2018 loppuun mennessä vastaavat luvut olivat 60 testattua ajoneuvoa ja 710 000km [83].

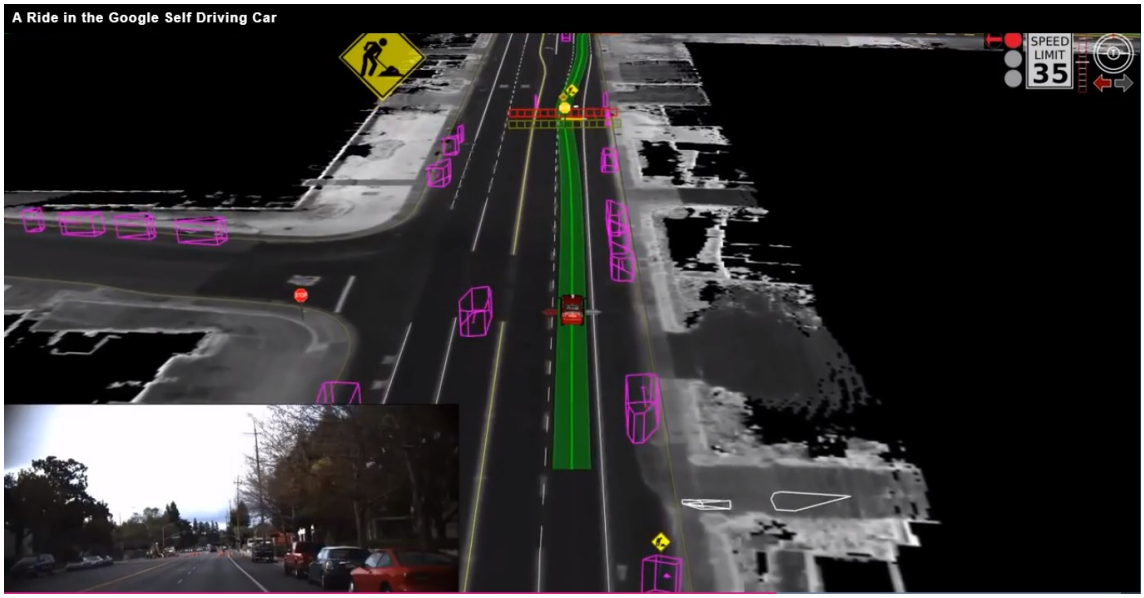
Autonomiseksi ajoneuvoa kutsutaan, kun se pystyy operoimaan omatoimisesti. Autonomian tasoja on kuusi (Taulukko 5). Tasolla 0 autonomiaa ei ole ja kuljettaja hoitaa ajamisen kokonaan itse, tasolla 1 ajoavustinjärjestelmä (ADAS, engl. Advanced Driver Assistance System) voi avustaa kuljettajaa joko jarrutuksen ja kiihdytyksen kanssa tai ohjauksessa. Vasta tasolla 2 ajoavustinjärjestelmä voi kontrolloida itsenäisesti sekä jarrutusta ja kiihdytystä, että ohjausta yhtäaikaisesti. Tasolla 3 automaattiajojärjestelmä (ADS, engl. Automated Driving System) voi sopivissa, ennalta määritellyissä olosuhteissa hoitaa kaikki ajoon liittyvät tehtävät, mutta olosuhteiden muuttuessa kuljettajan täytyy olla valmis ottamaan kontrolli takaisin itselleen. Tasolla 4 automaattiajojärjestelmä pystyy suoriutumaan ajamisesta itsenäisesti tietyissä olosuhteissa, mutta kuljettajalta vaaditaan edelleen tarkkaavaisuutta. Tasolla 5 ajoneuvo toimii täysin itsenäisesti ja puhutaan täydestä autonomiasta. Tällöin kaikki ihmiset autossa ovat matkustajia. [84]

Taulukko 5. *Ajoneuvojen autonomian tasot. Perustuu lähteeseen. [84]*

AUTONOMIAN TASOT	KUKA TEKEE, MITÄ JA MILLOIN.
TASO 0	Kuljettaja hoitaa kaiken ajamisen.
TASO 1	Ajoavustinjärjestelmä (ADAS) voi avustaa kuljettajaa joko ohjauksessa tai jarrutuksessa/kiihdytyksessä, mutta ei molempia samanaikaisesti.
TASO 2	Joissain olosuhteissa ajoavustinjärjestelmä (ADAS) voi itsenäisesti kontrolloida ohjausta ja jarrutusta/kiihdytystä yhtäaikaisesti. Kuljettajan täytyy kuitenkin säilyttää täysi tarkkaavaisuus ja hoitaa muut ajamiseen liittyvät tehtävät.
TASO 3	Automaattiajojärjestelmä (ADS) voi joissain olosuhteissa hoitaa kaikki ajoon liittyvät tehtävät, mutta kuljettajan pitää olla valmiudessa ottamaan kontrolli takaisin itselleen, järjestelmän niin vaatiessa. Muulloin kuljettaja hoitaa ajamisen.
TASO 4	Automaattiajojärjestelmä (ADS) voi hoitaa kaikki ajamiseen liittyvät tehtävät ja tarkkailla ympäristöään - periaatteessa hoitaa ajamisen -tietyissä olosuhteissa. Kuljettajan pitää olla tarkkaavaisena.
TASO 5	Automaattiajojärjestelmä (ADS) hoitaa kaikki ajamiseen liittyvät tehtävät kaikissa olosuhteissa. Ihmiset ovat vain matkustajina, eivätkä missään tilanteessa puutu ajamiseen.

Täysin autonomisessa ajoneuvossa ei tarvitse olla edes ohjauspyörää. Tällainen ajoneuvo hankkii kaiken tarvitsemansa tiedon itse, lukemalla ympäristöä sisäänrakennetuilla sensoreillaan, eikä se tarvitse syötteitä muilta ajoneuvoilta tai infrastruktuurilta. [85]

Kuva 10 on kuvakaappaus videolta [86,87], jossa esiteltiin autonomisen auton testaustilannetta. Isommassa kuvassa on sensoreiden muodostama näkymä ympäristöstä. Vasemmassa alakulmassa näkyy todellinen näkymä.



Kuva 10. *Testiajon näkymää sensoreiden ”silmin” ja todellisuudessa. Kuvakaappaus videolta [87]*

Sähköautonvalmistaja Tesla on asentanut uusimpiin malleihinsa Model 3, S ja X, mikropiirin, joka mahdollistaa täysin autonomisen ajamisen. Käyttöönotto vaatii, Teslan toimitusjohtaja Muskin mukaan [6], enää vain ohjelmiston kehittämistä. Tällä hetkellä Teslan valmius autonomiassa on tasolla 2, joka viittaa siihen, että ajoneuvo pystyy suorittamaan kahta asiaa yhtäaikaisesti ja itsenäisesti. Vasta tasolla 5 ajoneuvo toimisi täysin autonomisesti ja pystyisi suoriutumaan kaikista tilanteista itsenäisesti. [6]

Teslankaan autonomisen ajoneuvon pilotointi ei ole onnistunut ilman kuolonuhreja. Eräs Tesla Model S:n 40-vuotias omistaja kuoli ajettuaan autopilotilla kuorma-auton perävaunun alle. Onnettomuushetkellä vallitsevissa sääolosuhteissa sekä kuljettaja, että ajoneuvon sensorit epäonnistuivat havaitsemaan edessä olevan perävaunun. [88]

Edellä kuvatun onnettomuuden jälkeen Tesloihin on lisätty ominaisuus, joka neuvoo kuljettajaa pysymään tarkkaavaisena. Ajoneuvo myös kehottaa pitämään vähintään toista kättä ohjauspyörällä ja tarkkailee, että siihen kosketaan vähintään tietyn ajan välein. [88] Mikäli kuljettaja ei kehotuksista huolimatta koske ohjauspyörään, ajoneuvo laittaa kuljettajan ”jäähylle”. Eli ajoneuvo kytkee hätävilkut päälle, pysäyttää auton tien sivuun ja kytkee autopilotin pois. Autopilottia ei saa enää takaisin saman ajon aikana, vakionopeudensäädintä voi kuitenkin käyttää.

Täysin autonomisten ajoneuvojen käyttöönottoa rajoittavat myös moraaliset suunnittelukysymykset. Miten ajoneuvo ohjelmoidaan tekemään päätös tilanteessa, jossa onnettomuus ei ole vältettävissä ja vähintään yhden ihmisen turvallisuus vaarantuu. [89,90] Erilaisia päätöksentekomalleja on esitetty, mutta konsensukseen pääseminen ei ole ongelmatonta. Ihmiset perustavat moraalikäsityksensä eri asioihin, joten yksiselitteistä moraalisesti oikeata ratkaisua kaikkiin tilanteisiin lienee mahdotonta löytää. Santoni de Sio [89] lähestyy asiaa ajatellen, että moraaliset ongelmat on ratkaistu jo lainsäädännöllisesti ja laista löytyy perusta oikeutetun vahingon löytämiselle, moraalisista erimielisyyksistä riippumatta. Keeling [90] puolestaan haastaa tämän näkemyksen ja nostaa ongelmaksi juuri moraalisten erimielisyyksien ohittamisen.

Saattueajoa on testattu kuorma-autoilla myös Suomessa, mutta toistaiseksi vielä niin, että jokaisessa autossa on kuljettaja [91]. Täyden hyödyn saattueajosta saa vasta kun kuorma-autot ovat täysin autonomisia. Toisaalta pelkästään jo letkassa ajamalla saavutetaan hyötyä polttoaineen kulutuksessa.

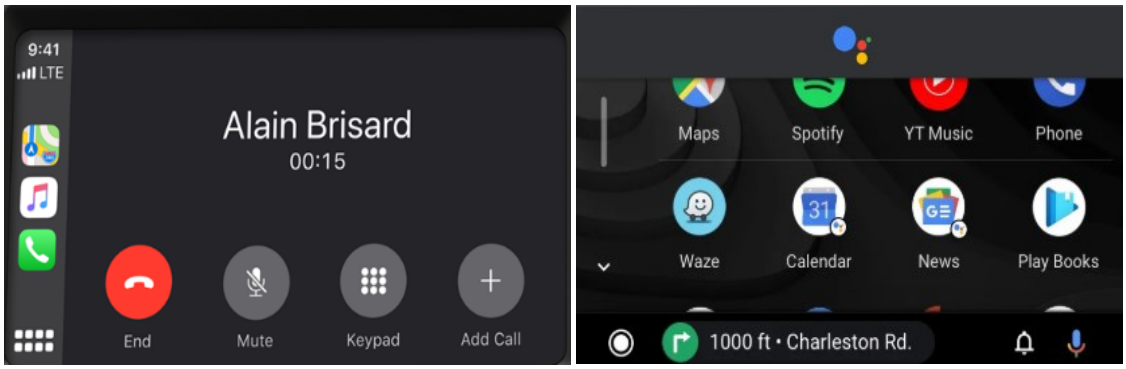
5.3 Matkapuhelimen käyttö autossa: Android Auto ja CarPlay

Matkapuhelinten käyttö on nykyään niin yleistä, että ne ovat jo ohittaneet perinteisen PC:n internetin käytössä [92]. Zendriven teettämän tutkimuksen [93] mukaan matkapuhelimen käyttö ajaessa on ollut ongelma jo pitkään, mutta tilanne pahenee edelleen. Tutkimuksen mukaan matkapuhelinriippuvaiset aiheuttavat jo enemmän onnettomuuksia kuin humalassa ajavat, eivätkä ihmiset välttämättä tunnista itseään matkapuhelinriippuvaisiksi. Zendriven tutkimuksen mukaan yli 69 miljoonaa ihmistä käyttää matkapuhelinta ajaessaan autoa, mikä tarkoittaa ainakin 60 prosenttia kuljettajista. [93]

Android Auto on Googlen kehittämä mobiilisovellus, jolla Android-älylaite peilataan ajoneuvon infotainment-järjestelmään. Jotta Android Autoa voi käyttää, täytyy älylaitteessa olla Android 5.0 tai uudempi käyttöjärjestelmä. [94] Automallista riippuen sovellusta voi käyttää ajoneuvon kosketusnäytöltä tai älylaitteen ruudulta. Myös älylaitteen näytöltä käytettynä sovellus yksinkertaistaa käyttöliittymää ja helpottaa yleisimmin käytettyjen sovellusten käyttöä ajon aikana. Android Auto -ympäristölle on myös tehty ajoneuvon itsediagnosointiin tähtääviä sovelluksia, joita voi käyttää Android Auto -käyttöliittymän kautta [95]. Google on luonut listan laatuvaatimuksista [96] sovelluksille, jotka on tarkoitettu käytettäväksi Android Auton kautta. Laatuvaatimusten tarkoituksena on pitää sovellukset sellaisina, että ne häiritsevät mahdollisimman vähän kuljettajaa. Esimerkkeinä tällaisista vaatimuksista voidaan mainita paluu ja koti -painikkeet, ääniohjauksen suosiminen ja animaatioiden välttäminen [95].

CarPlay taas on Applen samaan tarkoitukseen suunnittelema sovellus. Android Autosta poiketen, CarPlay toimii vain ajoneuvon omalla näytöllä ja se tukee vain ajoneuvomalleja, joista löytyy tarkoitukseen sopiva kosketusnäyttö. Edelleen CarPlayn avulla käytettävien sovellusten määrä on pienempi, sillä Apple on tarkka siitä mitä sovelluksia saa käyttää. Myös CarPlayn osalta on määritelty laatuvaatimukset sovelluksille, jotka on tarkoitettu käytettäväksi kyseisessä ympäristössä [97].

Matkapuhelinten ajonaikaisen käytön ja siitä aiheutuvien onnettomuuksien välttämiseksi on positiivista, että sekä Google että Apple ovat kehittäneet kykyä kytkeä matkapuhelin saumattomasti ajoneuvon infotainment-paneeliin. Kokonaan Android Auton tai CarPlayn käyttäminen ei ongelmaa poista, mutta se vähentää tarvetta näppäillä matkapuhelinta ajon aikana. Kuvassa 1 on näkymä sekä CarPlayn että Android Auton näytöistä.



Kuva 11. *Esimerkkikuvat vasemmalla CarPlay [97] ja oikealla Android Auto [98] – näytöistä.*

5.4 Puettavat älylaitteet

Useat ajoneuvovalmistajat ovat kehittäneet sovelluksia, jotka hyödyntävät puettavia älylaitteita, kuten älykelloja. Tällaiset älylaitteet voivat tarjota esimerkiksi ajoavustinjärjestelmälle tietoa biometrisillä mittauksilla. Näiden pohjalta voidaan parantaa ajomukavuutta, turvallisuutta ja taloudellisuutta. Puettavien älylaitteiden hyödyntäminen ajoneuvon toiminnallisuuksien parantamisessa, voisi parhaimmillaan tuoda helpotusta jokapäiväisiin asioihin terveydenhuollosta, kuljetukseen, viihteeseen ja kommunikointiin. [99]

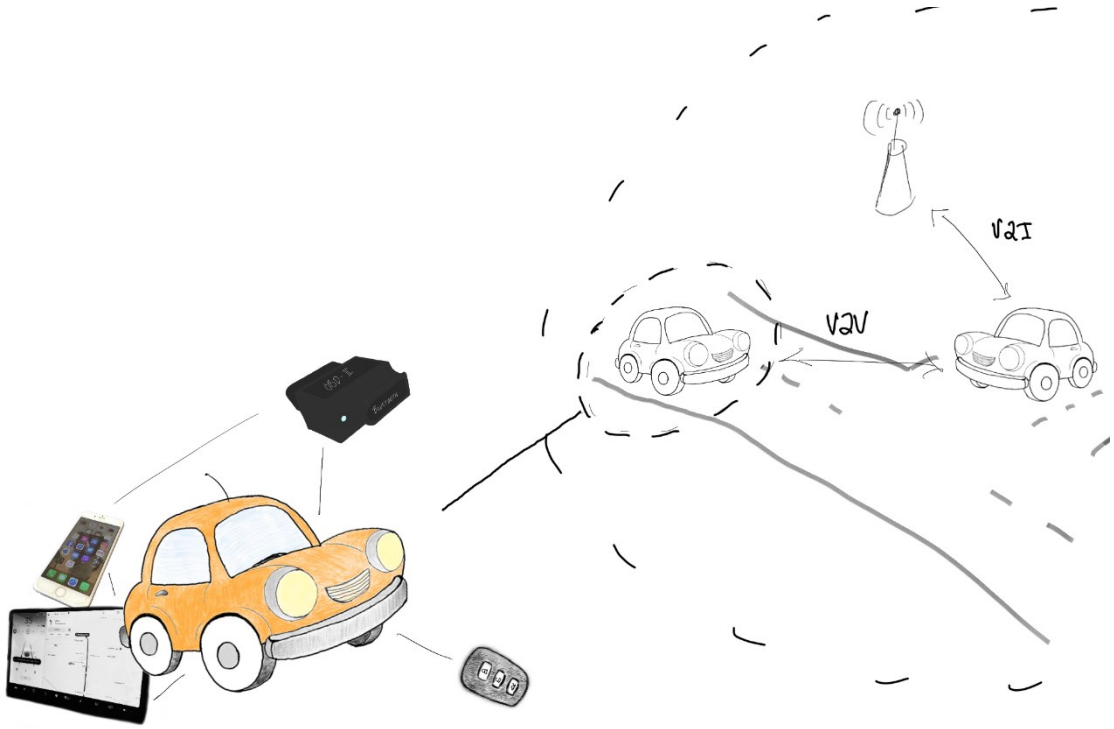
Puettavien laitteiden tutkimuslaboratorio Fordilla on testannut ääniohjausta MyFord-mobiilisovelluksen ja älykellon avulla. Sovelluksen avulla kuljettaja voi käynnistää, lukita ja avata ajoneuvonsa lukituksen äänikomennolla. Tämän lisäksi puettavat älylaitteet voisivat toimia yhteistyössä ajoneuvon infotainment-järjestelmän kanssa, joka esimerkiksi matkustajan älylaitteen ilmoittaessa terveysongelmasta, auttaisi kuljettajaa valitsemaan tehokkaimman reitin sairaalaan. Älykelloja voidaan käyttää myös kuljettajan uneliasuuden tunnistamisessa ja herätteen antamisessa [100,101]. [99]

Esimerkkeinä viihdepalveluista ajoneuvon matkustajille on musiikin ja videoiden toistaminen sekä interaktiivisten pelien pelaaminen mm. älykellojen ja -lasien avulla [102]. Lisäksi älylaitteiden ja ajoneuvojen yhteistyötä voisi hyödyntää ajoneuvovarkauksien vähentämisessä. Puettava älylaite voi oppia tuntemaan käyttäjänsä käyttäytymismallin ja järjestelmä voisi tämän tiedon avulla tunnistaa älylaitteen käyttäjän ajoneuvon omistajaksi. Autovarkaan yrittäessä viedä auto, järjestelmä tunnistaisi käyttäytymismallin normaalista poikkeavaksi ja lähettäisi ajoneuvon omistajalle ilmoituksen epäilyttävästä toiminnasta sekä auton sijaintitiedon. [99]

6. AJONEUVOJEN HAAVOITTUVUUDET

Tässä luvussa perehdytään tarkemmin ajoneuvon hyökkäyksille alttiisiin rajapintoihin. Näistä laajimpia kokonaisuuksia ovat kaikista ajoneuvoista löytyvä CAN-väylä ja ajoneuvojen sekä infrastruktuurin verkostosta muodostuva VANET. CAN-väylän haavoittuvuuksiin perehdytään aliluvussa 6.1 ja VANETin 6.5. Pienempiä, mutta silti merkittäviä, kokonaisuuksia ovat ajoneuvon itsediagnosointijärjestelmä OBD-II, Infotainment-järjestelmä sekä avaimeton avaus ja käynnistys. Näiden haavoittuvuuksiin tutustutaan aliluvuissa 6.2, 6.3, 6.4.

Kaikki yllä luetellut rajapinnat ovat haavoittuvia itsessään. Sen lisäksi ne mahdollistavat pääsyn erilaisiin haavoittuviin rajapintoihin. VANETin koostuessa ajoneuvoista, jotka keskustelevat kaiken kanssa (V2X, engl. Vehicle to Everything), haavoittuvuudet ajoneuvon rajapinnoissa on riski. Ryhmä V2X koostuu ajoneuvojen kommunikoinnista toisten ajoneuvojen (V2V, engl. Vehicle to Vehicle), infrastruktuurin (V2I, engl. Vehicle to Infrastructure) ja jalankulkijoiden (V2P, engl. Vehicle to Pedestrians) kanssa [103]. Koska ajoneuvot ovat olennainen osa VANETia, yksittäisen ajoneuvon rajapintojen haavoittuvuudet ovat myös VANETin haavoittuvuuksia (kuva 12).



Kuva 12. *Ajoneuvon haavoittuvuudet ovat myös VANETin ongelma. Kuvassa värillinen auto on nostettu esiin VANET kokonaisuudesta. Auton haavoittuvista rajapinnoista esiin on nostettu OBD-II, infotainment-järjestelmä sekä avaimeton avaus ja käynnistys.*

6.1 CAN

CAN [70,104] on eniten käytetty protokolla ajoneuvojen tiedonsiirtoväylissä [105]. Se toimii alustana kaikelle ajoneuvon sisäisen verkon toiminnalle. CAN-väylä yhdistää ajoneuvon elektroniset ohjausyksiköt toisiinsa ja mahdollistaa niiden keskinäisen kommunikaation. Johonkin ohjausyksikköön käsiksi pääseminen aiheuttaa näin ollen potentiaalisen uhan kaikille samaan väylään kytketyille yksiköille.

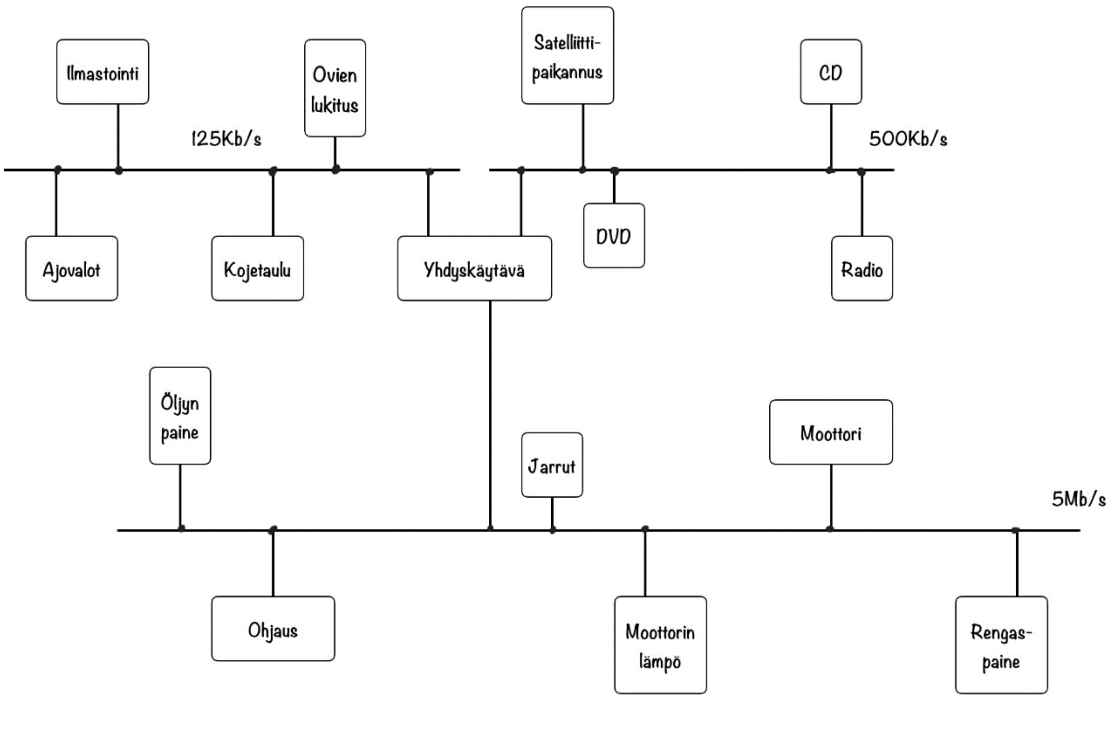
CAN on alun perin suunniteltu huomattavasti pienemmän ja suljetumman verkon käyttöön, eikä ajoneuvon käyttäjällä ole ollut pääsyä väylään. Turvallisuuskysymykset eivät siksi ole olleet päällimmäisinä suunnittelussa. CAN on altis ainakin nuuskinnalle, toistohyökkäyksille, dataväärennyksille ja datainjektiolle. [106] Nuuskinnalla tarkoitetaan verkon pakettien monitorointia ja kaappaamista. Dataväärennyksellä viitataan tilanteeseen, jossa järjestelmässä liikkuvaa datapakettia muokataan ja puolestaan datainjektiolla tarkoitetaan uuden datapaketin tuomista järjestelmään.

[106]Bozdal *et al.* [106] osoittivat CAN-väylän olevan haavoittuvainen laitteistotroijalaiselle. Laitteistotroijalaisella tarkoitetaan jo valmistusvaiheessa laitteistoon, esimerkiksi elektroniseen ohjausyksikköön, asennettua haittaohjelmaa, joka aktivoituu laitteistoa käytettäessä [107]. Riski laitteistotroijalaisiin ajoneuvoissa on kasvussa, kun yhä useampia laitteistoja ostetaan valmiina toteutuksina [106]. Laitteistotroijalainen vaikuttaa järjestelmään sisältäpäin. Tämän vuoksi se ei ole taltutettavissa perinteisillä tunkeutumisenestojärjestelmillä (IPS, engl. Intrusion Prevention System), jotka on suunniteltu estämään vain ulkoapäin tulevat hyökkäykset.

Kuvassa 13 on esitetty tyypillinen CAN-väylistä koostuvan verkon rakenne. Toiminnot on jaettu tarvittavan tiedonsiirtonopeuden perusteella eri väyliin. Hitaammat laitteet, kuten ovien lukitus ja ilmastoinnin ohjaus voidaan yhdistää pienemmän tiedonsiirtonopeuden väylällä. Nopeaa reagointia vaativat laitteet, kuten jarrujärjestelmä ja moottorin ohjaus on yhdistettävä verkkoon nopealla väylällä.

Väylät on liitetty toisiinsa yhdyskäytävän kautta. Täysin erillisiksi verkoiksi osioita ei voi irrottaa, sillä toiminnot tarvitsevat tietoa toisiltaan. Esimerkiksi kojetauluun välitetään tietoa moottorin pyörimisnopeudesta ja ilmoitus rengaspaineen laskiessa. Yhdyskäytävä

siis huolehtii tiedonsiirrosta väylien välillä. Jaottelua kuitenkin tarvitaan, jotta erityisesti turvallisuuskriittisten toimintojen riskiä altistua hyökkäykselle voidaan pienentää.



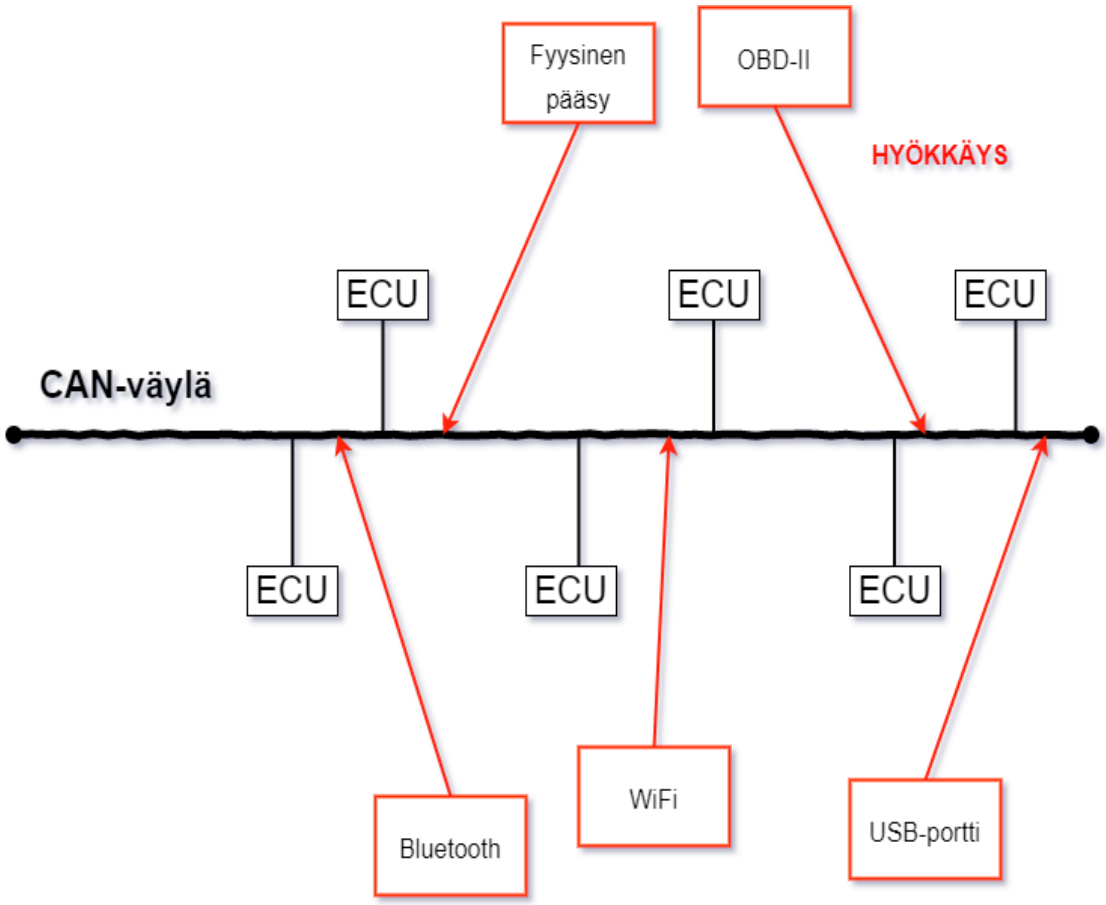
Kuva 13. *Tyypillinen verkon rakenne ajoneuvossa. Perustuu lähteeseen [108]*

CAN-protokollassa elektroniset ohjausyksiköt siirtävät tietoa toisilleen oman tunnisteensa sisältävissä datakehyksissä. Muut elektroniset ohjausyksiköt noutavat datakehyksiä valikoiden, tunnistettuaan lähettäjän tunnuksen, eli ID:n [9]. Tunnistetiedon lisäksi ID kertoo myös paketin tärkeysasteen: mitä pienempi numero sen tärkeämpi ja kiireellisempi paketti. Esimerkiksi ajoneuvon ohjaukseen ja moottorin toimintaan liittyvät paketit ovat tärkeämpiä kuin viihdepalveluiden viestintä. Näin ollen niiden ID-numero on pienempi. [109]

CAN on dynaamisesti laajennettavissa uusilla noodeilla ja siksi se kuljettaa dataa broadcast jakeluna. Tästä johtuen elektroniset ohjausyksiköt ovat valmiita hyväksymään kaikki paketit lähettäjän tunnisteesta riippumatta. Haitallisten laitteiden on näin ollen mahdollista toimittaa haitallisia pakettejaan väylässä. [109]

CAN-protokollan suurin heikkous on sen puutteet pääsynhallinnassa, autentikoinnissa ja salauksessa. Protokollasta kehitetty uudempi versio CAN-FD [70] tuo lisää kaistanleveyttä ja mahdollistaa suuremman hyötykuormamäärän. Valitettavasti se ei kuitenkaan tuo parannusta tietoturvaan. [71]

Sen jälkeen, kun hyökkääjä on päässyt tunkeutumaan ajoneuvon verkkoon, on hyökkääjän mahdollista suorittaa useita eri tyyppisiä hyökkäyksiä. Olettaen hyökkääjällä olevan pääsy CAN-väylään tai muihin siihen kytkeytyviin laiterajapintoihin kuten Bluetooth, OBD-II, Wi-Fi, USB tai fyysinen pääsy, uhkamalli on kuvan 14 mukainen. [109]



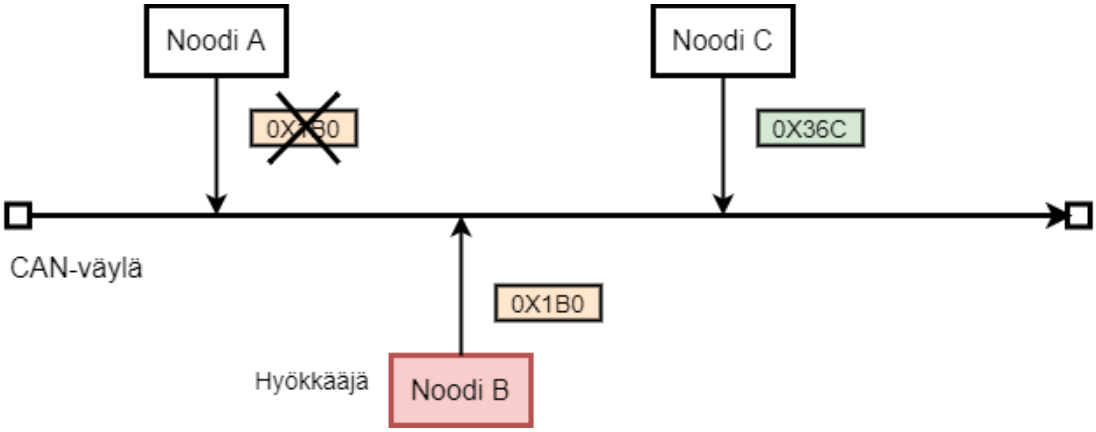
Kuva 14. *Uhkamalli. CAN-väylään mahdollistuu punaisella merkittyjen rajapintojen kautta. Tällä tavoin päästään kiinni elektronisten ohjausyksiköiden (ECU) viesteihin. Perustuu lähteeseen [109]*

Jos hyökkääjä pääsee kiinni ajoneuvon verkkoon ja pystyy kontrolloimaan ja muokkaamaan kohteeksi valittua elektronista ohjausyksikköä, voi hyökkääjä kyetä vaikuttamaan ajoneuvon toimintaan. Xiao *et al.* [109] kuvaavat kolme CAN-väylään suunnattua hyökkäystä: impersonaatio- palvelunesto- ja toistohyökkäys. Seuraavaksi nämä esitellään tarkemmin.

Impersonaatio-hyökkäyksessä (kuva 15) tunkeutuja korvaa alkuperäisen elektronisen ohjausyksikön omalla ohjausyksiköllään, joka ottaa alkuperäisen ohjausyksikön roolin väylässä. Impersonaatio-hyökkäys ei muuta alkuperäistä CAN-viestien lähetystahtia, joten aikataulutukseen perustuvat tunkeutumisenhavaitsemisjärjestelmät (IDS, engl. Intrusion Detection System) eivät sitä huomaa. Mikäli hyökkääjä ei muuta CAN-viestin sisältöä, elektroninen ohjausyksikkö vaikuttaa oikeutetulta. Hyökkääjä voi tällöin käyttää

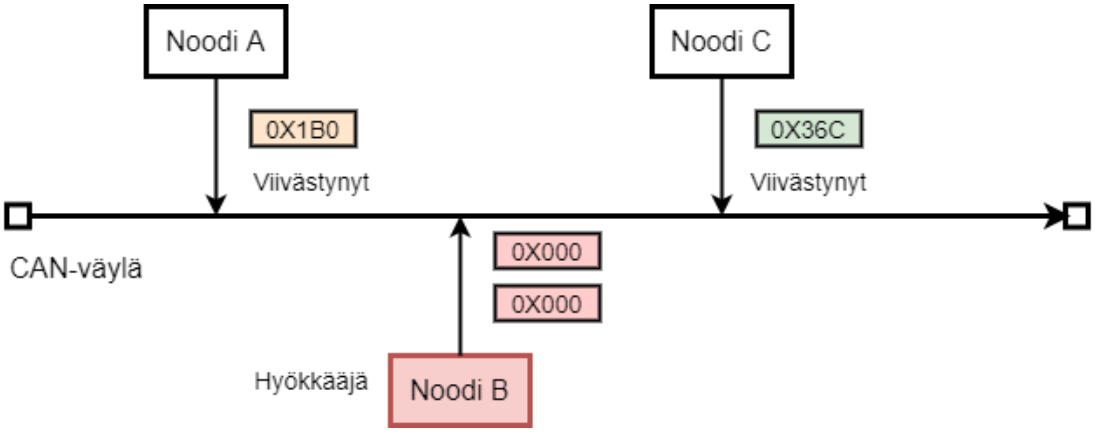
sitä muun tyyppisten hyökkäysten alustana. [109,110] Tällaisessa oikeutettuna ohjausyksikkönä esiintyvässä ohjausyksikössä voi esimerkiksi olla asennettuna takaportti järjestelmään.

Kuvan 15 esimerkissä noodi B on hyökkääjän asettama ohjausyksikkö, joka on tekeytynyt noodiksi A. Noodin B lähettämät paketit korvaavat alkuperäiset ohjausyksikön paketit, eikä ohjausyksikön joutumista hyökkäyksen kohteeksi havaita.



Kuva 15. *Impersonaatio-hyökkäys. Perustuu lähteeseen [110].*

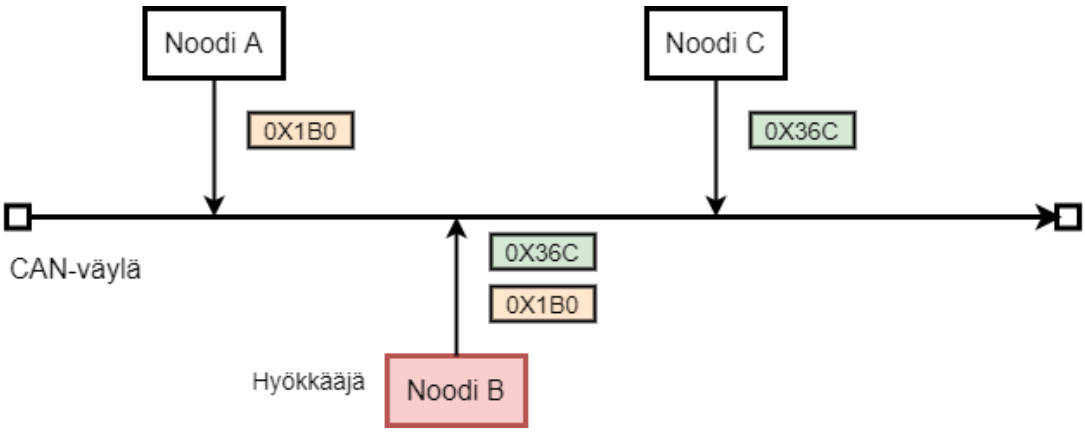
Palvelunestohyökkäyksessä (kuva 16) hyökkääjä syöttää toistuvasti CAN-väylään korkean prioriteetin käskyjä. Tämä johtaa siihen, että oikeutetut käskyt eivät pääse kulkemaan ajallaan. Kuvassa haitallinen noodi B lähettää teoreettisesti korkeimman ID:n *0x000* paketteja ja valtaa väylän koko kapasiteetin. Tämän seurauksena noodien A ja B pakettien välitys viivästyy. [109,110]



Kuva 16. *Palvelunestohyökkäys. Perustuu lähteeseen [110].*

Toistohyökkäyksessä (kuva 17) hyökkääjä lähettää valideja käskyjä CAN-väylään satunnaisesti, saaden ajoneuvon käyttäytymään odottamattomalla tavalla. Tällaista hyökkäystä varten hyökkääjän tarvitsee kerätä tietoja kohdeajoneuvosta. Esimerkiksi hyök-

kääjä voi tunnistaa sellaisen käskyn, joka voi aiheuttaa tilanteeseen nähden odottamatonta käytöstä, kuten ohjauspyörän tärinää ja suuntavilkkujen tai merkkivalojen vilkkumista. [109,110]



Kuva 17. *Toistohyökkäys. Perustuu lähteeseen [110].*

6.2 Ajoneuvon sisäinen diagnosointijärjestelmä OBD-II

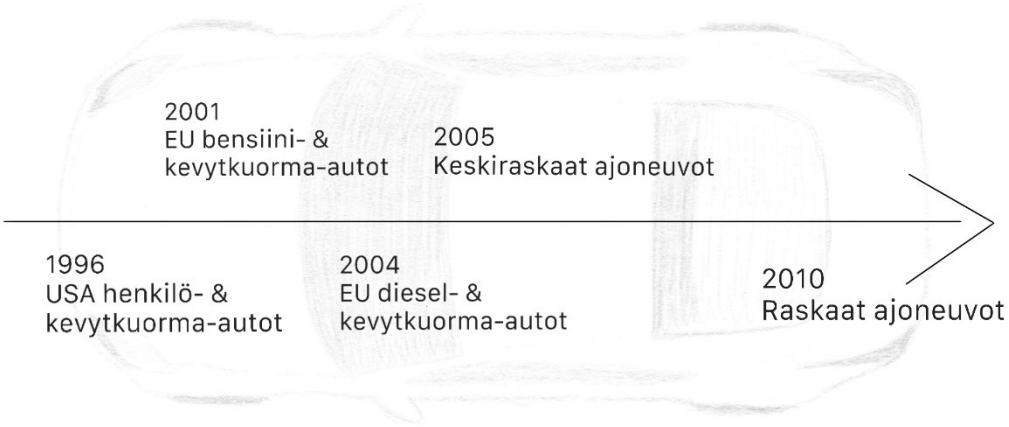
Ajoneuvon sisäinen diagnosointijärjestelmä OBD-II [111] on uudempi ja kehittyneempi versio OBD-I-standardista. Diagnosointijärjestelmä on ensisijaisesti ajoneuvomekaanikkojen käyttöön suunnattu nopean vikadiagnosoinnin työkalu [112].

Tässä luvussa käsitellään ajoneuvon sisäisen diagnosointijärjestelmän käyttöä ja haavoittuvuuksia. Järjestelmän historiaa ja kehitystä esitellään lyhyesti aliluvussa 6.2.1. Käytössä oleva versio on OBD-II ja siksi aliluvussa 6.2.2 keskitytään käsittelemään kyseistä versiota koskevia käyttötilanteita.

6.2.1 Kehitys

Ensimmäisenä, moottorin tilaa lukemaan kykenevän OBD:n, esitteli Volkswagen 1968. Kymmenen vuotta myöhemmin Datsun otti käyttöön yksinkertaisen OBD-järjestelmän [113]. OBD:n käyttö alkoi yleistyä 70- ja 80-luvun vaihteessa. Sitä käytettiin tarkkailemaan moottorin toimintaa ja tunnistamaan häiriöitä, pääasiassa vastaamaan Yhdysvaltojen ympäristönsuojeluvirasto EPA:n (engl. Environmental Protection Agency) päästöstandardeihin [114]. OBD standardoitiin 1980-luvun lopussa. Ennen sitä kaikilla valmistajilla oli omat järjestelmänsä käytössä. Kaliforniassa California Air Resource Board (CARB) on vuodesta 1991 vaatinut, että kaikki uudet autot on varustettu OBD:lla. Vuodesta 1996 eteenpäin kaikissa USA:ssa myydyissä henkilö- ja kevyissä kuorma-autoissa OBD-II on ollut pakollinen, EU:ssa sama vaatimus tuli voimaan 2001 bensiiniautojen ja vuonna 2004 dieselautojen osalta. Vuodesta 2005 vaatimus on koskenut myös keskiraskaita ja 2011 raskaita ajoneuvoja. Suurin osa nykypäivän henkilö- ja kevyistä kuorma-

autoista sisältävät OBD-II:n. [115] Kuva 18 havainnollistaa OBD-II järjestelmän aikajanaa.



Kuva 18. *OBD-II:n pakolliseksi tulo uusissa autoissa Yhdysvalloissa ja EU:ssa. Vuosiluvut videosta [116].*

Myös OBD-III-järjestelmä on olemassa, CARB aloitti sen testaamisen jo vuonna 1994. OBD-III kehitettiin poistamaan tarve korjaamokäynneille ajoneuvon vikadiagnoosien saamiseksi. Auton OBD-III-järjestelmä keskustelee tienvarteen sijoitettujen lukijoiden kanssa. Kun auto ilmoittaa lukijalle vikakoodin, ajoneuvon tunniste ja vikakoodi välitetään läheiselle toistimelle. Toistin ottaa vastaan tiedon viasta ja lähettää sen edelleen valmistajalle, joka ottaa yhteyttä ajoneuvon omistajaan. Järjestelmän käyttöönottaminen odottaa edelleen laillisuuskysymysten ratkaisemista. Tällaisia ovat erityisesti kysymykset liittyen yksityisen omaisuuden massavalvontaan. [112]

6.2.2 Haavoittuvuudet

OBD-II-dataan käsiksi pääseminen on ollut mahdollista myös kuluttajille jo useiden vuosien ajan. Markkinoilla on useita erimerkkisiä laitteita. Merkin lisäksi myös laitteen mahdollistamat toiminnot vaihtelevat. Osalla on mahdollista vain lukea vikakoodeja, osa tarjoaa valmiimpaa tietoa koodien sisällöstä ja lisäksi on laitteitta, joilla voidaan myös syöttää dataa järjestelmään OBD-liitynnän kautta [115]. Viimeksi mainitun kaltaiset ovat suurin riski järjestelmän tietoturvan kannalta. Asiaan perehtymätön kuluttaja ei kuitenkaan voi olla varma, ettei pelkkänä lukijana ostettu tuote ole kykenevä myös syöttämään dataa järjestelmään. Tämä riski korostuu, jos lukija hankitaan varmistumatta sen alkuperän luotettavuudesta.

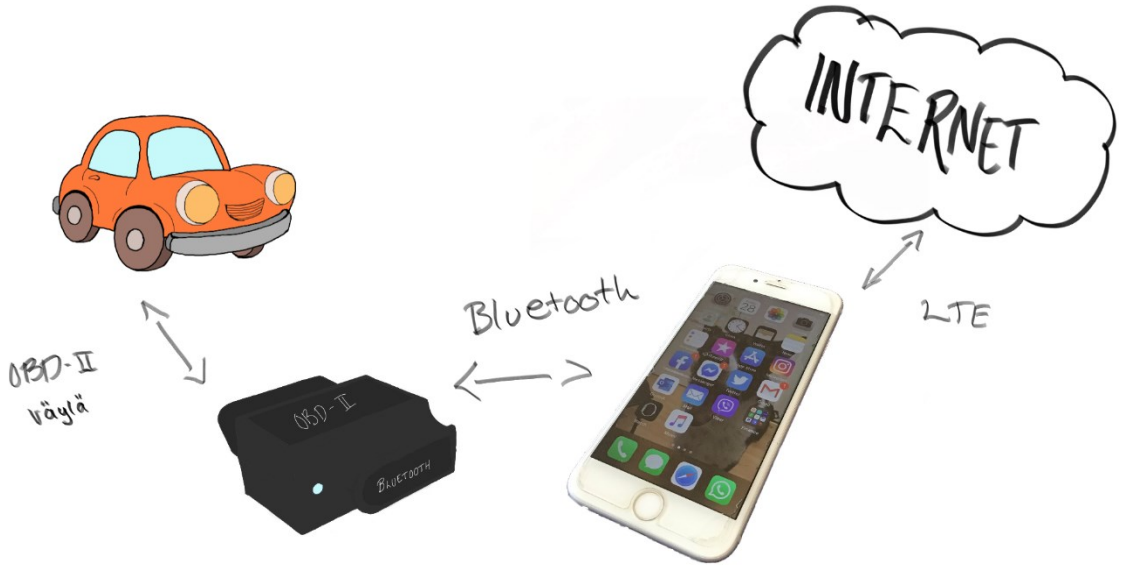
Koska yhä suurempaa osaa ajoneuvojen ominaisuuksista säädellään elektronisesti, varsinkin kuluttajapuolella yhä useammalle herää mielenkiinto hankkia laite, jolla pääsee

itse syöttämään dataa auton sisäiseen verkkoon. Internet on täynnä ohjeita auton itsetoimiseen koodaamiseen, joka ei edes vaadi minkäänlaisia ohjelmointitaitoja. Tässä yhteydessä koodaamisella tarkoitetaan konfigurointiparametrien arvojen muuttamista valmiiseen sovellukseen, joka on ladattavissa internetistä. Esimerkiksi BMW:n tapauksessa vuoden 2013 ja sitä vanhemmissa malleissa käytössä oli INPA-niminen sovellus ja sitä uudemmissa sovellus on nimeltään Esys.

Merkkikohtaisilta foorumeilta löytyy tietoa kunkin merkin ja mallin käyttämistä sovelluksista ja siitä mitä muuta vaaditaan. Esys-sovelluksen tapauksessa itse ohjelma on ladattavissa internetistä ja samoin kunkin BMW:n mallin vaatimat konfiguraatiotiedot. YouTubesta löytyy seikkaperäisiä ohjevideoita erilaisten ominaisuuksien muuttamiseen omassa autossa. Näiden avulla lähes kuka vaan voisi tehdä muutoksia autoonsa. Videollaan [117]nimimerkki ProjectF30 esittelee tarvittavat laitteistot ja toimenpiteet tiettyjen ominaisuuksien käyttöönottamiseen, itse ja ilmaiseksi, BMW F30 mallissa [117]. Videolla ei kuitenkaan erityisesti painoteta tietoturvan tärkeyttä, muuta kuin itse muutosten tekemisen kohdalla. On tietenkin erittäin tärkeää tehdä muutokset oikein, jotta ei vaaranna auton toimivuutta väärillä arvoilla. Vähintään yhtä tärkeätä olisi pitää huolta siitä, että ajoneuvoon OBD-II-liitoksen kautta kytketty tietokone on turvallinen. Autojen virittämisestä innostuneet ihmiset eivät kuitenkaan välttämättä ole tietoturvan ammattilaisia ja riski on suuri, että samaa, mahdollisesti vanhentuneilla tietoturvapäivityksillä varustettua, tietokonetta käytetään sekä auton koodaamiseen, että internetiin kytkettävänä koneena. Tällöin on vaarana, että tietokoneen kautta kulkeutuu haittaohjelma auton järjestelmään. Auton, tietokoneen ja ohjelmiston lisäksi hankittavaksi jää vain muutaman kymmenen dollarin arvoinen liitinkaapeli, jolla tietokone kytketään auton OBD-II-liitäntään.

OBD-II-sovittimen (engl. OBD-II dongle) avulla ajoneuvon vikakoodeja voi tarkastella langattomasti. Sovitin kytketään OBD-II-liittimeen ja siihen muodostetaan yhteys älypuhelimella Bluetoothin välityksellä. Älypuhelin puolestaan on yhteydessä internetiin LTE-yhteydellä. Toimintaperiaate on esitetty kuvassa 19. Sovitin alustaa itsensä, kun se kytketään ajoneuvoon ja jää odottamaan Bluetooth-yhteyttä. Kun puhelin on muodostanut Bluetooth-yhteyden, sovitin lähettää komennot tiedon noutamisesta puhelimelle ja jää odottamaan paluukomentoja. Paluukomennot saatuaan sovitin välittää komennot oikealle elektroniselle ohjausyksikölle ja vastauksen takaisin puhelimeen. [118]

Koska sovittimen myötä fyysistä pääsyä OBD-II-liitäntään ei hyökkääjältä vaadita, avautuu jälleen uusi näkymätön hyökkäyspinta. Bluetooth-yhteyden muodostaminen on mahdollista esimerkiksi liikennevaloissa tai parkkipaikalla viereen pysähtyvästä ajoneuvosta. Bluetoothin kantama voi käytetystä versiosta ja ympäristön esteistä riippuen yltää jopa kilometriin saakka [119], joten ihan lähelle hyökkääjän ei edes ole välttämätöntä päästä. Uhkia OBD-laitteelle on koottu taulukkoon 6.



Kuva 19. *OBD-II-sovittimen toimintaperiaate. OBD-II-sovitin kytketään autoon ja yhteys matkapuhelimeen muodostetaan Bluetooth-yhteydellä. Matkapuhelin puolestaan on yhdistettynä internettiin matkapuhelinverkon kautta.*

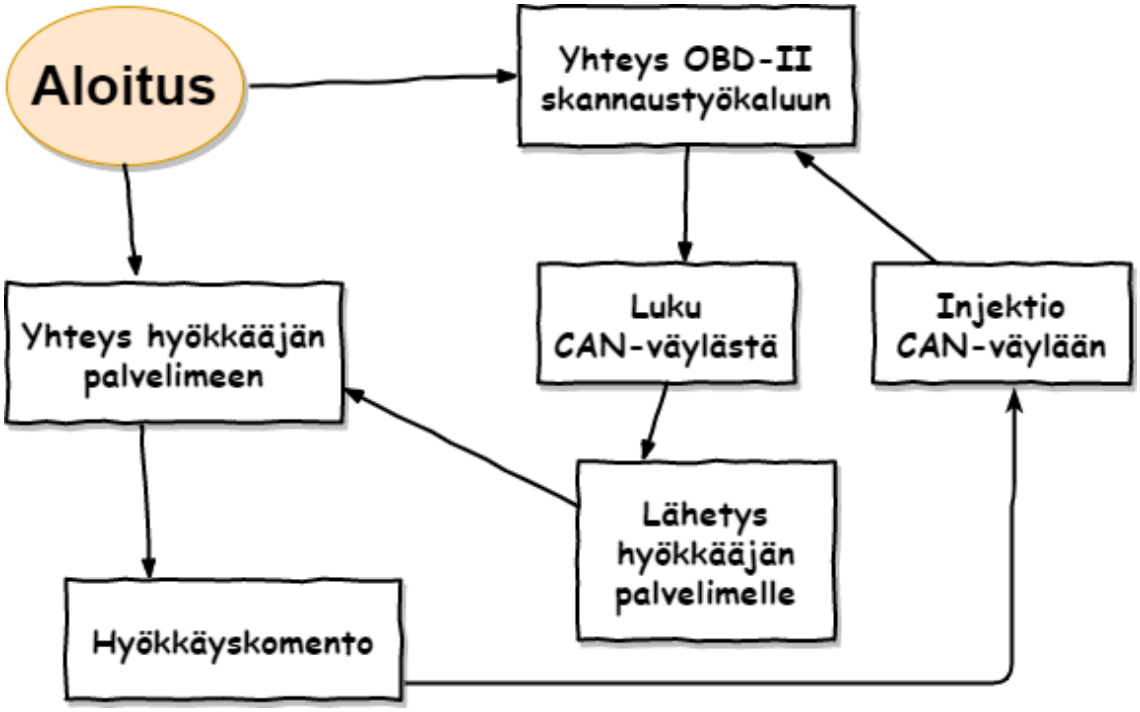
Taulukko 6. *OBD-sovellusten uhkia. Perustuu lähteeseen [95].*

HYÖKKÄYS-TEKNIIKKA	KUVAUS HYÖKKÄYKSESTÄ
CAN-INJEKTIO	Hyökkääjät lähettävät muokatun CAN-viestin suorittaakseen vaarallisen operaation.
OBD-II-LAITTEEN VAARANTAMINEN	Hyökkääjät käyttävät turvatonta OBD-laitetta kontrolloidakseen ajoneuvon tärkeitä komponentteja.
BLUETOOTH SALAKUUNTELU	Hyökkääjät ottavat OBD-laitteen kontrollin ja pääsyn kriittisiin komponentteihin, kun omistajan laite ei ole kytkettynä.
YKSITYISYYDEN LOUKKAUS	Tunkeutujat käyttävät OBD-laitetta hyökkäyksessä ajoneuvon mobiililaitteisiin ja varastavat henkilökohtaista dataa.
JÄLJITYS	Hyökkääjät hankkivat luvattomasti ajoneuvon tietoja ja seuraavat sen tilaa.

OBD-II-sovittimen asentaminen esimerkiksi ajoneuvomurron yhteydessä on mahdollista. Vastaavasti yhteiskäyttöisten ajoneuvojen kohdalla asentaminen ei tuota ongelmaa. Sovitin on ulkomitoiltaan melko pieni, joten sen havaitseminen OBD-II-liitännälle tyypillisestä sijainnista, ohjauspyörän alapuolelta läheltä kuljettajan jalkatilaa, ei ole helppoa. Yhteiskäyttöisten ajoneuvojen tapauksessa, yksittäinen käyttäjä, ei voi tietää onko sovitin asennettu palveluntarjoajan puolesta vai onko kyseessä hyökkääjän asentama laite. Yhteiskäyttöisistä ajoneuvoista asiattoman sovittimen havaitseminen vaatisi ajoneuvojen säännöllistä tarkistamista.

Woo, *et al.* [9] tutkivat työssään matkapuhelinsovelluksen avulla suoritettua langatonta hyökkäystä verkottuneeseen autoon. He tutkivat tilannetta, jossa käyttäjä asentaa OBD-II-sovittimen ja tarkkailee sen avulla matkapuhelimen kautta ajoneuvon diagnostiikkaa (kuva 20). Matkapuhelimeen asennettu diagnostiikkasovellus sisältää kuitenkin haitallista koodia, joka lähettää tietoja ajoneuvosta hyökkääjän palvelimelle. Näin saadun tiedon perusteella hyökkääjä pystyy muodostamaan kohdennettua haitallista dataa, joka syötetään ajoneuvon sisäiseen verkkoon. Sovelluksen käyttäjälle kaikki näyttää normaa-

lilta toiminnalta, kun sovellus näyttää diagnostiikkaa ajoneuvon tilasta. Tutkijat onnistuivat työssään saamaan ajoneuvosta käsiinsä CAN-datakehyksen, joka kontrolloi polttoaineen syöttöä, ja sammuttamaan ajoneuvon moottorin.



Kuva 20. *Kaaviokuva haittakoodia sisältävän, matkapuhelimeen asennettavan, diagnostiikkasovelluksen toiminnasta. Perustuu lähteeseen [9].*

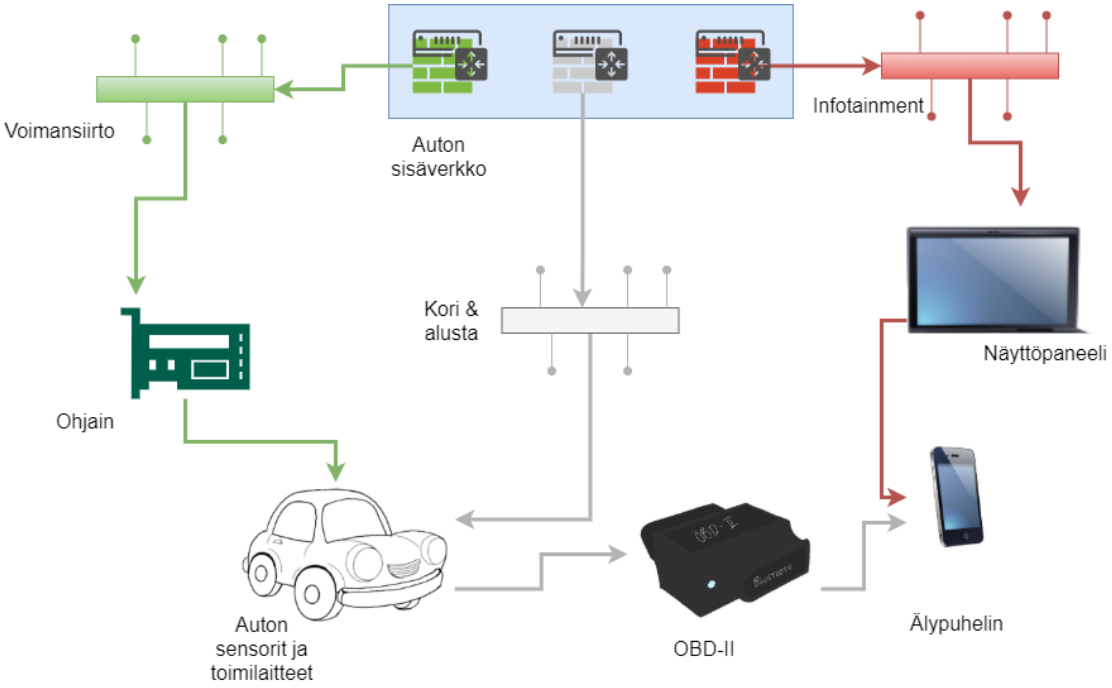
Mandal *et al.* kuvaavat artikkelissaan [95] OBD-II-väylän tietoja käyttävää sovellusta, joka itsessään ei suoraan sisällä haittakoodia, mutta joka lähettää keräämänsä tiedot palvelimelle salaamattomia reittejä pitkin. Myös palvelimella tieto on salaamatonta ja näin ollen suojaamatonta, joten sitä voidaan käyttää ilman ajoneuvon omistajan suostumusta. Mainitussa tapauksessa kyseessä oli sadetilannetta tarkkaileva sovellus, joka keräsi ajoneuvosta tietoja kuten sijainnin, tuulilasin tilan ja ajoneuvon nopeuden. [95] Hyökkääjän on siis mahdollista kaapata tiedot joko siirtovaiheessa tai palvelimelta. Tästä johtuen tiedon luottamuksellisuus vaarantuu.

6.3 Infotainment

Sulautettu infotainment-järjestelmä on kehittynyt perinteisestä autoradiosta. Infotainment-järjestelmä koostuu ohjelmistosta ja laitteistosta, kuten ohjauspaneelista, vahvistimesta ja kaiuttimista. Se on, kaiken muun ajoneuvotekniikan tavoin, kehittynyt merkittävästi ensimmäisestä versiostaan. Nykyaikaiseen infotainment-järjestelmään voi musiikkia viedä monin tavoin, mm. massamuisteilla ja jopa suoratoistaa internetistä. [120]

Infotainment-järjestelmät ovat kehittyneet huomattavasti alkuperäistä musiikintoistojärjestelmää älykkäämmäksi. Nykyään infotainment-järjestelmää voidaan käyttää esimerkiksi navigaattorina, ohjaamaan matkapuhelimen toimintoja ja pysäköintiavustajana. Useat autonvalmistajat tekevät myös yhteistyötä Applen ja Googlen kanssa. Applen tuoteperheen laitteiden kytkemiseksi ajoneuvon infotainment-järjestelmään on kehitetty CarPlay, Googlen Android-laitteille vastaava tuote on Android Auto. [120] Android-laitteille vastaavia ominaisuuksia tarjoaa myös tuote nimeltään MirrorLink.

Matkapuhelinten liittäminen ajoneuvon infotainment-järjestelmään ja sitä kautta koko ajoneuvon sisäiseen verkkoon, aiheuttaa huolta turvallisuudesta. Kuva 21 havainnollistaa infotainment-järjestelmän sijainnin ajoneuvon verkossa. Vaikka infotainment-järjestelmä ei kytkeydy suoraan ajoneuvon sisäiseen verkkoon, se kuitenkin yhdyskäytävien kautta liittyy siihen. [95]



Kuva 21. *Infotainment-järjestelmä ajoneuvon verkossa. Perustuu lähteeseen [95].*

Vastaavasti kuin matkapuhelinten kohdalla, puettavat älylaitteet, vaikka ovatkin hyödyllisiä, ajoneuvoon kytkettyinä avaavat uuden mahdollisen rajapinnan hyökkäyksille. Infotainment-järjestelmän uhkia on koottu taulukkoon 7.

Taulukko 7. *Uhat infotainment-järjestelmässä. Perustuu lähteeseen [95].*

HYÖKKÄYS-TAPA	KUVAUS HYÖKKÄYKSESTÄ
VIRUS / HAITTAOHJELMA	Suorittaa luvattomia toimia impersonaation tai ohjelmistovirheen avulla.
AUTENTIKOINTI	Ajoneuvon ominaistiedot, kuten ID, laitteisto tai autentikointitieto varastetaan tai naamioidaan luvattomaan käyttöön.
LUVATON ASETUS	Ajoneuvon data vaarannetaan impersonaatiolla tai ohjelmistovirheeseen hyökkäämällä.
VIRHEELLINEN INFORMAATIO	Haitallinen ohjelma lähettää väärää viestiä infotainment-järjestelmään harhauttaakseen kuljettajaa tai suorittaakseen luvattomia toimia.
HÄIRINTÄ	Haitallinen ohjelma hallinnan viestintäreittiin, kaappaa säännöllisen viestin ja sekoittaa luvattomalla viestillä.
JÄLJITYS	Hyökkääjät hankkivat luvattomasti ajoneuvon tietoja ja seuraavat tietoja, kuten nopeus, sijainti ja määränpää.
KULJETTAJAN HARHAUTUS	Haitallinen ohjelma häiritsee kuljettajaa näyttämällä näytössä kuvia, videota tai toistamalla ääntä.

Osassa moderneista ajoneuvoista infotainment-järjestelmä on itsessään kytketty internetiin mobiiliverkon kautta. Vähintään mahdollisuus mobiiliverkkoon liittämiselle löytyy monista uusista ja muutaman vuoden vanhoista ajoneuvoista. Esimerkiksi uudet Teslat on kytketty automaattisesti mobiiliverkkoon, jonka kautta autonvalmistaja toimittaa päivityksiä. Samaa verkkoa voi käyttää myös viihdepalveluihin tietyin rajoituksin. Teslan käyttämä mobiiliverkon kautta tapahtuva päivitysten jakaminen tuntuu kuitenkin turvallisemmalta, kuin Chryslerin vuonna 2015 tekemä ratkaisu lähettää ohjelmistovirheen korjaustiedostot postitse autojen omistajille USB-tikuilla. Sen lisäksi, ettei auton omistajien voida odottaa osaavan toteuttaa päivitys ongelmitta, on mukana riski, että joku levittää väärennettyjä massamuistilaitteita [121].

Checkoway *et.al.* [122] tutkivat takaisinmallinnuksen avulla mahdollisuutta tunkeutua ajoneuvon verkkoon Bluetooth- ja matkapuhelinverkon liitynnän kautta. Molemmissa tapauksissa he onnistuivat tunkeutumaan elektroniseen ohjausyksikköön ja sitä kautta avasivat pääsyn ajoneuvon verkkoon.

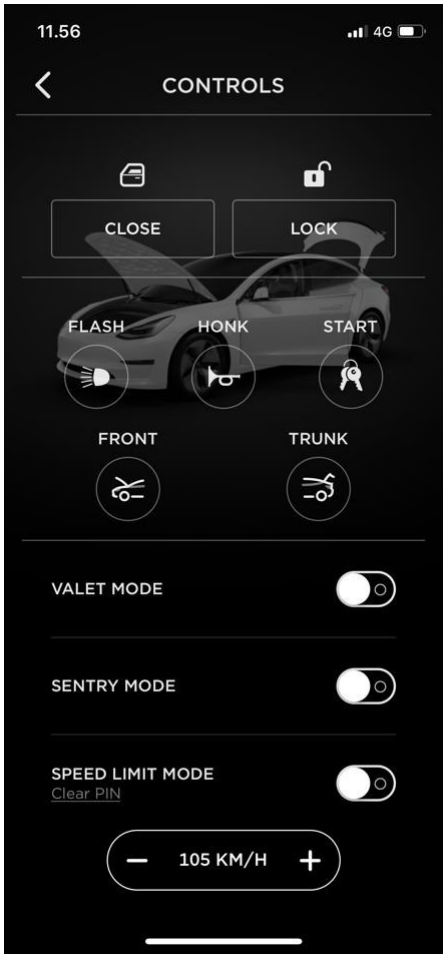
6.4 Avaimeton avaus ja käynnistys

Uusissa autoissa avaimeton avaus ja käynnistys (PKES, engl. Passive Keyless Entry and Start) on yleistynyt. Sen ajatuksena on, että riittää kunhan kuljettajalla on avain taskussa. Hän voi avata auton lukituksen ja käynnistää moottorin koskematta avaimeen. Tällaiset avaimet ovat lähinnä pieniä kaukosäätimiä tai jopa avainkortteja. Toisissa kaukosäädin mallisissa avaimissa on vielä sisään rakennettuna perinteinen fyysinen avain (kuva 22), mutta toisista fyysinen avain on jätetty kokonaan pois.

Kuva 22. *Auton kaukosäädin ja siihen integroitu fyysinen avain.*

Auton avaimena voi joidenkin automallien kohdalla käyttää myös matkapuhelinta. Tällainen ominaisuus on mm. uusissa Tesloissa. Kuva 23 on kuvakaappaus sovelluksesta,

jolla voidaan etänä muokata Teslan asetuksia. Lukituksen lisäksi sovelluksen kautta voidaan vaikuttaa moniin muihin asetuksiin, kuten lämmittää auton sisätila, sytyttää ajovalot tai asettaa autolle nopeudenrajoitus.



Kuva 23. *Kuvakaappaus Teslan matkapuhelinsovelluksesta.*

Toisissa automalleissa on oven kahvoissa painikkeet, joita painamalla, avaimen ollessa riittävän lähellä, ovet avautuvat ja menevät lukkoon. Maksimietäisyys, esimerkiksi vuoden 2017 Opel Vivarossa, on noin yksi metri [123]. Kaikissa autoissa ei ole näitä painikkeita vaan ovien avaus ja lukitseminen tapahtuvat automaattisesti avaimen etäisyyden mukaan.

Liikenteessä on autoja erilaisilla lukitusmekanismeilla, vaikka avaimeton käynnistys valtaa alaa uusien autojen myötä. Taulukkoon 8 on koottu erilaiset avaintyypit ja niiden toiminnallisuudet.

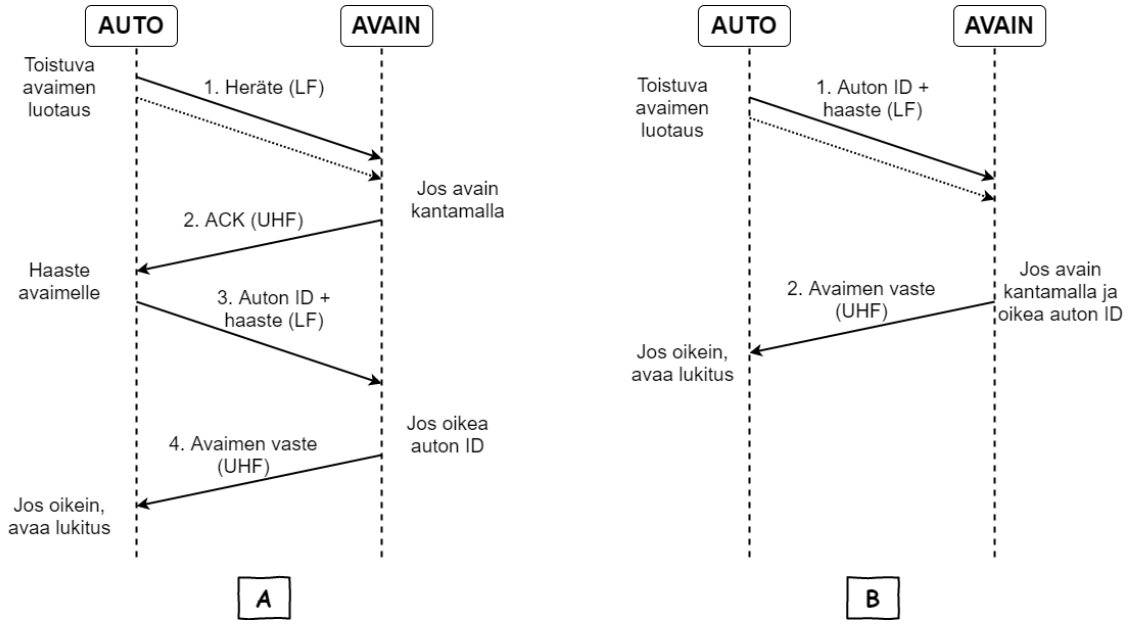
Taulukko 8. *Toiminnot avaintyypeittäin. Perustuu lähteeseen [124].*

Avaintyyppi	Lukitus	Käynnistys
Fyysinen avain	Fyysinen avain	Fyysinen avain
Fyysinen avain RFID ajonestolla	Fyysinen avain	Fyysinen avain + RFID
Avaimeton lukitus RFID ajonestolla	Kaukosäätöinen, aktiivinen (nappi kaukosäätimessä)	Fyysinen avain + RFID
Avaimeton käynnistys (PKES)	Kaukosäätöinen, passiivinen	Kaukosäätöinen, passiivinen

Auton lukituksen avaaminen kaukosäätimen napin painalluksella, toimii UHF-signaalilla tyypillisesti 10-100 metrin säteellä autosta. Ajonestolla varustetut avaimet sisältävät RFID-sirun, jonka auto autentikoi, kun avain asetetaan virtalukkoon. Vain aiemmin auton kanssa paritettu RFID-siru hyväksytään ja auton käynnistys sallitaan. [124]

Avaimeton käynnistys ja passiivinen ovien avaus perustuvat ajoneuvon ja avaimen haaste-vaste-pariin. Ajoneuvo luotaa toistuvasti avainta, määrittääkseen sen etäisyyden. Kun ajoneuvo havaitsee avaimen olevan riittävän lähellä, se lähettää avaimelle haasteen ja jää odottamaan avaimelta vastetta. Kättely voi olla toteutettu kahdella tapaa. Kuvassa 24 on esitetty kaksi vaihtoehtoista autentikointitapaa: energiatehokas ja nopea protokolla.

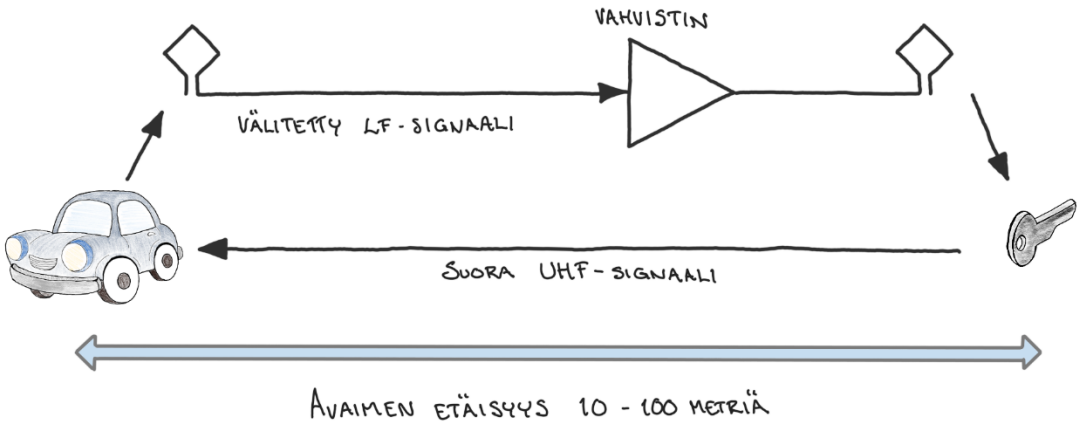
Ensimmäinen tapa vaatii useampia välivaiheita, mutta on energiatehokkaampi. Siinä ajoneuvo lähettää ensin luotauspaketin pelkistettynä, lyhyellä kantamalla. Vasta avaimen vastatessa luotaukseen, ajoneuvo lähettää ID:nsä ja haasteen LF-signaalina ja avain voi vastata haasteeseen. Toinen tapa on nopeampi, sillä ajoneuvo lähettää toistuvasti ID:stään ja haasteesta koostuvaa pakettia, jolloin avain pääsee vastaamaan haasteeseen suoraan. [124]



Kuva 24. *Kaksi kommunikointitapaa ajoneuvon ja avaimen välille. A energiatehokkaampi, B nopeampi. Perustuu lähteeseen [124].*

Kuva 25 esittää releointihyökkäyksen (engl. relay-attack), jota pidetään yhtenä avaimettoman avauksen ja käynnistyksen suurimpana uhkana. Hyökkäyksessä signaali välitetään kaapelin ja mahdollisen vahvistimen avulla kauemmaksi kuin se muuten kantaisi. Näin synnytetään vaikutelma, että ajoneuvo ja avain ovat lähempänä toisiaan kuin ne todellisuudessa ovat. Signaali välitetään kohteeseen radiotaajuisena signaalina. [124] Kohteen avain saa ajoneuvolta haasteen, johon se vastaa. Vaste saattaa kantaa perille ilman vahvistusta, sillä se lähetetään UHF-signaalina, jonka kantama on jopa 100 metriä. Hyökkäyksen avulla voidaan siis avata ajoneuvon lukitus ja käynnistää se ilman, että avain todella olisi ajoneuvon vieressä.

Francillion *et al.* [124] testasivat tutkimuksessaan myös muita releointihyökkäyksiä. Monimutkaisemmilla laitteistoilla ja järjestelyillä kantamaa onnistuttiin pidentämään merkittävästi ja sitä kautta, todellisessa tilanteessa, kiinni jäämisen riski pienenee. Koska turvallisuussyistä ajoneuvo ei sammuta itseään käynnistyttyään, vaikka avainta ei enää havaittaisi, voi autovaras ajaa pois paikalta.



Kuva 25. *Releointihyökkäys antennien, kaapelin ja vahvistimen avulla. Perustuu lähteeseen [124].*

Luvattoman pääsyn ajoneuvoon voi mahdollistaa myös radiohäirinnällä. Kun käyttäjä poistuessaan painaa avaimen kaukosäätimestä lukituspainiketta, ovien tulisi mennä lukkoon. Mikäli tätä radioliikennettä häiritään, ei viesti saavuta ajoneuvoa ja ovet jäävät auki. [124]

Ajoneuvon tai irtaimen anastamisen lisäksi PKES-järjestelmän haavoittuvuuden hyödyntäminen avaa mahdollisuuden jatkohyökkäyksille. Fyysisen pääsyn saatuaan, hyökkääjä voi esimerkiksi asentaa OBD-väylän tai USB-median kautta haittaohjelman ajoneuvon järjestelmään. Näin hyökkääjä pystyy myöhemmin ottamaan yhteyttä etänä asentamaansa haittaohjelmaan. Murrosta ei jää jälkiä, sillä ajoneuvo keskustelee valtuutetun avaimen kanssa.

6.5 Ajoneuvoverkko VANET

Ajoneuvoverkko VANET, MANETin (engl. Mobile Ad hoc NETwork) aliryhmä, on älykkäiden ajoneuvojen muodostama dynaaminen verkko, jossa ajoneuvot kommunikoivat keskenään ja tienvarsi-infrastruktuurin kanssa langattomasti. [125] VANET on lupaava teknologia liikenteen sujuvuuden ja turvallisuuden parantamisen kannalta. Se avaa myös mahdollisuuden muiden sovellusten hyödyntämiseen ajoneuvojen välisessä kommunikaatiossa [126].

VANETin avulla on tarkoitus välittää tietoa niin liikenneolosuhteista, onnettomuuksista kuin tarjolla olevista palveluista kaikille liikenteessä liikkujille. Kuitenkin infrastruktuurin kehitystä ja ajoneuvokannan uudistumista tarvitaan vielä, jotta VANET-verkkoa päästään hyödyntämään. Varsinkin Suomessa autokanta on keskimäärin vanhaa. Vuonna 2019 autokannan keski-ikä oli henkilöautojen kohdalla reilut 12 vuotta ja kuorma-autojen osalta vastaavasti hieman vajaat 14 vuotta [127,128].

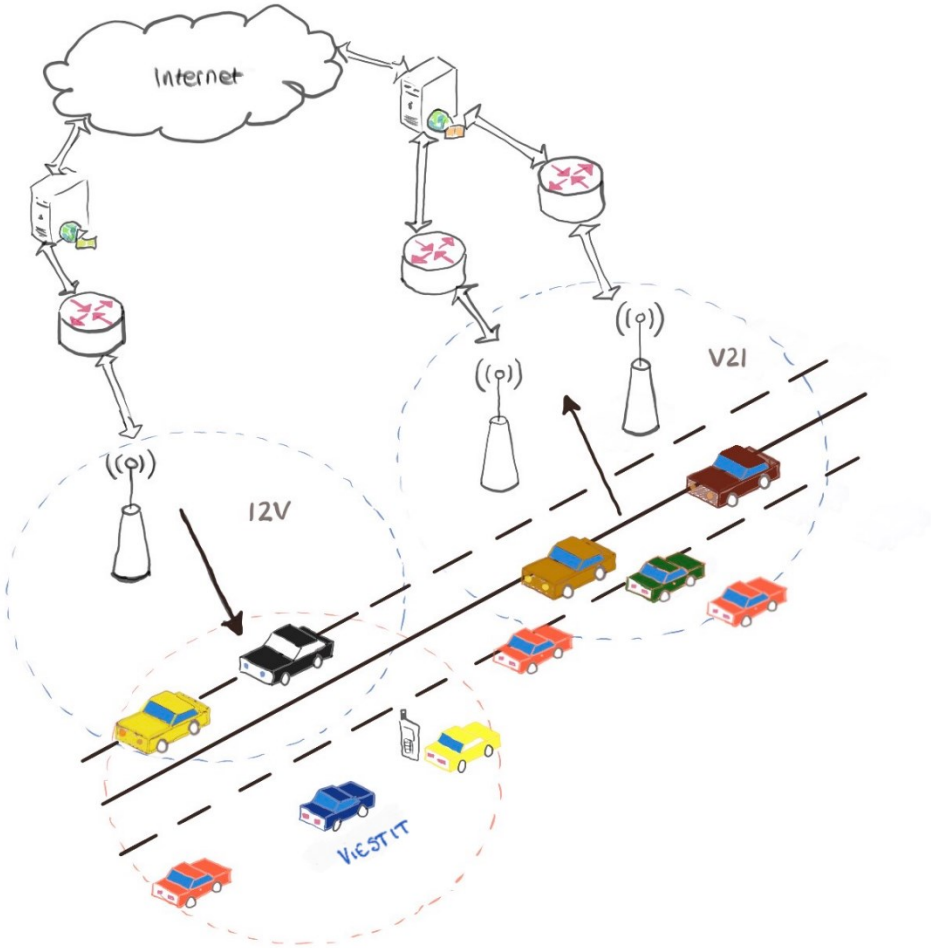
6.5.1 Viestintä VANETissa

Älykkäässä liikennejärjestelmässä kaikki solmut toimivat lähettäjinä, vastaanottajina ja reitittiminä, välittäen tietoa verkkoon eteenpäin jaettavaksi. VANET on merkittävässä roolissa älykkään liikennejärjestelmän toteutuksessa. Kuvassa 26 on esitetty yksinkertainen VANET-järjestelmäarkkitehtuuri. Toimiakseen tehokkaana osana verkkoa, jokainen solmu kerää tietoa ympäristöstään ja tekee päätöksiä keräämänsä ja muualta saamansa tiedon perusteella. Tietoa kerätään ja jaetaan käyttämällä erilaisia sensoreita, kameroita, sisäisiä tietokoneita, GPS-vastaanottimia, tallentimia (EDR, Event Data Recorder) ja suuntaamattomia antenneja. [129]

Ajoneuvojen sisäiset yksiköt (OBU, On-Board Unit) ja tienvarsiyksiköt (RSU, engl. Road Side Unit) muodostavat yhteisen tilapäisen verkon, jonka solmujen olemassaolosta ei tarvita ennakkotietoa [125]. VANET-verkon toiminta perustuu siis tiedonvaihtoon yksiköiden välillä ja saadun tiedon perusteella tehtyihin päätöksiin [130]. Verkko muuttaa muotoaan sitä mukaan, kun ajoneuvot liikkuvat. VANET-yksiköltä toiselle välitetty tieto saattaa vaikuttaa kuljettajan päätöksiin ja siten myös toimenpiteisiin. Tällä tavoin verkossa välitettävällä tiedolla on mahdollista vaikuttaa verkon rakenteeseen. [125,126]

Tienvarsiyksiköt toimivat kiinteinä yhteyspisteinä ja reitittiminä ajoneuvoille. Ajoneuvojen sisäiset yksiköt kommunikoivat tienvarsiyksiköiden kanssa käyttämällä lyhyen kantaman tiedonvälitykseen tarkoitettua DSRC-radiotekniikkaa (engl. Dedicated Short Range Communication). Infrastruktuurin mahdollistaessa WLAN- ja matkapuhelinverkon käyttäminen on myös mahdollista. [125,126] Solmujen dynaamisuuden ja verkon heterogee-

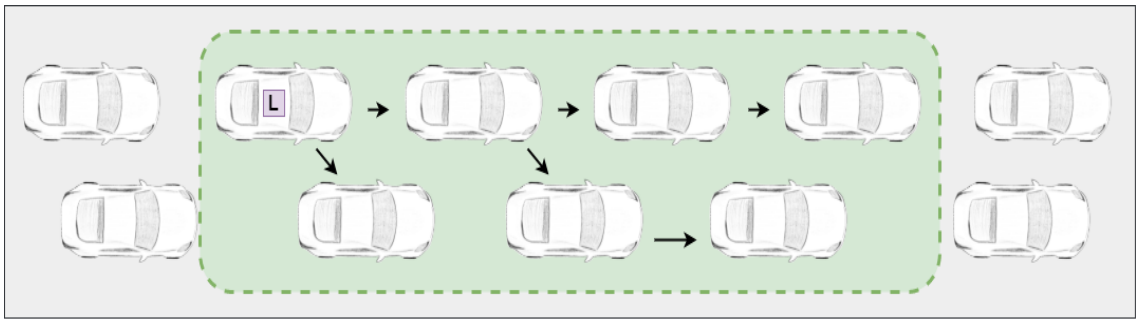
nisuuden vuoksi VANET eroaa merkittävästi muista Ad Hoc -verkoista [131]. Pilvipalveluiden, esineiden internetin ja älykkäiden liikennejärjestelmien kasvu ja kehittyminen on kiihdyttänyt VANETin kehitystä [132].



Kuva 26. *Yksinkertainen VANET-järjestelmäarkkitehtuuri, jossa ajoneuvot keskustelevat keskenään ja tienvarsiyksiköiden välityksellä internetiin. Perustuu lähteeseen [125].*

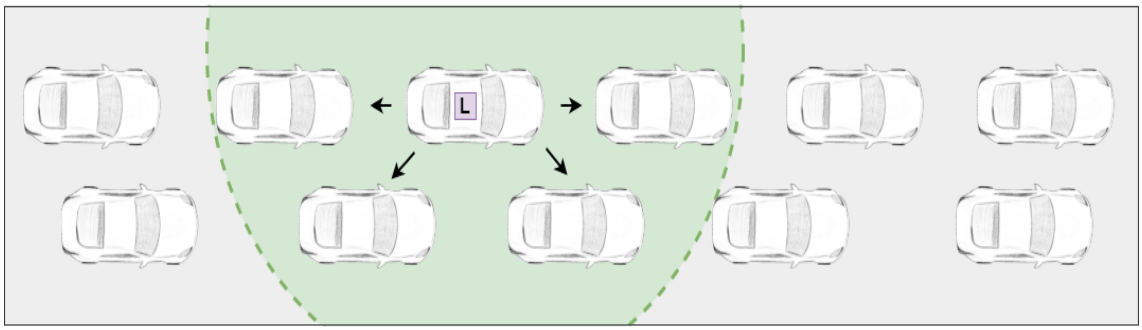
Turvallisuuden kannalta kriittiset viestit on tärkeää saada perille riittävän nopeasti, jotta laitteistolle tai kuljettajalle jää aikaa reagoida saamaansa tietoon. Schoch *et al.* [131] ovat tutkineet pakettien välityksen tehokkuutta erilaisilla kommunikointimalleilla. Tutkijat ovat päätyneet esittämään viittä sopivinta mallia, jotka ottavat huomioon noodien välisten etäisyyksien suuret vaihtelut. Nämä kommunikointimallit esitellään alla.

Sijaintiin perustuvassa lähetyksessä (engl. geobroadcast) (kuva 27) datapaketti toimitetaan lähettäjän (L) määrittämälle alueelle. Tieto datan toimitusalueesta liitetään datapakettiin. Paketti lähetetään siirtokerrosjakeluna lähimmille naapureille toimitusalueella. Kaikki alueella olevat ajoneuvot välittävät pakettia eteenpäin. Sijaintiin perustuva lähetystapa soveltuu erityisesti tiedon jakamiseen suurelle alueelle, esimerkiksi lähestyville ajoneuvoille äkillisestä tapahtumasta tiedottamiseen. [131]



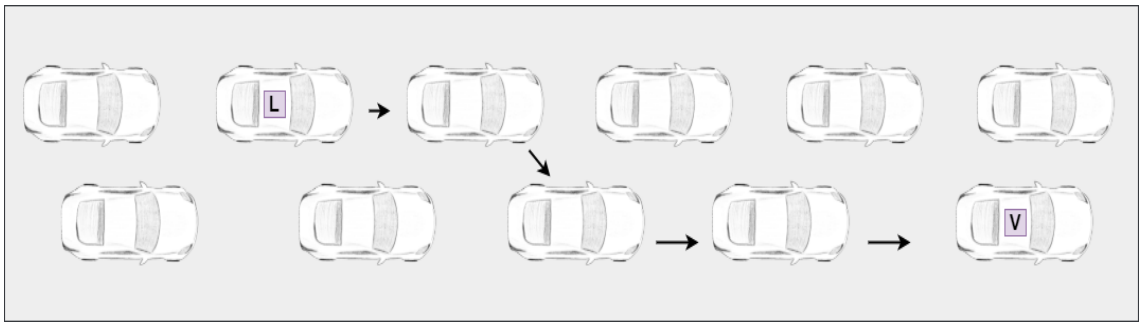
Kuva 27. *Sijaintiin perustuva paketin välitys. Perustuu lähteeseen [131].*

Majakka (engl. beaconing) kommunikointimallissa (kuva 28) pakettia lähetetään kaikille lähistön ajoneuvoille kantoetäisyydellä. Yhteys on yksihyppyinen eikä paketin tietoja yleensä välitetä eteenpäin. Tämä kommunikointimalli on tarkoitettu jatkuvaan tiedonjakoon viereisten ajoneuvojen kanssa. Yhteistoiminnan mahdollistamiseksi jaetaan ympärille tietoa kuten ajoneuvon nopeus, paikka ja suunta.



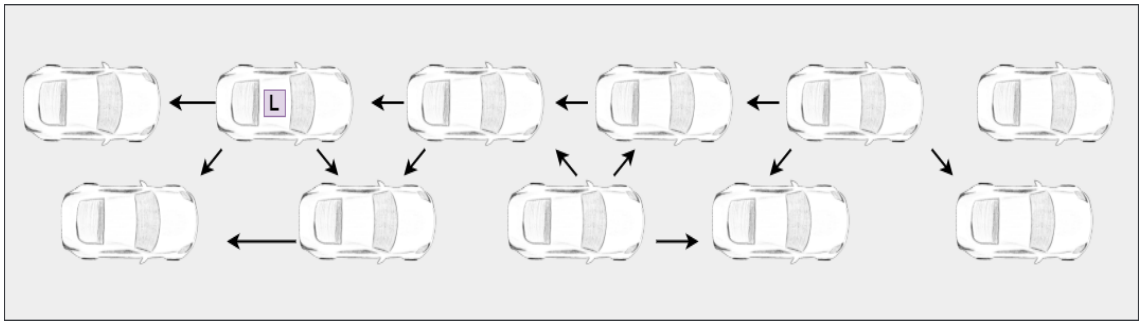
Kuva 28. *Majakkaan perustuva paketin välitys. Perustuu lähteeseen [131].*

Täsmäreitityksessä (engl. unicast routing) (kuva 29) kommunikointi koostuu joko yksittäisestä hypystä noodien välillä tai reititetystä monihyppyisestä viestinnästä kohti paketin vastaanottajaa (V). Täsmäreititys on tarkoitettu datan kuljettamiseen määränpäähänsä Ad Hoc -verkon läpi. Vastaanottava noodi voi olla ajoneuvo tai tienvarsiyksikkö.



Kuva 29. *Täsmäreititykseen perustuva paketin välitys. Perustuu lähteeseen [131].*

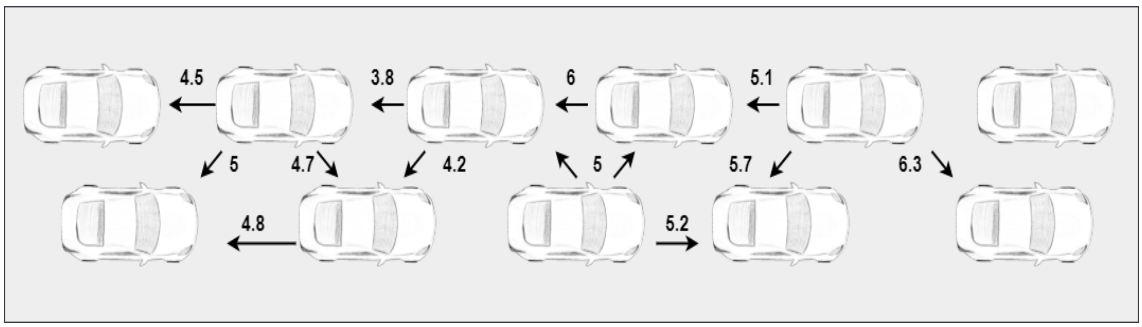
Edistynyt tiedonvälitysmalli (engl. advanced information dissemination) (kuva 30) perustuu viestin välittämiseen yksihyppyisesti, tiedon varastointiin ja useisiin eteenpäin välityksiin. Päätös, viestin välittämisestä, tapahtuu viestin mukana kulkevien parametrien avulla. Välityksen voi aikaansaada esimerkiksi uuden noodin ilmestyminen lähistölle. Edistyneen tiedonvälitysmallin tarkoituksena on jakaa tietoa tietyn ajanjakson aikana ajoneuvojen kesken. Tämä malli mahdollistaa verkon osien siltaamisen ja tiedon priorisoinnin sekä tiedon jakamisen ajoneuvoille, jotka saapuvat tilanteeseen myöhemmin.



Kuva 30. *Edistyneeseen tiedonvälitykseen perustuva paketin välitys. Perustuu lähteeseen [131].*

Tiedon koostamismallissa (engl. information aggregation) (kuva 31) keskeisenä tekijänä on tietämyskanta, joka koostuu ajoneuvon paikallisesta datasta ja muilta ajoneuvoilta kerätystä etätiedosta. Kommunikaatio voi olla yksi- tai monihyppyistä, vastaanottaja ei kuitenkaan enää välitä viestejä eteenpäin vaan data kerätään tietämyskantaan. Ajoneuvot keräävät toisiltaan vain tiedonosia tietämyskantaan, eikä kokonaisia viestejä lähetetä. Tätä kuvataan lukuarvoilla kuvassa 31. Muista kommunikointimalleista poiketen

koostamismallissa verkon noodit yhdistelevät saamiaan tietoja, eivätkä vain välitä niitä eteenpäin. Tietämyskannan ansiosta sisäinen tilannekuvan piirtäminen on mahdollista.



Kuva 31. *Tiedon koostamiseen perustuva paketin välitys. Perustuu lähteeseen [131].*

Jotta kriittiset viestit menevät perille mahdollisimman tehokkaasti, paketeilla tulee olla myös keskinäinen arvojärjestys. Turvallisuuteen vaikuttavat viestit ovat mukavuuteen ja viihteeseen verrattuna kiireellisempiä ja niiden tulee aina ohittaa muut viestit jonossa. Taulukossa 9 on esitetty VANETin esimerkkisovelluksia kategorioittain. Ominaisuudet on jaettu neljään pääkategoriaan, jotka, kriittisyysjärjestyksessä, ovat: aktiivinen turvallisuus, julkinen palvelu, parannettu ajokokemus ja kaupallinen/viihde.

Taulukko 9. *VANETin ominaisuuksia kategorioittain. Perustuu lähteeseen [131].*

	Tilanne/Tarkoitus	***Esimerkkisovellus***
I. Aktiivinen turvallisuus	1. Vaaralliset tien ominaisuudet	1. Nopeusvaroitus kurviin, 2. Varoitus matalasta sillasta, 3. Varoitus punaisen valon tai stop-merkin huomiotta jättämisestä.
	2. Poikkeukselliset liikenne- ja tieolosuhteet	1. Ajoneuvoperustainen tieolosuhdevaroitus, 2. Ympäristöperustainen tieolosuhdevaroitus, 3. Näkyvyyden vahvistus, 4. Tietyövaroitus
	3. Yhteenajon vaara	1. Kuolleen kulman varoitus, 2. Kaistanvaihtovaroitus, 3. Risteysalueen yhteenajovaroitus, 4. Nokkakolari/peräänajovaroitus, 5. Elektroniset hätäjarruvalot, 6. Raide yhteenajovaroitus, 7. Varoitus tietä ylittävistä jalankulkijoista.
	4. Lähestyvä törmäys	1. Lähestyvän törmäyksen ennalta havainnointi.
	5. Onnettomuus sattunut	1. Kolarin jälkivaroitus 2. Konerikkovaroitus 3. SOS palvelu
II. Julkinen palvelu	1. Ensiapu	1. Varoitus lähestyvästä hälytysajoneuvosta 2. HALI (Hälytysajoneuvojen etuudet liikennevaloissa) 3. Varoitus läsnä olevasta hälytysajoneuvosta
	2. Viranomaistuki	1. Elektroninen rekisterikilpi 2. Elektroninen ajokortti 3. Ajoneuvon turvallisuus tarkistus 4. Varastetun ajoneuvon jäljitys
III. Parannettu ajokokemus	1. Tehostettu ajaminen	1. Moottoritienliittymäavustin 2. Vasemmalle kääntymisavustin 3. Yhteistoiminen adaptiivinen vakionopeudensäädin 4. Yhteistoiminnallinen häikäisemätön kaukovalojärjestelmä 5. Ajoneuvon sisäinen opastus 6. Adaptiivinen ajolinjanhallinta
	2. Liikenteen sujuvoittaminen	1. Ilmoitus liikenteenohjauskeskukseen kolarista tai tienpinnan kunnosta 2. Älykäs liikennemäärän tarkkailu 3. Tehostettu liikenneopastus ja navigointi 4. Karttojen lataus/päivitys 5. Parkkiruudun paikallistamispalvelu
IV. Kaupallinen/viihde	1. Ajoneuvon huolto	1. Langaton diagnosointi 2. Ohjelmistopäivitys/flashing 3. Takaisinkutsuilmoitus 4. JIT-korjaus
	2. Mobiilipalvelut	1. Internetpalvelun toimittaminen 2. Pikaviestintä 3. Ilmoitus kiinnostavista palveluista
	3. Liiketoimintaratkaisu	1. Kalustonhallinta 2. Autovuokraus 3. Kulunvalvonta 4. Vaarallisen materiaalin kuljetuksen seuraaminen
	4. Sähköinen maksaminen	1. Tullimaksut 2. Pysäköintimaksut 3. Polttoainemaksut

6.5.2 VANETin hyödyt ja haasteet

Liikenneturvallisuuden kohentamisen lisäksi VANET tuo saataville erilaisia viihdepalveluita sekä sujuvuutta kuljettajan toimiin, esimerkiksi tarjoamalla tietoa läheisistä tankkausmahdollisuuksista tai automaattisesti hoituvat tullimaksut [129]. Aktiiviset turvallisuussovellukset ovat toivotuin ja yleisin ryhmä VANETin sovelluksista, sillä niillä on suora vaikutus liikenneturvallisuuteen. Näiden sovellusten pohjimmainen tarkoitus on tehdä ajamisesta turvallisempaa kommunikoinnin avulla. Ajoneuvo voi esimerkiksi varoittaa kuljettajaa vaarallisesta tilanteesta, pyrkiä välttämään onnettomuuden tai jopa toimia tilanteen vaatimalla tavalla, mikäli onnettomuus ei enää ole vältettävissä. Erilaisten sovellusten, toisistaan poikkeavat, vaatimukset tekevät kokonaisvaltaisen kommunikointijärjestelmän suunnittelusta haastavaa. [126]

Ajoneuvojen kommunikoidessa keskenään ja tienvarsi-infrastruktuurin kanssa on erittäin tärkeää, että viestin sisältöön voidaan luottaa. Valheellisella viestillä voi olla kohtalokkaita seurauksia, mikäli älykäs ajoneuvo viestin seurauksena esimerkiksi päättelee joutuvansa väistämättä onnettomuuteen ja kytkee tilanteeseen tarvittavat ominaisuudet käyttöön. Kuvaan 32 on koottu erilaisia tapoja vaikuttaa ajoneuvojen väliseen kommunikaatioon. [133]

Väärennyshyökkäyksessä (kuva 32 a) välikäsi kuuntelee langatonta viestintää, kerää paketteja, muokkaa niitä tarkoituksiinsa sopiviksi ja lähettää ne uudelleen verkkoon. Tämä hyökkäys vaikuttaa kaikkiin tietoturvan osa-alueisiin. [133]

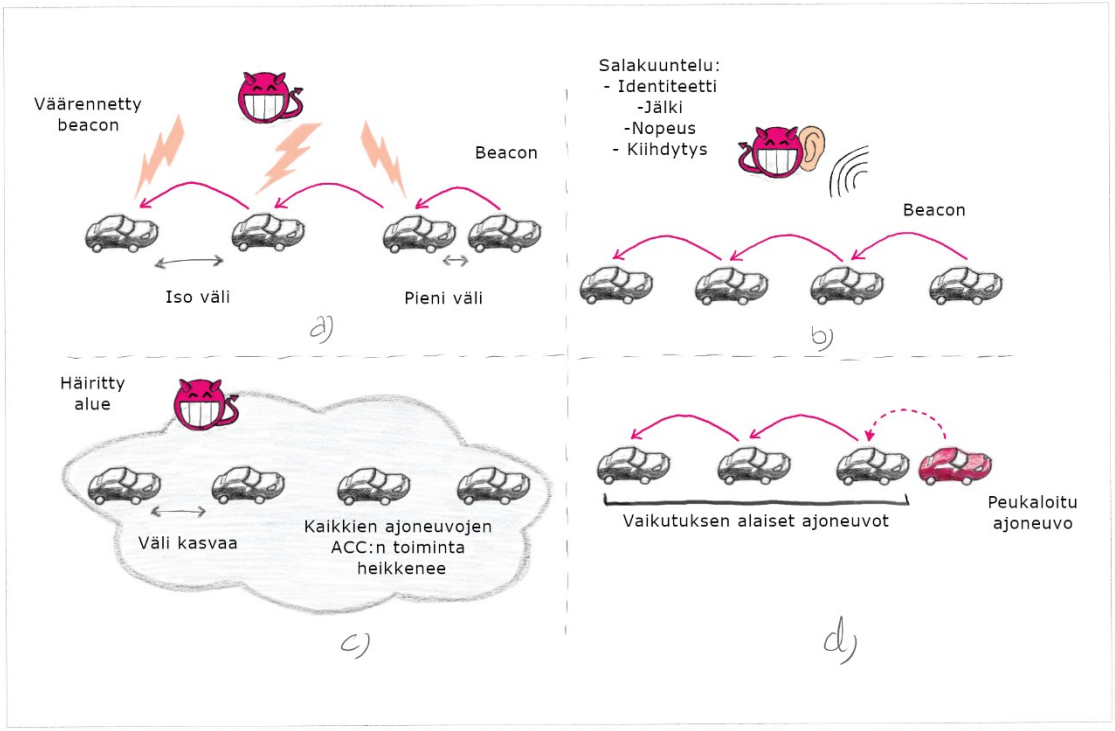
Salakuuntelulla (kuva 32 b) hyökkääjä pyrkii saamaan haltuunsa itselleen hyödyllistä dataa, kuten ajoneuvon reitin, ja käyttää näin hankittua tietoa omiin tarkoituksiinsa. Salakuuntelulla menetetään tiedon luottamuksellisuus. [133]

Radiohäirinnällä (kuva 32 c) hyökkääjä voi pienellä alueella estää ajoneuvojen välisen viestinvaihdon. Radiohäirinnällä pyritään ensisijaisesti vaikuttamaan tiedon saatavuuteen. Radiohäirintä yhdistettynä oman haitallisen viestin lähettämiseen voi aiheuttaa tilanteen, jossa vain virheellinen viesti pääsee perille. [133]

Hyökkääjä voi myös käyttää ajoneuvoa hyökkäysalustanaan peukaloimalla ajoneuvoa (kuva 32 d), jolloin ajoneuvo saadaan lähettämään valheellista dataa sisältäviä paketteja. Näin ollen paketin alkuperän varmentaminen ei riitä sen aitouden todentamiseen, sillä paketin eheys on rikottu. [133]

Vielä vuonna 2014 Engoulou *et al.* [125] mainitsivat, että kriittisten viestien perille toimittamiseen liittyvien erittäin tiukkojen aikarajojen noudattaminen ei jättänyt aikaa viestin alkuperän todentamiseen. Sittemmin tekniikka on kehittynyt nopeammaksi eikä lähettäjän identiteetin todentaminen enää ole yhtä suuri haaste. Kuitenkin viestin sisällön ja

lähettäjän autenttisuuden todentaminen lähettäjän identiteettiä paljastamatta, on yhä edelleen haasteellista [134,135].



Kuva 32. *Turvallisuuspoikkeamia ajoneuvojen välisessä kommunikaatiossa: a) väärennys, b) salakuuntelu, c) radiohäirintä ja d) peukalointi. Perustuu lähteeseen [133].*

Edellä esitettyjen hyökkäysten vaikutus on luokiteltu kuvassa 33. Liikenneturvallisuuden heikentämisen lisäksi dataan kiinni pääsevä välikäsi voi siis varastaa ajoneuvosta identiteetti- tai paikkatietoja tai aiheuttaa omistajalle rahallista tappiota. Kaupallisiin palveluihin tarkoitettujen sovellusten, kuten yllä taulukossa 9 esitettyjen automaattisten tulli- ja pysäköintimaksujen, kautta välikäden on mahdollista tehdä vilpillisiä rahansiirtoja itselleen, mikäli pyynnön aitoutta ei pystytä varmistamaan. [133]

	Väärennys	Salakuuntelu	Radiohäirintä	Peukalointi
C	✓	✓		
I	✓			✓
A	✓		✓	

Kuva 33. *Hyökkäykset luokiteltuna vaikutuksen mukaan. Pystyakselilla vaikutus, vaaka-akselilla hyökkäystavat.*

7. HAAVOITTUVUUSEROT: HENKILÖAUTOT – RASKAS KALUSTO

Tässä luvussa käsitellään haavoittuvuuksia ajoneuvotyyppikohtaisesti. Vaikka suurin osa uhista on yhteisiä sekä raskaalle kalustolle että henkilöautoille, on kummallakin ryhmällä ominaispiirteitä, jotka vaikuttavat uhkakuvaan. Pakettiautojen uhkakuvasto on lähempänä henkilöautoja ja siksi ne käsitellään samassa aliluvussa. Myös aikaisemmin esitelty VANET koskee kumpaakin ryhmää, vaikkakin sen hyödyntämismekanismit eri ajoneuvotyypeillä saattavat erota toisistaan. Luvun lopuksi, aliluvussa 7.3, pohditaan voiko jotain tiettyä ryhmää nimetä erityisen riskialttiiksi.

Ajoneuvoteollisuutta hallitsee kolme keskeistä trendiä; liitettävyys, sähköajoneuvot ja autonominen ajaminen. Näiden teknologioiden tulo kiihdyttää elektronisten ohjausjärjestelmien kehitystä sekä lisää ohjelmistojen ja digitaalisten liityntäpintojen määrää ajoneuvoissa. Tämä puolestaan lisää järjestelmien kompleksisuutta sekä kyberuhkien määrää. [136] Nopea kehitys koskee kaikkia ajoneuvotyyppejä, eikä mikään niistä ole täysin turvassa kyberhyökkäyksen riskiltä.

Autonomisten ajoneuvojen osalta esiin nousee usein henkilöliikenne. Ihmistä houkuttelee ajatus siitä, että hän voi siirtyä omassa autossaan matkustajaksi. Raskaan kaluston kohdalla kehitystä jouduttaa autonomian ja saattueajon yhdistämisen tuomat edut.

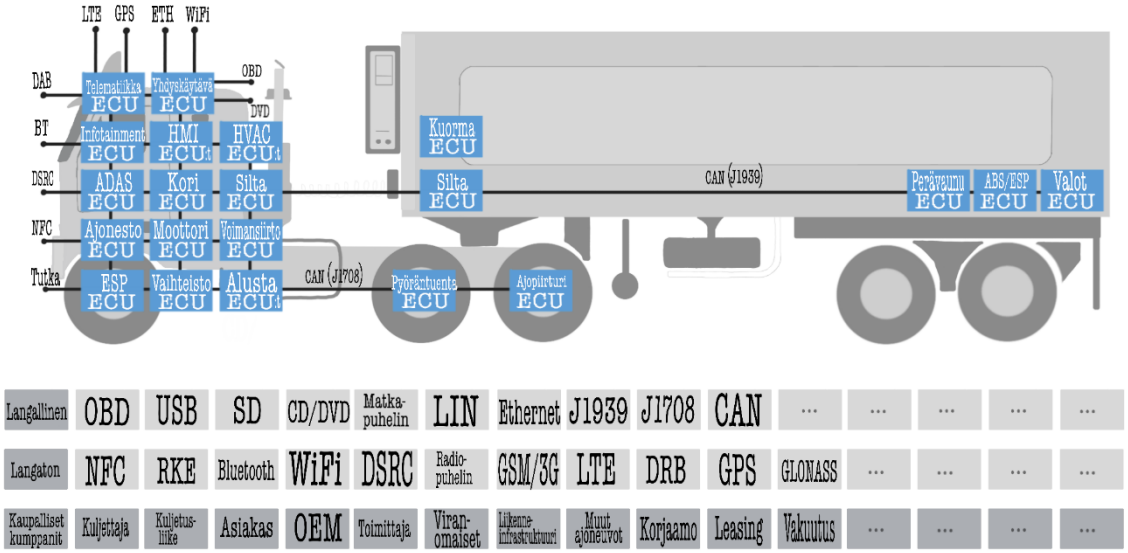
7.1 Raskaat ajoneuvot

Henkilöautojen tavoin myös raskas kalusto toimii kasvavassa määrin ohjelmistojen varassa, joka lisää kyberhyökkäyksien riskiä. Edelleen raskasta kalustoa koskevat myös itseohjautuvuuden lisääntyminen ja itsenäinen kommunikointi ympäristön kanssa. [136] Suurikokoisina raskaat ajoneuvot ovat suuremmassa vaarassa joutua välineeksi esimerkiksi terroristiseen toimintaan.

Erityisesti kuorma-autojen osalta kyberturvallisuus on yhtä merkittävä tekijä kuin perinteinen liikenneturvallisuus. Kuorma-autoissa käytetään henkilöautoihin verrattuna enemmän kompleksisia ja ohjelmallisesti ohjattuja ominaisuuksia, kuten esimerkiksi kuljetuskaluston seuranta. Samalla tavoin kuorma-autojen pitää tukea henkilöautoja laajempaa valikoimaa liityntämuotoja datan siirtämiseksi. Kuorma-autojen ominaispiirteisiin kuuluu myös se, että ne muodostavat keskenään homogeenisen ja varsin tarkkaan standardoidun ryhmän, joka mahdollistaa helpomman hyökkäysten suunnittelun. Sen lisäksi,

että ne ovat lähes vuorokauden ympäri liikkeellä ja toimivat usein laajalla maantieteellisellä alueella, hyökkäyksen vaikutus yksittäiseen kuorma-autoon on suurempi verrattuna vastaavaan henkilöautoon kohdistuvaan hyökkäykseen. Edellä mainituista syistä, kuorma-autot ovat alttiimpia kyberhyökkäykselle kuin henkilöautot. [136]

Raskaan kaluston sisäinen elektroninen arkkitehtuuri on samankaltainen kuin henkilöautoilla. Se koostuu noin 50 elektronisesta ohjausyksiköstä, jotka kommunikoivat toistensa kanssa ajoneuvon tiedonsiirtomoduulien, kuten CAN-väylän, välityksellä. Elektronisen arkkitehtuurin perusperiaatteita on esitelty kuvassa 34.



Kuva 34. *Tyypillinen kuorma-auton elektroninen arkkitehtuuri. Perustuu lähteeseen [136].*

7.2 Henkilö- ja pakettiautot

Pakettiautoihin saa nykyään lähes kaikki samat ominaisuudet kuin henkilöautoihin, joskin osan henkilöautoissa jo lähtökohtaisesti olevista ominaisuuksista joutuu pakettiautoon hankkimaan lisävarusteena. Tästä varustelun laajuudesta johtuen myös pakettiautot kärsivät samoista kyberriskeistä kuin henkilöautot.

Sähköautojen yleistyminen nostaa niiden merkitystä haavoittuvana kohteena. Sähköautoihin pätevät samat ongelmat kuin muihin moderneihin ajoneuvoihin, mutta yhteisten vaaranpaikkojen lisäksi sähköautoille virrankulutus on herkkä paikka [56]. Sähköautot ovat siis haavoittuvampia energiankulutukseen vaikuttaville hyökkäyksille, kuten ilmastoinnin tehon säätämiselle. Siinä missä polttomoottoriajoneuvoissa ilmastoinnin voimakas puhallus voi olla epämiellyttävää, sähköauton kohdalla sillä on lisäksi suora vaikutus jäljellä olevaan toimintasäteeseen ennen seuraavaa latausta.

Henkilö- ja pakettiautojen osalta riskinä korostuu erilaisten ajomukavuuden parantamiseen tähtäävien ominaisuuksien lisääntyminen ajoneuvoissa. Autoissa vietetään paljon aikaa ja silloin halutaan käyttää samoja palveluita kuin muissakin tilanteissa. Mukavuuspalvelut ovat hyökkääjän kannalta hyvä kohde, sillä uusien sovellusten turvallisuudesta ei aina ymmärretä varmistua, kun halutaan ominaisuuksia käyttöön omaan ajoneuvoon. Osa sovelluksista on huonosti suojattuja, jotkut jopa itsessään vahingollisia. Vaaraa lisää se, etteivät sovellusten käyttäjät tiedosta niissä piileviä riskejä.

Yhteiskäyttöisten ajoneuvojen tuomat riskit painottuvat henkilö- ja pakettiautoihin. Yhteiskäyttöisiä ajoneuvoja on jo paljon käytössä ja niiden määrä tulee jatkossa lisääntymään. Autonomiset ajoneuvot tulevat viimeistään kasvattamaan yhteiskäytön suosiota, kun ajoneuvon voi tilata kotiovelle silloin kun on tarve.

7.3 Riskiryhmä – onko sitä?

Koska ajoneuvoihin kohdistetut hyökkäykset eivät ole vielä yleisiä, on helppo tuudittautua ajatukseen, ettei vaaraa itselle ole. Tavallisen tielläliikkujan näkökulmasta varmasti myös vaikuttaa siltä, ettei henkilökohtaisesti ole tarpeeksi kiinnostava joutuakseen hyökkäyksen kohteeksi. Osittain tässä ajattelussa voi olla jopa perää, todennäköisyys niin sanotulla tavallisella ihmisellä joutua hyökkääjän suoraan valitsemaksi kohteeksi, lienee pieni. Se ei valitettavasti kuitenkaan poista mahdollisuutta joutua kohteeksi. Valinnan ei tarvitse kohdistua tiettyyn henkilöön tai edes tiettyyn ajoneuvoon. Hyökkääjä saattaa valita kohteen satunnaisesti, joidenkin automallien joukosta, joihin tietää hyökkäyksensä tehoavan. Sen lisäksi hyökkäyksen vaikutukset voivat ulottua ulkopuolisiin, esimerkiksi jalankulkijoihin kohteen lähellä.

Motiivina saattaa olla yksinkertaisesti kiusanteko, halu kokeilla ja näyttää kykyjään tai aiheuttaa vaaratilanne. Kiristyshyökkäyksen kohdalla motiivina toimii raha, samalla tavalla kuin ihmisten henkilökohtaisiin tietokoneisiin suunnatuissa hyökkäyksissä. Kohteen henkilöllisyydellä ei hyökkääjän kannalta ole välttämättä merkitystä.

Kalliit tai muuten erikoiset autot herättävät erityistä kiinnostusta. Kyberhyökkäys nousee esiin vaihtoehtona myös autovarkauksien osalta, erityisesti kun avaimeton käynnistys on yleistynyt huomattavasti. Vaikka kalliit ja erikoiset autot ovat houkuttelevia myös autovarkaiden silmissä, eniten varastetaan kuitenkin edelleen tavallisia, keskihintaisia, autoja. Vuonna 2018 varastetuimpia autoja, Yhdysvalloissa, olivat Honda Civik ja Accord, sekä Ford PickUp [137].

Erityisesti kuorma-autojen kohdalla korostuu itse auton arvo kohteeksi joutumisen riskiä nostavana tekijänä. Sen lisäksi kuorma-auton kuorma voi toimia arvonsa tai vaarallisuutensa vuoksi hyökkäyksen motiivina. [136] Raskaiden ajoneuvojen painon mahdollistama tuhovoima on myös tekijä, joka nostaa niiden kohteeksi päätymisen riskiä.

Vakoilutarkoituksessa hyökkäyksellä voidaan selvittää ajoneuvon kulkureittejä, pysähdyspaikkoja ja muita mahdollisesti kiinnostavia tietoja ajoneuvon liikkeistä ja toiminnasta. Jatkamalla vakoilua pidemmän aikaa voidaan selvittää rutiineja, oli kiinnostuksen kohteena sitten henkilö tai itse seurattava ajoneuvo.

Sähköajoneuvojen osalta nousee esiin myös mahdollisuus käyttää ajoneuvoa välineenä sähköverkkoa kohtaan suunnatussa hyökkäyksessä. Lähes kaiken toimiessa nykypäivänä sähköllä, sähköverkosta on tullut entistä kiinnostavampi ja todennäköisempi kohde. Hyökkäys sähköverkkoa vastaan voi vaikuttaa koko yhteiskunnan toimintakykyyn. Sähköajoneuvot ovat potentiaalinen alusta tällaisen hyökkäyksen toteuttamiselle. Modernit autot sisältävät suuren määrän internet-yhteyttä hyödyntäviä toimintoja, jotka altistavat ajoneuvon hyökkäyksille. Lisäksi sähköajoneuvojen kytkeytyessä sähköverkkoon, aukeaa yhteys myös siihen suuntaan. [138]

Sähköajoneuvojen laitteistojen, sovellusten ja viestintäjärjestelmien suunnittelussa ja toteutuksessa on todettu haavoittuvuuksia. Monissa tapauksissa sovellusten oletussalasanat ovat helposti pääteltävissä, mikä avaa hyökkääjille helpon pääsyn laitteiden hallintaan ja tileihin. Tämä ongelma ei toki koske pelkästään sähköajoneuvoja. Lukuisat heikkoudet ja käyttäjät johtavat huonoon turvallisuuteen. Salaamattoman tiedon siirtäminen mahdollistaa tiedon urkinnan. Myös sosiaalinen tiedustelu kohdistettuna ajoneuvotehtaan työntekijöihin on mahdollista. [138]

8. VASTATOIMET

Ajoneuvojen haavoittuvuuksien korjaaminen on suurelta osin ajoneuvo- ja komponenttivalmistajien käsissä. Suureen määrään koodia mahtuu kuitenkin paljon haavoittuvuuksia, eikä valmistaja ole kaikista tietoinen. Jonkin haavoittuvuuden korjaaminen voi puolestaan altistaa uudelle haavoittuvuudelle, jota ei välttämättä huomata korjausta tehtäessä. Modernit internet-yhteydelliset ajoneuvot ovat haavoittuvuutensa lisäksi myös nopeasti ohjelmistokorjausten tavoitettavissa. Ajoneuvoa ei välttämättä tarvitse edes viedä korjaamolle, vaan korjaustiedosto voidaan toimittaa verkossa.

Haavoittuvuuksien etsiminen ja niistä valmistajalle raportoiminen on yksi merkittävimmistä asioista, jolla ajoneuvojen kyberturvallisuutta voidaan parantaa. Tämä perustuu kuitenkin suurilta osin vapaaehtoisuuteen. Osa autonvalmistajista on myös lanseerannut kampanjoita, jossa merkittävän haavoittuvuuden löytämisestä voi saada palkkion [139]. Lisäksi olisi toivottavaa, että valmistajat suhtautuvat löydettyihin haavoittuvuuksiin riittävällä vakavuudella.

Mahdolliset vastatoimet voidaan jakaa kahteen kategoriaan, käyttäjien omiin toimiin ja järjestelmän kovennuksiin. Käyttäjien mahdollisuus vaikuttaa oman ajoneuvonsa kyberturvallisuuteen ei poista haavoittuvuuksia, mutta tekee tilanteesta lievästi siedettävämmän. Toiseen kategoriaan menee järjestelmään tehtävät kovennukset. Nämä ovat niitä toimia, joilla tilanteeseen voitaisiin oikeasti vaikuttaa. Korjattavaa on kuitenkin paljon ja sitä muodostuu jatkuvasti lisää. Seuraaviin alilukuihin 8.1 ja 8.2 on kerätty niin oman ajattelun tuotoksia, kuin lähdemateriaaleista löytyneitä ratkaisuja. Vastatoimina tässä luvussa mainitut asiat eivät ole ainoita eivätkä riittäviä. Täydellistä luetteloa ei ole olemassa.

8.1 Omat toimet

Tässä esitellään muutamia käyttäjän kannalta yksinkertaisia keinoja pienentää oman ajoneuvon haavoittuvuutta. Tärkein vaihe on tiedostaa, että ajoneuvot ovat tietokoneita ja näin ollen alttiita kyberhyökkäyksille. Toinen tärkeä asia tiedostaa on se, että kaikki eivät ymmärrä ajoneuvojen alttiutta kyberhyökkäyksille. Tämä johtaa siihen, että liikenteessä on lukuisia altistuneita ajoneuvoja.

Ajoneuvon diagnostiikan seuraaminen kotona on mielenkiintoista ja mahdollisesti myös hyödyllistä. Myös ajoneuvon itsekoodaaminen on vähintään taloudellisesti houkuttelevaa. On kuitenkin äärimmäisen tärkeää tietää mitä tekee, sekä mitä laitteita ja ohjelmia

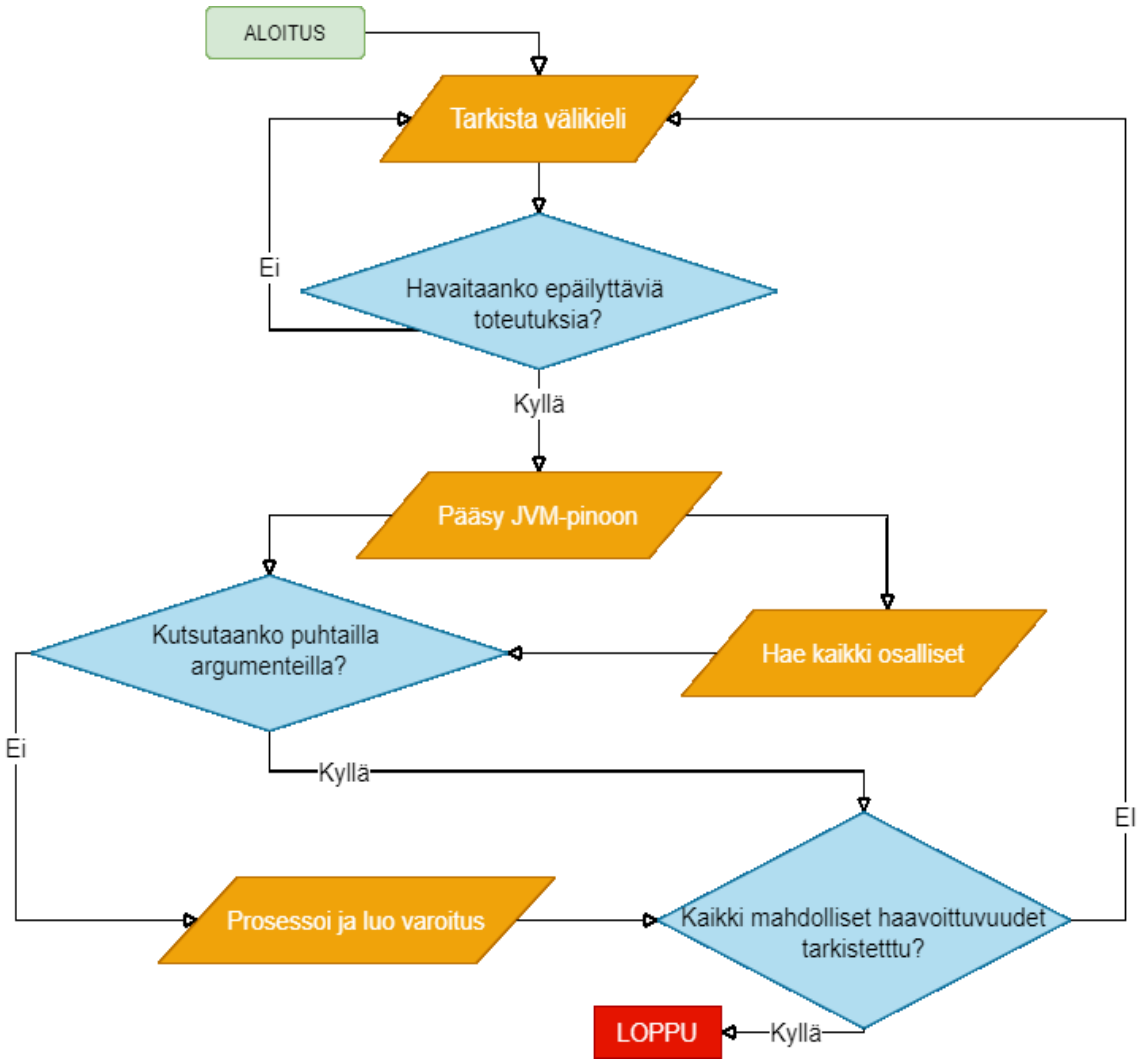
tähän käyttää. Jos liittää tietokoneen ajoneuvoon, olisi syytä varmistua tietokoneen puhtaudesta. Paras vaihtoehto olisi, jos kyseistä tietokonetta ei koskaan kytkettäisi muihin verkkoihin. Koodauksia tehdessä pitää myös olla varma siitä, että tietää mitä mikäkin muokkaus aiheuttaa ajoneuvossa. Varoivaisuutta tulee noudattaa myös itsediagnostiikkasovellusten kanssa, ettei vahingossa käytä haittakoodia sisältäviä sovelluksia. OBD-sovittimen jatkuvan ajoneuvossa kiinni pitämisen tarvetta on syytä harkita, jotta ylimääräisiä langattomia rajapintoja voidaan välttää.

Matkapuhelinten ja massamuistilaitteiden kanssa on tärkeää olla tarkkana. Ennen ajoneuvoon kytkemistä on syytä tarkastaa, ettei massamuisti sisällä haittaohjelmia. Tällä tavoin voi pienentää riskiä, että esimerkiksi navigaattoria päivittäessä, tule asentaneeksi haittaohjelmaa infotainment-järjestelmään. Valitettavasti virustorjuntaohjelmat eivät kuitenkaan ole aukottomia. Matkapuhelimen tietoturvasta huolehtimiselle on toki useita perusteita, mutta erityisen tärkeää se on, mikäli puhelin kytketään ajoneuvoon.

Mandal *et.al.* kuvaavat artikkelissaan [95] tekemäänsä tutkimusta OBD-II ja Google Play -kaupasta infotainment-järjestelmään ladattavien sovellusten haavoittuvuuksista. Tuloksista kävi ilmi, että testatuista sovelluksista 60% on potentiaalisesti haavoittuvia. Käytetty analysointityökalu ei korjaa haavoittuvuuksia, eikä suoraan tarjoa ratkaisuja niiden korjaamiseksi. Tällaista työkalua voisi kuitenkin käyttää haavoittuvien kohteiden etsimiseen. [95]

Kuvaan 35 on piirretty Mandal *et.al.* artikkelissa [95] esitetyn Android Auto -analyysin prosessikaavio. Ensimmäisenä tarkastetaan välikieli, jota käytetään korkeamman tason ohjelmakoodin lähdekielen ja lopullisen konekielen välillä ohjelman tulkinnassa. Jos epäilyttäviä toteutuksia välikielessä havaitaan, tarkastetaan käyttääkö se Java virtuaalikonetta (JVM, engl. Java Virtual Machine). Välikielen käyttäessä JVM-pinoa tarkastetaan

kaikkien osallisten argumentit. Kun argumentit ovat puhtaita ja kaikki haavoittuvuudet on tarkastettu, analyysi päättyy.

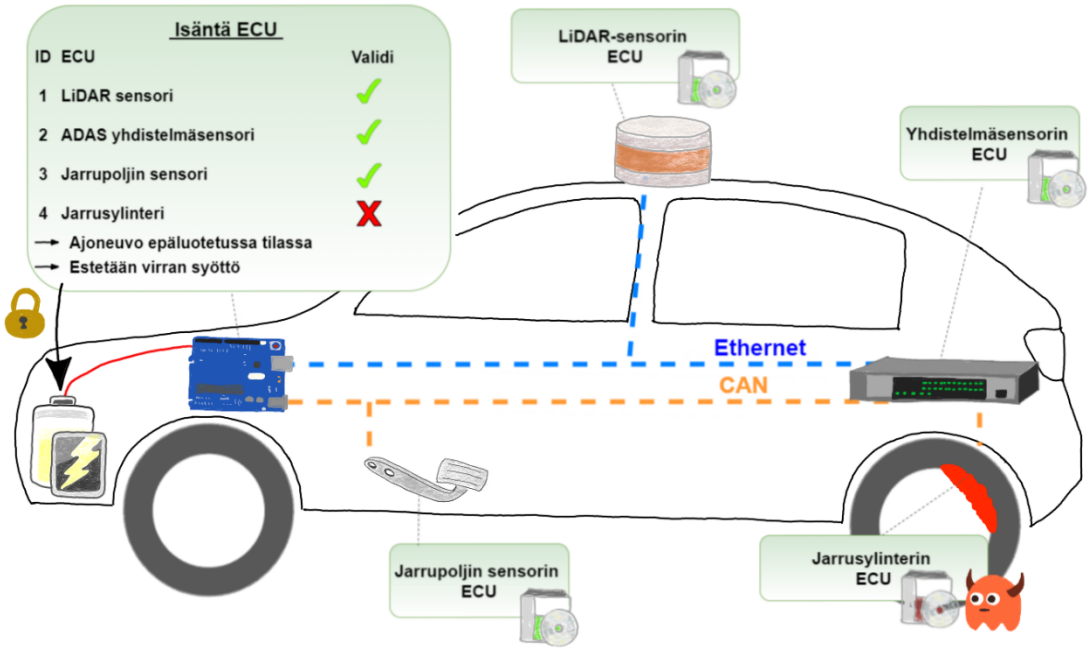


Kuva 35. *Android Auto -analyysi. Perustuu lähteeseen [95].*

PKES-järjestelmän haavoittuvuuksia vastaan käyttäjä voi suojautua pitämällä avainta metallisessa suojakotelossa, aina kun avain ei ole aktiivisesti käytössä. Tällä tavoin avaimen ympärille muodostuu Faradayn häkki, joka suojaa avainta releointihyökkäykseltä. Toinen yksinkertainen suojausmekanismi on poistaa UHF-radiolle virtaa antava paristo avaimesta. Näiden molempien menetelmien huonona puolena on se, että PKES-järjestelmän käyttö estyy. Molemmissa tapauksissa käyttäjältä vaaditaan toimenpiteitä lukituksen avaamiseen. [124] Näitä keinoja kevyempi vaihtoehto on käyttää avaimen kaukosäätimen painiketta, kun auto lukitaan paikoissa, joissa hyökkäykselle on suurempi todennäköisyys, esimerkiksi suuret markettien parkkipaikat. Osa ajoneuvoista, joissa on valittavana kaukosäätimellä ja oven painikkeella lukitus, estää lukituksen avaamisen oven painikkeesta, mikäli ovet on lukittu kaukosäätimellä.

8.2 Järjestelmän kovennukset

Kohnhäuser *et al.* esittelevät julkaisussaan [140] menetelmän, jossa luotettu elektroninen ohjausyksikkö varmentaa kaikkien turvallisuuskriittisten ohjausyksiköiden eheyden. Mikäli epäluotettava tila huomataan, moottoria ei käynnistetä. Modernien ajoneuvojen ollessa heterogeenisia järjestelmien järjestelmiä Kohnhäuser *et al.* menetelmässä käytetään kahta eri todentamistekniikkaa. Näiden avulla sekä yksinkertaisten ohjausyksiöiden, kuten sensoreiden ja toimilaitteiden, että kompleksisempien ohjausyksiköiden, kuten yhdistelmäsensorien todentaminen hoidetaan. Tätä menetelmää kuvataan kuvassa 36.



Kuva 36. *Luotettu isäntä elektroninen ohjausyksikkö (ECU). Tämän menetelmän tapauksessa isäntä ECU on aina luotettu. Havaitessaan jarrusylinterin ohjausyksikössä poikkeuksen isäntä ECU estää moottorin käynnistyksen. Perustuu lähteeseen [140].*

Yritys OnBoard Security® on kehittänyt Auto Care -yhdistyksen tuella standardin turvalliseen pääsyyn ajoneuvon verkkoon. Tämä standardi, ISO 21177 [141], voisi mahdollisesti poistaa tarpeen haavoittuvan OBD-II:n käytölle. Uusi standardi on kehitetty vastaamaan älykkään liikennejärjestelmän kyberturvallisuusvaatimuksiin, tarkoituksenaan varmistaa viestin lähettäjän todennus ja luotettujen laitteiden välillä tapahtuvien toimintojen luottamuksellisuus ja eheys. Sen turvallinen kommunikointi perustuu kaksisuuntaiseen todennukseen vertaissovellusprosessien välillä, käyttäen rooli- tai attribuuttipohjaista pääsynhallintaa. [142]

Yhdysvaltain liittovaltion liikenneturvallisuusvirasto NHTSA (engl. National Highway Traffic Safety Administration) etsii ratkaisuja ajoneuvon elektronisen arkkitehtuurin suojaamiseksi kyberuhilta. NHTSA ohjeistaa ajoneuvoteollisuutta käyttämään kerrostettua lähestymistapaa ratkaisuksi ajoneuvoihin kohdistuvien hyökkäysten onnistumisen minimointiin ja mahdollisen luvattoman pääsyn seurausten lieventämiseen. Ajoneuvoteollisuudessa tulisi täten noudattaa yhdysvaltalaisen tietoturvastandardointijärjestö NIST:n (engl. National Institute of Standards and Technology) dokumentoimaa kyberturvallisuuden viitekehystä [143] ja rakentaa sen avulla kerrostettu suojaus ajoneuvoille. [144]

Kerrostetun turvallisuusmetodin neljä pääkohtaa ovat: 1) ennaltaehkäisevät toimet, 2) reaaliaikainen tunkeutumisenhavaitseminen, 3) reaaliaikainen vaste ja 4) mekanismien arviointi. Ennaltaehkäiseväksi toimeksi luokitellaan esimerkiksi turvallisuuskriittisten toimintojen eristäminen omaksi osakseen verkossa. Tunkeutumisenhavaitsemisjärjestelmältä vaaditaan jatkuvaa potentiaalisten järjestelmään tunkeutumisten seurantaa. Reaaliaikaisen vasteen tarkoituksena on mahdollistaa, että kuljettaja pystyy säilyttämään ajoneuvon hallinnan myös onnistuneen hyökkäyksen aikana. Mekanismien toimivuutta arvioidaan tutkimalla kumppaneilta saatua dataa tilanteista, joissa hyökkäys on onnistunut ennakkotoimista huolimatta. [57]

9. TULOKSET

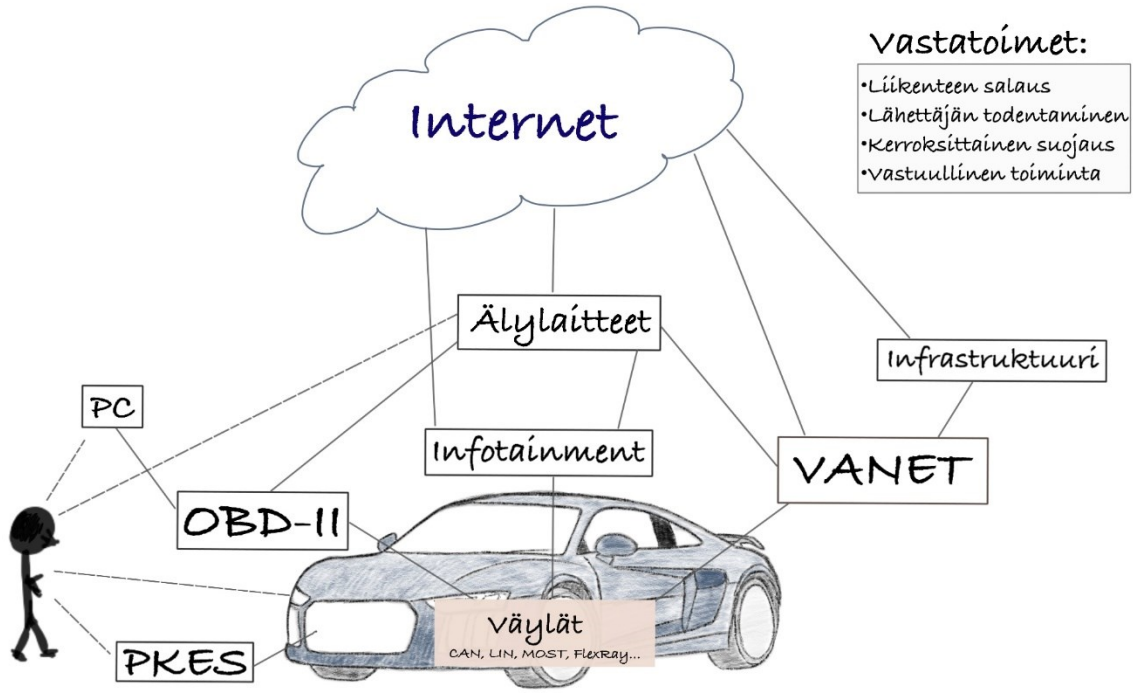
Tässä luvussa esitellään lyhyesti tutkimuksen tulokset. Aluksi käydään läpi merkittävimmät haavoittuvat kohteet ja mahdollisia hyökkäysreittejä. Lopuksi listataan keinoja, joilla hyökkäykselle altistumisen riskiä voidaan pienentää.

Merkittävimpänä suojattavana kohteena voidaan pitää ajoneuvon väylistä ja ohjausyksiköistä koostuvaa sisäistä verkkoa. Väylien kriittisyys kohteena korostuu, koska niitä pitkin kulkee lähes kaikki ajoneuvon toimintaan vaikuttava informaatio ohjausyksiköiden välillä. Väylien määrä vaihtelee ajoneuvomallien ja -tyyppien kesken, mutta toimintaperiaate on kaikissa samankaltainen.

Vaikuttaakseen ajoneuvon toimintaan hyökkääjä tarvitsee pääsyn ajoneuvon väyliin, kuten CAN- tai LIN-väyliin. Moderneissa ajoneuvoissa rajapintoja on ajoneuvojen liitettävyydestä johtuen useita. Ilmeisemmän riskin aiheuttaa VANET, joka on yhteydessä niin ajoneuvoon, infrastruktuuriin, muihin ajoneuvoihin, älylaitteisiin kuin internetiin. VANETin toimintaperiaatteesta johtuen viestin välitys on myös aikakriittistä. Myös infotainment-järjestelmä ja OBD-II-liitin voivat toimia reitteinä, erilaisten älylaitteiden kautta, ajoneuvon verkkoon. Avaimeton avaus ja käynnistys -ominaisuutta vastaan hyökkäämällä tai käyttäjän huolimattomuutta hyödyntämällä, voi hyökkääjä saada itselleen fyysisen pääsyn ajoneuvoon.

Ajoneuvojen alttiutta kyberhyökkäyksille voidaan pientään salaamalla ajoneuvojen sisäinen sekä ajoneuvojen ja niiden ympäristön välinen tietoliikenne. Tiedon luottamuksellisuuden ja eheyden varmistamisen lisäksi, viestin lähettäjän todentamisella on suuri vaikutus ajoneuvojen kyberturvaan. Kerroksittaisella suojalla voidaan pienentää haitallisen datan todennäköisyyttä päätyä kohteeseensa, vaikka jonkin kerroksen suojaus pettäisi. Käyttäjä itse voi pienentää oman ajoneuvonsa riskiä joutua hyökkäyksen kohteeksi toimimalla vastuullisesti ja käyttämällä harkintaa kytkiessään älylaitteita ajoneuvoonsa.

Edellä esitettyjä haavoittuvia yhteyksiä ajoneuvon sisäisen verkon ja ympäristön välillä on havainnollistettu kuvassa 37. Kuvaan on lisäksi listattu mainitut vastatoimet.



Kuva 37. *Potentiaalisia haavoittuvia yhteyksiä ajoneuvon ja ympäristön välillä sekä vastatoimia kyberuhkia vastaan.*

Kuvassa 38 on listattu tässä työssä käsitellyt kirjallisuudesta löytyneet hyökkäystavat. Lisäksi kuvassa on ehdotettu parhaaksi koettua keinoa torjua kyseinen hyökkäys. Radiohäirinnälle ei ole merkitty torjuntakeinoa, sillä yksiselitteistä ratkaisua ei ole.

Pääosa hyökkäyksistä voidaan toteuttaa monella tavalla ja siksi myös torjuntaan löytyy eri tapoja. Merkittävimmän lisän turvallisuuteen toisi ajoneuvon sisäisen dataliikenteen salaaminen ja sanomien lähettäjän todentaminen. Nämä yhdistettynä käyttäjän vastuulliseen toimintaan, jolla voidaan pienentää riskiä ajoneuvon joutumiselle hyökkäyksen

kohteeksi, muodostavat jo itsessään kerrostettua suojausta. Edellä mainittujen lisäksi tunkeutumisen havaitsemis- ja estojärjärjestelmät parantavat turvallisuutta merkittävästi.

<table>
<tr><th>Luottamuksellisuus</th><th>Saatavuus</th><th>Eheys</th><th>Ensisijainen torjuntakeino</th></tr>
<tr><td>Salakuuntelu:
Hyökkääjä pyrkii saamaan haltuunsa hyödyllistä dataa</td><td></td><td></td><td>Salaus</td></tr>
<tr><td colspan="2">Kiristyshaittaohjelma:
Salaa tiedot, vaatii maksua vastineeksi salauksen purkamisesta.</td><td></td><td>Lähettäjän todentaminen</td></tr>
<tr><td colspan="3">Impersonaatiohyökkäys:
Hyökkääjä esiintyy oikeutettuna toimijana ja syöttää dataa järjestelmään.</td><td>Lähettäjän todentaminen</td></tr>
<tr><td colspan="3">Väärennyshyökkäys:
Hyökkääjä kuuntelee viestintää, kerää paketteja ja muokkaa niitä.</td><td>Salaus / Käyttäjän todentaminen</td></tr>
<tr><td colspan="3">Releointihyökkäys:
Signaalia välitetään kauemmas kuin se itsenäisesti kantaisi.</td><td>Käyttäjän toimet</td></tr>
<tr><td></td><td>Radiohäirintä:
Viestiliikennettä häiritään lähettämällä taajuudelle muuta dataa.</td><td></td><td>-</td></tr>
<tr><td></td><td colspan="2">Toistohyökkäys:
Hyökkääjä ujuttaa dataliikenteeseen sanoman, joka on jo aimmin lähetetty.</td><td>Lähettäjän todentaminen</td></tr>
</table>

Kuva 38. *Tutkimuksessa esiin nousseet hyökkäystavat ja niiden ensisijaiset torjuntakeinot.*

Tutkimuksessa selvisi, että ajoneuvot sisältävät useita haavoittuvia komponentteja ja kyberhyökkäyksen seurausten vakavuuksissa on suurta vaihtelua. Lisäksi tutkimus osoitti, että suojautumiskeinoja kyberuhkia vastaan on jo olemassa ja uusia menetelmiä kehitetään parantamaan turvallisuutta. Kuitenkin myös uusia haavoittuvuuksia aukeaa jatkuvasti, eikä näin ollen kaiken kattavaa listaa turvallisuustoimista voida tehdä.

10. YHTEENVETO

Kyberturvallisuus on ajoneuvojen osalta liikkuva maali, johon hakkerit etsivät jatkuvasti uusia keinoja hyödyntää haavoittuvuuksia. Ajoneuvovalmistajien tulee olla varovaisia ja valmiita taistelemaan hakkereita vastaan.

Viimeisen kymmenen vuoden aikana ajoneuvojen kyberturvallisuutta on tutkittu runsaasti. Enimmäkseen tutkimukset ovat kuitenkin keskittyneet vain johonkin ajoneuvon haavoittuvaan osa-alueeseen. Erityisesti laajasti ajoneuvojen kyberturvaa käsittelevät tutkimukset ovat lähes poikkeuksetta englanninkielisiä. Parilta viime vuodelta tällaisia tutkimuksia löytyi alle kymmenen.

Ajoneuvojen verkon perustan luovat kommunikointijärjestelmät on suunniteltu alun perin täysin erilaiseen tilanteeseen. Tästä syystä ne eivät ole sellaisenaan turvallisia nykyhetken vaatimuksiin nähden. CAN-väylän tapa kommunikoida broadcast-jakelulla ja väylän heikkoudet salauksen, autentikoinnin ja pääsynhallinnan suhteen altistavat sen vaaroille.

Uudet tavat käyttää ajoneuvoja valtaavat alaa. Yhteiskäyttöiset ajoneuvot yleistyvät ja autonomisia ajoneuvoja odotetaan entistä laajempaan käyttöön. Hybridi- ja sähköautojen osuus autoista kasvaa. Ajoneuvojen täytyy kommunikoida ympäristön ja toistensa kanssa, jotta kaikki kehitetyt turvallisuus-, viihde- ja mukavuusominaisuudet saadaan käyttöön. Ajoneuvoilta odotetaan nykyään paljon enemmän kuin kulkuneuvona toimimista. Odotukset ajoneuvojen tarjoamiin viestintä- ja viihdepalveluihin kasvavat, kun ihmiset viettävät paljon aikaa autoissaan. Sen seurauksena autot halutaan voida liittää matkapuhelimiin ja muihin älylaitteisiin.

Uudet ominaisuudet lisäävät ajoneuvojen turvallisuutta ja viihtyvyyttä. Liikenneinfrastruktuurin palveluilla on myös selviä liikennettä sujuvoittavia vaikutuksia. Kaikkien näiden palveluiden integroimisessa piilee kuitenkin riski, sillä jokainen uusi yhteys on uusi potentiaalinen haavoittuvuus. Ajoneuvojen kirjosta ja laajasta ikähaarukasta johtuen liikenteessä on eritasoisia ajoneuvoja, joissa on samoja ja myös toisistaan poikkeavia haavoittuvuuksia.

Terroristisen toiminnan potentiaalisimpina kohteina vaikuttaisivat olevan raskas kalusto ja sähköajoneuvot. Raskaan kaluston kohdalla riski perustuu ajoneuvon suureen kokoon tai mahdollisesti vaaralliseen kuormaan. Sähköajoneuvot taas nousevat esiin potentiaalisina työkaluina sähköverkon lamaannuttamiseen. Kaiken kaikkiaan haavoittuvuudet kriittisissä järjestelmissä tulisi tunnistaa, ennen kuin hyökkääjät ehtivät niitä hyödyntää.

Ilman terroristisia tavoitteita toimiville hakkereille on paljon houkuttelevia kohteita. Kiusanteko ja omien kykyjen todistaminen ovat aina kuuluneet hakkereiden motiivirepertuaariin. Näihin modernit ajoneuvot tarjoavat mielenkiintoisen alustan. Kiristyshaittaohjelmilla hakkerit voivat tavoitella suoraa rahallista hyötyä. Ajoneuvojen ja käyttäjien tietojen urkkiminen ja niiden edelleen välittäminen on myös mahdollinen ansaintalogiikka hakkerille. Ajoneuvon liikkeiden, rutiinien ja erityisesti kuorma-autojen osalta kuorman tiedot saattavat olla arvokasta dataa.

Paljon työtä on tehty ajoneuvojen kyberturvallisuuden parantamiseksi, mutta työ sillä saralla ei ole lähelläkään valmista. Tuskin siitä täysin valmista koskaan tuleekaan. Johtuen uusien ominaisuuksien jatkuvasta kehittämisestä ja sen myötä rajapintojen lisääntymisestä, tulee kyberturvallisuuskysymysten ratkominen myös jatkumaan. Tärkeintä olisi niin ajoneuvovalmistajien, kuin loppukäyttäjien muistaa, että ajoneuvot ovat suuressa määrin tietokoneita ja näin ollen alttiita kyberhyökkäyksille.

Työn tarkoituksena oli kartoittaa ajoneuvoihin kohdistuvia kyberuhkia ja tapoja torjua niitä. Tämä tehtiin etsimällä vastauksia kysymyksiin 1) Mitkä ovat modernien ajoneuvojen merkittävimmät kyberuhat? ja 2) Mitä voidaan tehdä ajoneuvojen kyberturvallisuuden parantamiseksi? Tutkimuksessa kävi ilmi, että haavoittuvia järjestelmiä ajoneuvoissa on paljon ja työtä näiden järjestelmien turvaamiseksi on tehtävä. Tutkimuksessa selvisi myös, että aihetta tutkitaan laajasti ja ratkaisuja pyritään kehittämään, mikä on paras keino parantaa ajoneuvojen turvallisuutta.

Tutkimus onnistui tavoitteessaan löytää ajoneuvojen kyberturvaa uhkaavia tekijöitä ja mahdollisia ratkaisuja. Tutkimusta tehdessä valkeni kuitenkin, kuinka paljon enemmän ja syvällisemmin aihetta olisi syytä tutkia. Erityisesti aiempaa tutkimusta tarkastellessa löytyi uusia näkökulmia, joista aihetta olisi hyvä tarkastella. Tässä työssä tutkitun lisäksi olisi kiinnostavaa perehtyä haavoittuviin rajapintoihin yksityiskohtaisemmin. Ennen kaikkea mielenkiintoista olisi kokeilla ajoneuvon koodaamista käytännössä. Myös ajoneuvon toimintojen, kuten vilkkujen ja lukituksen ohjaus tietokoneelta OBD-II-väylän kautta olisi ollut kiinnostavaa, nyt tätä kokeiltiin ainoastaan virtuaalisesti. Nämä saattavat hyvinkin olla kirjoittajan jatkotutkimuksen kohteita.

LÄHTEET

[1] Shanken AM. Unit. Representations 2018; 143(1):91-117.

[2] Murray C. The 10 Biggest Milestones Automotive Electronics History. 2018; Saatavilla: https://www.designnews.com/electronics-test/10-biggest-milestones-automotive-electronics-history (viitattu: 7.2.2020).

[3] Safety Research & Strategies, Inc. A Brief History of Electronic Stability Controls and their Applications. 2004; Saatavilla: https://www.safetyresearch.net/blog/articles/brief-history-electronic-stability-controls-and-their-applications (viitattu: 7.2.2020).

[4] What Will Drive the Future of Vehicles? Credit Union Magazine 2018; 84(8):36.

[5] What will drive us tomorrow? When it comes to the future of transport, we need every solution we can get. Financial Express 2018.

[6] Korosec K. Tesla's full self-driving computer is now in all new cars and a next-gen chip is already 'halfway done' – TechCrunch. 2019; Saatavilla: https://social.techcrunch.com/2019/04/22/teslas-computer-is-now-in-all-new-cars-and-a-next-gen-chip-is-already-halfway-done/ (viitattu: 15.2.2020).

[7] Li X, Yu Y, Sun G, Chen K. Connected Vehicles' Security from the Perspective of the In-Vehicle Network. IEEE Network 2018; 32(3):58-63.

[8] Tuohy S, Glavin M, Hughes C, Jones E, Trivedi M, Kilmartin L. Intra-Vehicle Networks: A Review. IEEE Transactions on Intelligent Transportation Systems 2015; 16(2):534-545.

[9] Woo S, Hyo JJ, Dong HL. A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN. IEEE Transactions on Intelligent Transportation Systems 2015; 16(2):993-1006.

[10] Schlosser RW, Wendt O, Bhavnani S, Nail-Chiwetalu B. Use of information-seeking strategies for developing systematic reviews and engaging in evidence-based practice: the application of traditional and comprehensive Pearl Growing. A review. International journal of language & communication disorders 2006; 41(5):567.

[11] Ramer S, Ramer S. Site-ation pearl growing: methods and librarianship history and theory. Journal of the Medical Library Association (JMLA) 2005; 93(3).

[12] Andor. Saatavilla: https://andor.tuni.fi (viitattu: 29.4.2020).

[13] Google Scholar. Saatavilla: https://scholar.google.com/ (viitattu: 29.4.2020).

[14] IEEE Xplore Digital Library. Saatavilla: https://ieeexplore.ieee.org/ (viitattu: 29.4.2020).

[15] Tervo J. Ajoneuvoteknisten järjestelmien tietoturvallisuusselvitys. 2018.

[16] Jalli S. Tietoturva auton sisäisissä CAN-verkoissa. 2019.

[17] Kainulainen AO. Autonomisen ajoneuvon tietokonenäkö ja tietoturvahyökkäyksiltä puolustautuminen. 2018.

[18] Muukkonen N. Itseohjautuvien ajoneuvojen kyberturvahaavoittuvuudet. 2019.

[19] Myllysuo H. Älykkäiden kuljetusjärjestelmien tietoturvamekanismit autonomisten ajoneuvojen verkkoympäristössä. 2017.

[20] Miller C, Valasek C. A Survey of Remote Automotive Attack Surfaces. 2014.

[21] Dibaei M, Zheng X, Jiang K, Maric S, Abbas R, Liu S, et al. An Overview of Attacks and Defences on Intelligent Connected Vehicles. arXiv.org 2019.

[22] Sommer F, Jürgen Dürrwang, Kriesten R. Survey and Classification of Automotive Security Attacks. Information 2019; 10(4):148.

[23] Kennedy J, Holt T, Cheng B. Automotive cybersecurity: assessing a new platform for cybercrime and malicious hacking. Journal of Crime and Justice: New Directions in Cybercrime Research 2019; 42(5):632-645.

[24] Le VH, Den Hartog J, Zannone N. Security and privacy for innovative automotive applications: A survey. Comput Commun 2018; 132:17-41.

[25] Hu Q, Luo F. Review of Secure Communication Approaches for In-Vehicle Network. Int J Automot Technol 2018; 19(5):879-894.

[26] Jadoon AK, Wang L, Li T, Zia MA. Lightweight Cryptographic Techniques for Automotive Cybersecurity. Wireless Communications and Mobile Computing 2018; 2018.

[27] A Survey on Security in Automotive Networks. 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA): IEEE; 2018.

[28] Research on Information Security Framework of Intelligent Connected Vehicle. Proceedings of the 2017 International Conference on cryptography, security and privacy: ACM; 2017.

[29] Bertolino A, Calabro' A, Giandomenico F, Lami G, Lonetti F, Marchetti E, et al. A tour of secure software engineering solutions for connected vehicles. Software Qual J 2017; 26(4):1223-1256.

[30] Much A. Automotive Security: Challenges, Standards, and Solutions. Software Quality Professional 2016; 18(4):4-12.

[31] Saed M, Bone S, Robb J, Saed M. Security Concepts and Issues in Intra-Inter Vehicle Communication Network. Proceedings of the International Conference on Security and Management (SAM) 2014:1.

[32] Paradigm change of vehicle cyber security. 2012 4th International Conference on Cyber Conflict (CYCON 2012): IEEE; 2012.

[33] Pierre Kleberger. A Structured Approach to Securing the Connected Car-Chalmers University of Technology and Göteborg University; 2012.

[34] Security aspects of the in-vehicle network in the connected car. 2011 IEEE Intelligent Vehicles Symposium (IV): IEEE; 2011.

[35] Kleberger P, JAVAHERI A, Olovsson T, Jonsson E. A Framework for Assessing the Security of the Connected Car Infrastructure. 2011:236.

[36] Kleberger P, Olovsson T, Jonsson E. An In-Depth Analysis of the Security of the Connected Repair Shop. 2012:99.

[37] Kleberger P, Olovsson T. Protecting Vehicles Against Unauthorised Diagnostics Sessions Using Trusted Third Parties. 2013;Lecture Notes in Computer Science(8153):70.

[38] Avatefipour O, Malik H. State-of-the-Art Survey on In-Vehicle Network Communication (CAN-Bus) Security and Vulnerabilities. arXiv.org 2018.

[39] Bozdal M, Samie M, Jennions I. A Survey on CAN Bus Protocol: Attacks, Challenges, and Potential Solutions. 2018:201-205.

[40] Oyler A, Saiedian H. Security in automotive telematics: a survey of threats and risk mitigation strategies to counter the existing and emerging attack vectors. Security and Communication Networks 2016; 9(17):4330-4340.

[41] Survey on vehicular attacks - building a vulnerability database. 2015 IEEE International Conference on Vehicular Electronics and Safety (ICVES: IEEE; 2015.

[42] Zhong J, Du S, Zhou L, Zhu H, Cheng F, Chen C, et al. Security Modeling and Analysis on Intra Vehicular Network. 2017;2017-:1-5.

[43] Zeng W, Khalid MAS, Chowdhury S. In-Vehicle Networks Outlook: Achievements and Challenges. IEEE Communications Surveys & Tutorials 2016; 18(3):1552-1571.

[44] Chockalingam S, Lallie HS. Alarming! Security aspects of the wireless vehicle. International Journal of Cyber-Security and Digital Forensics 2014; 3(4):200-208.

[45] Survey on security threats and protection mechanisms in embedded automotive networks. 2013 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop (DSN-W): IEEE; 2013.

[46] A two-year survey on security challenges in automotive threat landscape. : Institute of Electrical and Electronics Engineers Inc; 2015.

[47] Hoppe T, Kiltz S, Dittmann J. Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures. Reliability Engineering and System Safety 2011; 96(1):11-25.

[48] Koscher K, Czeskis A, Roesner F, Patel S, Kohno T, Checkoway S, et al. Experimental Security Analysis of a Modern Automobile. 2010:447-462.

[49] Sanastokeskus. Kyberturvallisuuden sanasto (TSK 52). TSK-sarja 2018.

[50] Pfleeger CP, Pfleeger SL, Margulies J. Security in computing. Fifth ed. Upper Saddle River, NJ: Prentice Hall; 2015.

[51] Rountree D. 4 - System Security. In: Rountree D, editor. Security for Microsoft Windows System Administrators Boston: Syngress; 2011. p. 109-134.

[52] Tuttle H. Hacking cars. Risk Management 2017; 64(1):20-25.

[53] ISO/TC 204 Intelligent transport systems. Intelligent transport systems — Framework for green ITS (G-ITS) standards — Part 1: General information and use case definitions . 1st ed.: ISO/TC 204 Intelligent transport systems; 2017.

[54] Eskandarian A. Handbook of intelligent vehicles. 2nd ed.: Springer London; 2012.

[55] Vehicle Cybersecurity. Saatavilla: https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity (viitattu: 24.4.2020).

[56] Automotive connectivity, cyber attack scenarios and automotive cyber security. 2017 IEEE International Conference on Electro Information Technology (EIT): IEEE; 2017.

[57] Hashem Eiza M, Ni Q. Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity. IEEE Vehicular Technology Magazine 2017; 12(2):45-51.

[58] Charette RN. This car runs on code. IEEE Spectrum 2009; 46(3):3.

[59] GAO. Washington: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack. US Official News, Toukokuu 2, 2016.

[60] Delgrossi L, Zhang T. Vehicle safety communications : protocols, security, and privacy. Hoboken, New Jersey: John Wiley & Sons, Inc; 2012.

[61] Winning A. Number of automotive ECUs continues to rise. eeNews Automotive, Toukokuu 15, 2019.

[62] SaberRD for Invehicle and Avionics Network. Saatavilla: https://powersys-solutions.com/application/sub-application/sub-application-software/sub-application-software-details/?software=SaberRD&study=Invehicle-and-Avionics-Network (viitattu: 19.4.2020).

[63] Johansson K, Törngren M, Nielsen L. Vehicle Applications of Controller Area Network. ; 2005. p. 741-765.

[64] CAN Bus Explained - A Simple Intro. 2020; Saatavilla: https://www.csselectronics.com/screen/page/simple-intro-to-can-bus/language/en (viitattu: 19.4.2020).

[65] ISO/IEC. Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model. 2nd ed.: ISO/IEC; 1994.

[66] SAE J1939 Standards Collection. Saatavilla: https://www.sae.org/standards-dev/groundvehicle/j1939a.htm (viitattu: 18.5.2020).

[67] Dressler C, Fisher O, Mack Monica, Zitzmann R. CANdictionary. 2008.

[68] Marcon Zago G, Pignaton de Freitas E. A Quantitative Performance Study on CAN and CAN FD Vehicular Networks. IEEE Trans Ind Electron 2018; 65(5):4413-4422.

[69] Understanding CAN with Flexible Data-Rate (CAN FD). 2019; Saatavilla: https://www.ni.com/fi-fi/innovations/white-papers/14/understanding-can-with-flexible-data-rate--can-fd-.html (viitattu: 7.4.2020).

[70] ISO/TC 22/SC 31 Data communication. Road vehicles — Controller area network (CAN) — Part 1: Data link layer and physical signalling. 2nd ed.: ISO/TC 22/SC 31 Data communication; 2015.

[71] Yu T, Wang X. Topology Verification Enabled Intrusion Detection for In-Vehicle CAN-FD Networks. IEEE Communications Letters 2020; 24(1):227-230.

[72] LIN BUS EXPLAINED - A SIMPLE INTRO. Saatavilla: https://www.csselectronics.com/screen/page/lin-bus-protocol-intro-basics/language/en (viitattu: 20.4.2020).

[73] FlexRay Automotive Communication Bus Overview. 2019; Saatavilla: https://www.ni.com/fi-fi/innovations/white-papers/06/flexray-automotive-communication-bus-overview.html (viitattu: 23.4.2020).

[74] MOST - The High-Speed Multimedia Network Technology. Saatavilla: https://www.vector.com/int/en/know-how/technologies/networks/most/ (viitattu: 24.4.2020).

[75] LIN vs CAN vs FlexRay vs MOST-Difference between LIN,CAN,FlexRay,MOST. Saatavilla: https://www.rfwireless-world.com/Terminology/LIN-vs-CAN-vs-FlexRay-vs-MOST.html (viitattu: 19.4.2020).

[76] Suomalainen Sensible4 valittiin maailman parhaaksi itseajavien ajoneuvojen startupiksi. ePressi 2019.

[77] Uber in fatal crash had safety flaws say US investigators. BBC News, Marraskuu 6, 2019.

[78] Volvo Cars and Uber Present Production Vehicle Ready for Self-Driving. Targeted News Service (TNS), Kesäkuu 17, 2019.

[79] Coldewey Devin. Uber in fatal crash detected pedestrian but had emergency braking disabled. 2018; Saatavilla: https://techcrunch.com/2018/05/24/uber-in-fatal-crash-detected-pedestrian-but-had-emergency-braking-disabled/ (viitattu: 15.2.2020).

[80] Atiyeh Clifford. Uber Reportedly Removed Critical Auto-Braking System on Self-Driving Test Car. Car and Driver, Marraskuu 18, 2019.

[81] Intelligent Transportation System Leads to First Test Bed 'K-City' for Connected Cars in South Korea. PR Newswire Asia, Marraskuu 16, 2017.

[82] Herrmann A, Brenner W, Stadler R. Autonomous driving : how the driverless revolution will change the world. Bingley, England: Emerald Publishing; 2018.

[83] HO-JEONG L. K-City to open for autonomous vehicle testing. 2019; Saatavilla: http://mengnews.joins.com/view.aspx?aid=3059902 (viitattu: 15.2.2020).

[84] NHTSA. Automated Vehicles for Safety | NHTSA. Saatavilla: https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety (viitattu: 30.3.2020).

[85] Raiyn J. Data and cyber security in autonomous vehicle networks. Transport and Telecommunication 2018; 19(4):325-334.

[86] Connecting smartphones and cars can make self-driving safe, says Ford boss. Express (Online), Helmikuu 28, 2018.

[87] A Ride in the Google Self Driving Car. Toukokuu 27, 2014, YouTube, Saatavilla: https://www.youtube.com/watch?v=TsaES--OTzM.

[88] Tesla Autonomous-Driving Feature Linked to a Death--3rd Update. Dow Jones Institutional News 2016.

[89] Santoni de Sio F. Killing by Autonomous Vehicles and the Legal Doctrine of Necessity. Ethic Theory Moral Prac 2017; 20(2):411-429.

[90] Keeling G. Legal Necessity, Pareto Efficiency & Justified Killing in Autonomous Vehicle Collisions. Ethic Theory Moral Prac 2018; 21(2):413-427.

[91] Raskaan liikenteen semiautonominen ajaminen. TransDigin tiedonvaihtoseminaari; Nov 15, 2019.

[92] Enge E. MOBILE VS. DESKTOP USAGE IN 2019. 2019; Saatavilla: https://www.perficientdigital.com/insights/our-research/mobile-vs-desktop-usage-study (viitattu: 31.3.2020).

[93] Boykoff MT. Public Enemy No. 1? American Behavioral Scientist 2013; 57(6):796-817.

[94] Google. Google Play. 2020; Saatavilla: https://play.google.com/store/apps/details?id=com.google.android.projection.gearhead&hl=fi (viitattu: 31.3.2020).

[95] Mandal AK, Panarotto F, Cortesi A, Ferrara P, Spoto F. Static analysis of Android Auto infotainment and on-board diagnostics II apps. Software: Practice and Experience 2019; 49(7):1131-1161.

[96] Android app quality for cars. 2020; Saatavilla: https://developer.android.com/docs/quality-guidelines/car-app-quality (viitattu: 31.3.2020).

[97] CarPlay. 2020; Saatavilla: https://developer.apple.com/carplay/ (viitattu: 31.3.2020).

[98] On your car display. Saatavilla: https://www.android.com/auto/ (viitattu: 9.4.2020).

[99] Sun W, Liu J, Zhang H. When Smart Wearables Meet Intelligent Vehicles: Challenges and Future Directions. IEEE Wireless Communications 2017; 24(3):58-65.

[100] Zaleski Andrew. Ford's New Wearables Lab is Pioneering In-Car Health Tech. 2016; Saatavilla: https://fortune.com/2016/02/19/ford-wearables-lab-health-tech/ (viitattu: 29.4.2020).

[101] B. Lee, B. Lee, W. Chung. Standalone Wearable Driver Drowsiness Detection System in a Smartwatch. IEEE Sensors Journal 2016; 16(13):5444-5451.

[102] Multimedia transmissions over vehicular networks. 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC): IEEE; 2016.

[103] Hussain R, Hussain F, Zeadally S. Integration of VANET and 5G Security: A review of design and implementation issues. Future Generation Comput Syst 2019; 101:843-864.

[104] ISO/TC 22/SC 31 Data communication. Road vehicles — Low-speed serial data communication — Part 1: General and definitions. 1st ed.: ISO/TC 22/SC 31 Data communication; 1994.

[105] Zaman N. Automotive Electronics Design Fundamentals. 1st ed. Cham: Springer International Publishing; 2015.

[106] Bozdal M, Randa M, Samie M, Jennions I. Hardware Trojan Enabled Denial of Service Attack on CAN Bus. Procedia Manufacturing 2018; 16:47-52.

[107] Bhunia S, Hsiao MS, Banga M, Narasimhan S. Hardware Trojan Attacks: Threat Analysis and Countermeasures. Proc IEEE 2014; 102(8):1229-1247.

[108] Ibrahim D. Chapter 9 - Advanced PIC18 Projects—CAN Bus Projects. Advanced PIC Microcontroller Projects in C: Elsevier Ltd; 2008. p. 475-514.

[109] Xiao JC, Wu H, Li XX. Internet of Things Meets Vehicles: Sheltering In-Vehicle Network through Lightweight Machine Learning. SYMMETRY-BASEL 2019; 11(11):1388.

[110] OTIDS: A Novel Intrusion Detection System for In-vehicle Network by Using Remote Frame. 2017 15th Annual Conference on Privacy, Security and Trust (PST); 2017.

[111] ISO/TC 22/SC 31 Data communication. Road vehicles — Communication between vehicle and external equipment for emissions-related diagnostics — Part 1: General information and use case definition. 2nd ed.: ISO/TC 22/SC 31 Data communication; 2010.

[112] Smith C. The car hacker's handbook : a guide for the penetration tester. San Francisco, California: No Starch Press; 2016.

[113] What is OBD II? History of On-Board Diagnostics | Geotab. 2017; Saatavilla: https://www.geotab.com/blog/obd-ii/ (viitattu: 29.11.2019).

[114] OBD-II - On-Board Diagnostic System. 2013; Saatavilla: obdii.com (viitattu: 26.11.2019).

[115] CSS Electronics. OBD2 Explained - A Simple Intro (2019). 2019; Saatavilla: https://www.csselectronics.com/screen/page/simple-intro-obd2-explained/language/en (viitattu: 26.11.2019).

[116] OBD2 Explained - A Simple Intro (2018). Heinäkuu 19, 2017, YouTube, Saatavilla: https://www.youtube.com/watch?v=OhShoU_E-0g&feature=youtu.be.

[117] ESys FDL Coding - BMW F30. Huhtikuu 17, 2018, YouTube, Saatavilla: https://www.youtube.com/watch?v=S1kb1n1WnBQ.

[118] Development of On-Board Diagnostics for Car and it's Integration with Android Mobile. 2017 2nd International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS): IEEE; 2017.

[119] Sponås JG. Things You Should Know About Bluetooth Range. 2018; Saatavilla: https://blog.nordicsemi.com/getconnected/things-you-should-know-about-bluetooth-range (viitattu: 28.2.2020).

[120] An Innovative Wireless Design for a Car Infotainment System. 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS): IEEE; 2018.

[121] Whittaker Z. Why Chrysler's car hack 'fix' is staggeringly stupid. ZDNet, Heinäkuu 27, 2015.

[122] Comprehensive experimental analyses of automotive attack surfaces. USENIX Security Symposium: San Francisco; 2011.

[123] Opel Vivaro Car. MENA Report 2019.

[124] Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. Network and Distributed System Security Symposium (NDSS): Eidgenössische Technische Hochschule Zürich, Department of Computer Science; 2011.

[125] Engoulou RG, Bellaïche M, Pierre S, Quintero A. VANET security surveys. Computer Communications 2014; 44:1-13.

[126] Liang W, Li Z, Zhang H, Wang S, Bie R. Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends. International Journal of Distributed Sensor Networks 2015; 11(8):745303.

[127] Ajoneuvokannan tilastot. 2020; Saatavilla: https://www.traficom.fi/fi/tilastot/ajoneuvokannan-tilastot?toggle=Kuvaus (viitattu: 15.5.52020).

[128] Lahtinen S. Tilastokeskus - Moottoriajoneuvokanta 2019. 2020; Saatavilla: https://www.stat.fi/til/mkan/2019/mkan_2019_2020-02-28_tie_001_fi.html (viitattu: 15.5.2020).

[129] Zeadally S, Hunt R, Chen Y, Irwin A, Hassan A. Vehicular ad hoc networks (VANETS): status, results, and challenges. Telecommunication Systems 2012; 50(4):217-241.

[130] Soleymani SA, Abdullah AH, Hassan WH, Anisi MH, Goudarzi S, Rezazadeh Baee MA, et al. Trust management in vehicular ad hoc network: a systematic review. EURASIP Journal on Wireless Communications and Networking 2015; 2015(1):146.

[131] E. Schoch, F. Kargl, M. Weber, T. Leinmuller. Communication patterns in VANETs. IEEE Communications Magazine 2008; 46(11):119-125.

[132] M. Ma, D. He, H. Wang, N. Kumar, K. R. Choo. An Efficient and Provably-Secure Authenticated Key Agreement Protocol for Fog-Based Vehicular Ad-Hoc Networks. IEEE Internet of Things Journal 2019:1.

[133] M. Amoozadeh, A. Raghuramu, C. Chuah, D. Ghosal, H. M. Zhang, J. Rowe, et al. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Communications Magazine 2015; 53(6):126-132.

[134] Zeng M, Xu H. Mix-context-based pseudonym changing privacy preserving authentication in VANETs. Mobile Information Systems 2019; 2019:1-9.

[135] Singh A, Fhom HCS. Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection. International Journal of Information Security 2017; 16(2):195-211.

[136] Hacking trucks - cybersecurity risks and effective cybersecurity protection for heavy-duty vehicles. Gesellschaft fur Informatik (GI): Gesellschaft fur Informatik (GI); 2017.

[137] Facts + Statistics: Auto theft | III. Insurance Information Institute, Inc 2020.

[138] Electric vehicle technology as an exploit for cyber attacks on the next generation of electric power systems. 2016 4th International Conference on Control Engineering & Information Technology (CEIT): IEEE; 2016.

[139] Virtanen J. Teslalta haaste hakkereille: miljoona käteen ja tuliterä Tesla Model 3 alle. Tärkeimmät talousuutiset | Kauppalehti, Tammikuu 13, 2020.

[140] Ensuring the Safe and Secure Operation of Electronic Control Units in Road Vehicles. 2019 IEEE Security and Privacy Workshops (SPW): IEEE; 2019.

[141] ISO/TC 204 Intelligent transport systems. Intelligent transport systems — ITS station security services for secure session establishment and authentication between trusted devices. 1st ed.: ISO/TC 204 Intelligent transport systems; 2019.

[142] OnBoard Security Creates Standard for Secure In-Vehicle Network Access Control. PR Newswire 2018.

[143] Sedgewick A. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. Journal of Research of the National Institute of Standards and Technology 2014.

[144] Cybersecurity Best Practices for Modern Vehicles. National Highway Traffic Safety Administration 2016.

LIITE A: KIRJALLISUUSKARTOITUKSESSA KÄYTETYT HAKUSANAT

Tutkittavaa järjestelmää/ympäristöä kuvaavat sanat:

- Autonomous
- Automobile
- Automotive
- CAN
- Car
- Connected car
- Connected vehicle
- ECU
- Electronic vehicle
- Esys
- Infotainment
- Invehicle
- Modern vehicle
- OBD
- OBD2
- OBDII
- OBD-II
- PKES
- Platooning
- Self-driving car
- Telematics
- Truck
- VANET
- Vehicle
- Vehicular

Tilannetta kuvaavat sanat:

- Attack
- Cyberattack
- Cybersecurity
- Cyberthreat
- Explotation
- Hack
- Hacking
- Privacy
- Security
- Threat
- Trust
- Vulnerability

Täydentävät sanat:

- Application
- Bus
- Code
- Coding
- Connected
- Network
- Surface
- V2V
- V2I
- V2X