CAN Classicin haavoittuvuudet ja suojausmenetelmät autoalalla

Turun yliopisto
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Kesäkuu 2026
Teemu Roiha

TURUN YLIOPISTO
Tietotekniikan laitos

Teemu Roiha: CAN Classicin haavoittuvuudet ja suojausmenetelmät autoalalla

TkK-tutkielma, 21 s.
Tietotekniikka
Kesäkuu 2026

Nykypäivän ajoneuvot koostuvat jopa sadoista elektronisista ohjausyksiköistä, jotka kommunikoivat keskenään usein CAN-väylän (Controller Area Network) välityksellä. Koska kyseinen protokolla on alun perin suunniteltu vain nopeaa ja luotettavaa reaaliaikaista kommunikaatiota varten, siitä puuttuvat nykyaikaiset tietoturvamekanismit, kuten viestien salaus ja lähettäjän autentikointi. Tämä yleislähetysperiaatteella toimiva ja prioriteettiin perustuva rakenne tekee väylästä erittäin haavoittuvan. Näiden puutteiden vuoksi ajoneuvot altistuvat erilaisille kyberuhille, kuten salakuuntelulle, tekeytymis-, toisto- sekä palvelunestohyökkäyksille.

Tässä kartoittavassa kirjallisuuskatsauksessa tarkastellaan CAN Classic -tiedonsiirtoprotokollan tietoturvaa autoissa. Tutkielmassa keskitytään protokollan rakenteellisiin haavoittuvuuksiin sekä menetelmiin, joilla havaittuja uhkia voidaan torjua jo olemassa olevan arkkitehtuurin puitteissa.

Tutkielma osoittaa, että perinteisten raskaiden kryptografisten menetelmien soveltaminen on haastavaa CAN Classicin rajallisen laskentatehon ja tiukan kahdeksan tavun maksimiviestikoon vuoksi. Tällaisten turvaominaisuuksien lisääminen hidastaa herkästi aikakriittistä kommunikaatiota ajoneuvon kriittisten ohjausyksiköiden, kuten jarrujen, välillä. Esimerkiksi autoalan standardin, AUTOSAR SecOCn, sovittaminen vanhaan arkkitehtuuriin vaatii merkittäviä kompromisseja turvallisuuden ja nopeuden suhteen. Näiden rajoitteiden vuoksi erityisesti kone- ja syväoppimiseen perustuvat tunkeutumisen havaitsemisjärjestelmät (IDS) nousevat esiin tehokkaimpina ratkaisuina. Koska IDS toimii passiivisesti vain verkkoliikennettä tarkkailemalla, se kykenee havaitsemaan poikkeavuuksia ja uhkia reaaliajassa ilman, että se hidastaa väylän normaalia viestintää tai vaatii muutoksia viestien rakenteeseen.

Asiasanat: CAN Classic, haavoittuvuudet, tietoturva, hyökkäykset, Controller Area Network

Sisällys

Kuvat

1 Johdanto

Nykypäivän autot ovat liikkuvia hajautettuja järjestelmiä. Hajautetulla järjestelmällä tarkoitetaan joukkoa itsenäisiä tietokoneita, jotka työskentelevät samassa verkossa kohti yhteistä tavoitetta. [1] Autosta riippuen, järjestelmä voi sisältää jopa yli sata elektronista ohjausyksikköä (engl. electronical control unit, ECU). [2] Nämä tietokoneet tai tarkemmin sanottuna pienet sulautetut järjestelmät muodostavat yhdessä suuremman sulautetun järjestelmän, auton. Yhdessä ne mahdollistavat mukavuuksia, kuten lämmitetyt penkit ja ilmastoinnin, turvallisuutta, kuten hätäjarrut ja turvatyynyt sekä tietysti moottorin, jarrujen ja auton muun ohjauksen. [2]

Nämä elektroniset ohjausyksiköt ovat yhteydessä toisiinsa auton sisäisten verkkojen välityksellä (engl. in-vehicle networks, IVN). Autoissa yleisimpiä verkkoja ovat CAN, LIN, FlexRay ja MOST, joilla kaikilla on autoissa oma käyttötarkoituksensa, omine etuineen ja haittoineen [3].

Näistä merkityksillisin on tämän kartoittavan kirjallisuuskatsauksen aihe, CAN (engl. Controller Area Network). Sitä voidaan ajatella auton keskushermostona, joka välittää tietoa autojen eri verkkojen, sensoreiden, sekä toimilaitteiden välillä. CAN-teknologiasta puhuttaessa on tärkeä selventää ero CAN-väylän ja CAN-protokollan välillä. OSI-mallin mukaisesti väylästä puhuttaessa on kyse fyysisestä kerroksesta (physical layer) eli esim. johdoista ja kuinka ne liittävät tietokoneet toisiinsa. CAN-protokollalla tarkoitetaan puolestaan järjestelmän siirtokerrosta (engl.

Data link layer) eli miten väylällä lähetetty informaatio tulkitaan. CAN-teknologialla tai CAN-verkolla taas viitataan järjestelmään kokonaisuutena. [4], [5]

CANin ensimmäinen versio on jo vuosikymmeniä vanha, mutta vuosien aikana siitä on kehitettty uusia ja parempia versioita. Tässä työssä keskitytään aikaisimpaan versioon, CAN Classic (CAN CC). Uusimissa autoissa uudemmat versiot ovat pitkälti syrjäyttäneet sen, mutta se on edelleen käytössä vähemmän kriittisissä auton osissa, sekä pääasiallisessa käytössä vanhemmissa autoissa, jotka ovat edelleen tieliikennekäytössä.

CAN on häiriösietoinen, helppokäyttöinen ja luotettava tiedonjakeluteknologia, mutta se on myös haavoittuvainen. Tämän työn aikana käsitellään CAN-väylän perusperiaatteita, haavoittuvuuksia, siihen kohdistuvia hyökkäyksiä ja sen hyökkäyspinta-alaa. Lisäksi läpi käydään nykyisiä ja tulevia mahdollisia keinoja puolustautua näitä hyökkäyksiä vastaan. [6] Työn tutkimuskysymyksinä ovat:

TK1: Mitä ovat CAN Classicin haavoittuvuudet?

TK2: Mitä ovat CAN Classicin puolustusmekanismit?

Työ suoritettiin kartoittavana kirjallisuuskatsauksena käyttäen Web of Sciencen Core Collection tietokantaa. Tiedonhaku suoritettiin englanniksi ja pääasialliset hakulauseet olivat: *("CAN bus"OR "Controller Area Network") AND (Authentication OR Cryptography OR encryption)* ja **("Controller Area Network"OR "CAN bus"OR CAN) AND ("intrusion detection system"OR IDS) AND automotive**. Näistä hakutuloksista on valittu artikkelit, jotka käsittelivät haavoittuvuuksia, hyökkäyksiä ja puolustumekanismeja nimenomaan CAN Classic protokollassa. Työssä käytettiin hyödyksi myös valittujen artikkeleiden lähdeluetteloa tukena aiheen kartoittamisessa ja tutkimuksessa.

Luvussa 2 esitellään CAN-teknologian perusperiaatteita. Luvussa 3 tarkastellaan sen tietoturvaa käymällä läpi sen haavoittuvuuksia ja siihen kohdistuvia hyök-

käyksiä. Luvussa 4 esitellään eri puolustusmekanismeja näiden hyökkäyksien torjumiseksi. Luvussa 5 pohditaan CAN-teknologian tietoturvan nykytilaa ja esiteltyjen suojautumiskeinojen käytännön rajoitteita. Lopuksi luvussa 6 tehdään yhteenveto keskeisimmistä havainnoista.

2 CAN-teknologian perusperiaatteet

CAN on sarjallisen kommunikaation teknologia, jota käytetään kaikkialla teollisuudessa hisseistä ja laivoista, lääketeknologiaan sekä autoihin. Autossa se yhdistää useita elektronisia ohjausyksiköitä (engl. electronical control unit, ECU), sensoreita ja toimilaitteita toisiinsa. [7] CAN-väylä on tehokas, halpa, yksinkertainen ja vankka protokolla, minkä vuoksi sen iästä huolimatta sitä käytetään yhä. Sen etuja ovat nopeus ja elektronisten häiriöiden kestävyys, jonka vuoksi se on ideaali reaaliaikaiseen kommunikointiin, kuten jarrujen ja moottorin hallintaan. [8]

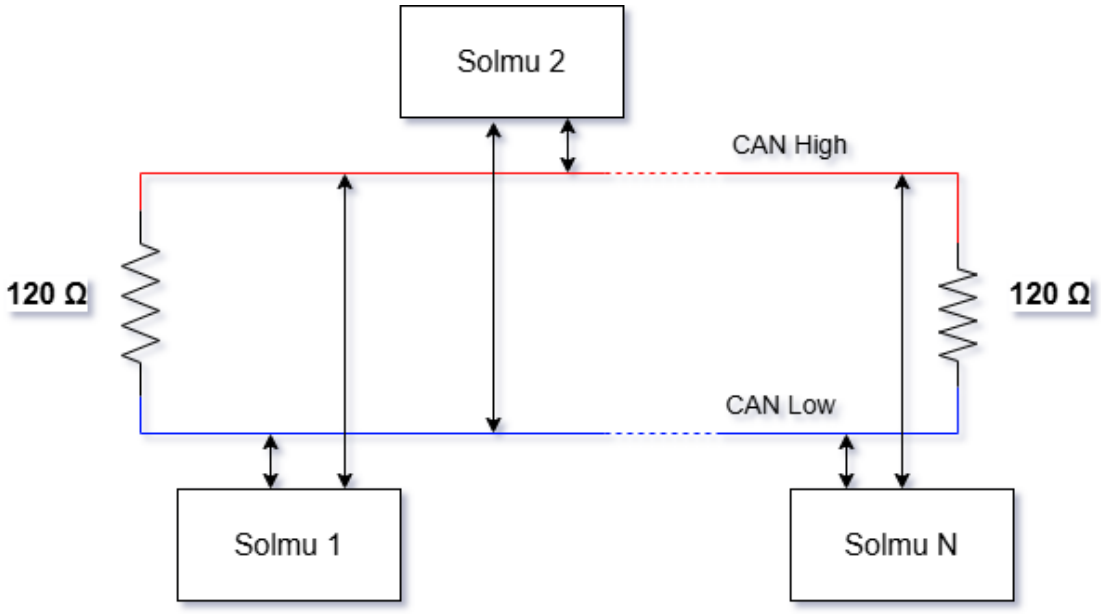
Vuosien aikana on kehittynyt kolme vakiintunutta versiota, joita kaikki käytetään tänä päivänä edelleen: CAN CC, CAN-FD, ja CAN-XL. Ensimmäinen, ja tämä työn aihe, on alkuperäinen CAN CC, joka kehitettiin alun perin 1980-luvulla Robert Bosh GmbH toimesta. Kehitys aloitettiin, sillä ohjausyksiköiden kasvaessa autoissa, jokaisen osan erikseen johdottaminen alkoi käymään kalliiksi ja monimutkaiseksi. CAN oli ratkaisu tähän ongelmaan. Se mahdollistaa erillisten laitteiden välisen kommunikoinnin yksinkertaisella ja halvalla tavalla yhdistämällä ne väylään. Ensimmäiseen autoon se tuli käyttöön jo vuotena 1991 ja on käytössä edelleen autoissa tähän päivään saakka. [9], [10]

2.1 CAN Classic -arkkitehtuuri

Controller Area Network Classic ISO standardi 11898-1 toimii yleislähetysperiaatteella. Viesti lähetetään kaikille kanavan jäsenille, ja on vastaanottajan vastuulla,

joko siivuuttaa tai huomioida vastaanotettu viesti. Tämä toteutetaan filttereiden avulla. Verkko noudattaa Master-Master -arkkitehtuuria eli jokaisella solmulla (laitteella) on samat oikeudet vastaanottaa ja lähettää viestejä verkossa. Viestien lähetys toimii tuottaja-kuluttaja periaatteella eli kun yksi solmu lähettää muut kuuntelevat.

CAN käyttää parikaapelia, toinen näistä on CAN High ja toinen CAN Low. Näiden välinen jännite-ero määrittää loogisen nollan (resessiivinen) tai ykkösen (dominantti). Tätä kutsutaan differentiaaliseksi signaloinniksi, joka mahdollistaa CAN-verkon häiriösietoisuuden. Ulkoinen häiriö osuu molempiin johtimiin yhtä aikaa, jolloin jännite-ero pysyy samana ja signaali säilyy eheänä. Kuvassa 2.1 esitellään kuinka laitteet yhdistyvät CANiin.



Kuva 2.1: Esimerkki CAN-verkosta N-määrällä solmuja Oladimeji et al. [11]

Kaikki CAN-väylät eivät ole kuitenkaan samanarvoisia, niitä on kaksi varianttia: Nopea (High-speed) ja hidas (Low-speed). High-speed CAN-väylän nopeus 125 Kbps-1 Mbps välillä, kun taas low-speed CAN-väylä 5-125 Kbp/s välillä. Aikakriittiset osat kuten moottori ja jarrut on kytketty nopeaan verkkoon, kun taas vähemmän

aikakriittiset osat kuten ikkunat ja ilmastointi on kytketty hitaampaan väylään. Nämä kaksi väylää on kytketty toisiinsa yhdyskäytävän avulla. Yhdyskäytävät (engl. Gateway) tekevät paljon erilaisia asioita auton sisäisessä ja CAN-verkossa. Ne toimivat tulkkeina protokollien ja verkkojen välillä sekä yhdistävät eri nopeuksisia CAN-väyliä kuten High- ja low-speed CAN. Ne toimivat myös palomuureina verkkojen välisessä kommunikaatiossa. [7], [12]

2.2 Viestintä CAN-verkossa

CAN-standardin terminologiassa kaikkiin viesteihin viitataan kehyksinä (engl. frames). CAN CCssä on neljä kehystyyppiä: data frame, remote frame, error frame ja overload frame. Tyypillisin näistä on data frame, jolla lähetetäään nimensä mukaisesti dataa. Remote framella solmu voi pyytää toista solmua lähettämän dataa. Error frame lähetetään automaattisesti, kun solmu havaitsee virhetilanteen väylällä. Overload frame puolestaan toimii virtauksenhallinnan välineenä, kun solmu tarvitsee käsittelyaikaa ennen seuraavan kehyksen vastaanottamista.

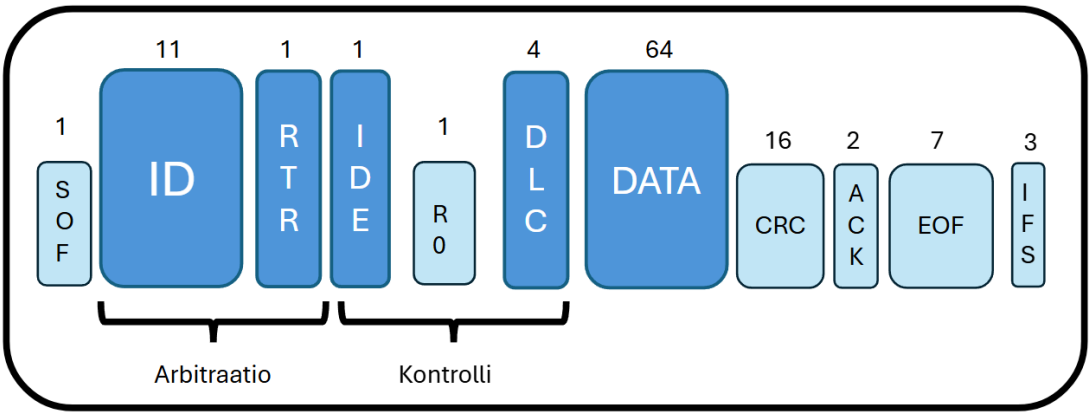
Jokainen kehys tarjoaa tunnisteen, joka on uniikki verkon kontekstissa. Tämä tunniste määrittelee mm. viestin prioriteetin ja tietysti identifioi lähettäjän verkossa. Mitä alhaisempi ID numero, sitä korkeampi prioriteetti. Prioriteetti määrittää missä järjestyksessä viestit lähetetään. [13]

Monissa muissa protokollissa, kuten TCP/IPssä, lähettäjän identiteetti ja viestin eheys tarkistetaan ennen kuin viesti hyväksytään käsiteltäväksi. CAN-protokollassa kehysten sisältöä ei kuitenkaan validoida etukäteen, vaan viestien muoto tarkistetaan vasta lähetyksen yhteydessä. Protokolla olettaa, että kaikki solmut toimivat standardin mukaisesti, ja jos viestissä ilmenee poikkeama, sille palautetaan virhe.

CAN-verkon tärkeimpiä ominaisuuksia on sen nopeus, ja yksikin virheitä jatkuvasti aiheuttava solmu hidastaa koko verkon toimintaa. Tätä varten jokaisella solmulla on kaksi virhelaskuria. Nämä ovat lähetysvirhelaskuri (engl. TEC) ja vas-

taanottovirhelaskuri (engl. REC). Kumman tahansa laskurin ylittäessä raja-arvon ongelmallinen solmu siirtyy error active-tilasta error passive-tilaan, ja lopulta bus off-tilaan, jossa se irrotetaan väylästä kokonaan. Error active-tilassa solmu toimii normaalisti, ja passive tilassa sen error biteistä tulee resessiivisiä eli sen lähettämät virheet eivät välttämättä näy muille solmuille, koska dominantti bitti ylikirjoittaa resessiivisen.

Törmäystilanteiden hallitsemiseksi CAN käyttää hävittämätönta bittikohtaista arbitraatiota (engl. non-destructive bit-wise arbitration), joka mahdollistaa ettei kumpikaan viesti tuhoudu törmäystilanteessa. Käytännössä tämä tarkoittaa sitä, että kaksi samanaikaisesti lähettävää solmua kilpailevat väylän hallinnasta, ja matalamman IDn omaava viesti voittaa. Tarkastellaan seuraavaksi CAN-viestien rakennetta 2.2.



Kuva 2.2: CAN CC Standardi formaatti viesteille Wang ja Ghaleb [14]

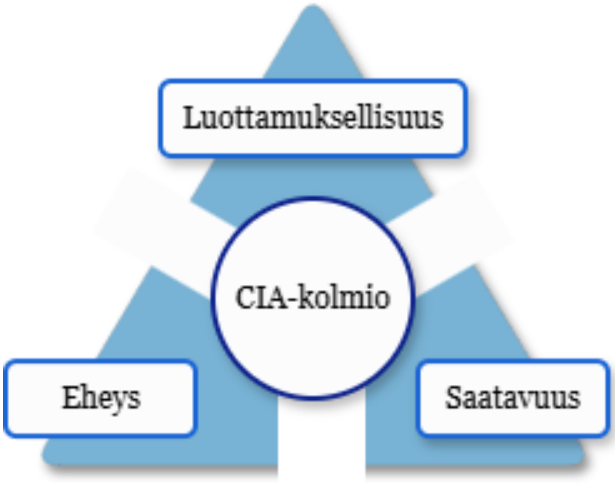
CAN-viestin lähetys alkaa kehyksen alkua osoittavalla SOF-bitillä (engl. Start of Frame). Se on yksittäinen dominoiva bitti, joka synkronoi kaikki väylän ohjausyksiköt. Tätä seuraa arbitraatio eli sovittelukenttä (engl. Arbitration Field), joka määrittää viestin prioriteetin. Vakiomuotoisessa CAN-kehyksessä käytetään 11-bittistä tunnistetta (ID), kun taas laajennetussa formaatissa tunniste on 29-bittinen. Tun-

nisteen lisäksi kenttään kuuluu RTR-bitti (engl. Remote Transmission Request), joka erottelee varsinaiset dataviestit (0) tiedon lähetyspyynnöistä (1). Itse hyötytieto sijaitsee datakentässä. CAN-viestien hyötytieto on rajattu 0–8 tavuun, mikä pitää viestit lyhyinä ja takaa korkean prioriteetin viesteille minimaalisen siirtoviiveen. Tiedonsiirron luotettavuus varmistetaan tarkistussummalla (engl. Cyclic Redundancy Check, CRC), joka paljastaa siirron aikana mahdollisesti syntyneet virheet. Viestin virheetön vastaanotto vahvistetaan kuittaus- eli ACK-kentässä. Viimeisenä osana on kehyksen loppu (engl. End of Frame, EOF), joka päättää sanoman seitsemän peräkkäisen resessiivisen bitin sekvenssillä. [3], [5], [13]

3 Tietoturva-analyysi

CAN on standardoitunut tapa välittää tietoa auton sisällä. Se kehitettiin alun perin aikana, jolloin tärkeintä ei ollut turvallisuus vaan nopea, luotettava reaaliaikainen kommunikaatio. Tästä johtuen CAN jäi haavoittuvaiseksi, sillä turvallisuusmekanismien, kuten autentikoinnin ja salauksen lisäys olisi lisännyt kustannuksia, ja hidastanut kommunikointia väylässä. Lisäksi CANia kehittäessä loppukäyttäjällä ei ollut tarkoituksena saada fyysistä pääsyä väylään, joka on sen keskeisin hyökkäysvektori. [9] Kuten jo aikaisemmin mainittiin CAN-väylän viestintä toimii yleislähetysperiaatteella. Tämä, salauksen ja autentikoinnin puute sekä tapa, jolla prioriteetti jaetaan väylässä, altistavat CANin lukuisille hyökkäyksille joita käsitellään myöhemmin tämän luvun aikana. [7]

Tarkastellaan CANin haavoittuvuuksia peilaten niitä klassisen CIA-kolmion kautta 3.1. kuvassa CIA-kolmio on tietoturvan perustavanlaatuinen malli, joka jakaa tietoturvan kolmeen eri osaan. Ensimmäinen on luottamuksellisuus (engl. Confidentiality, C). Luottamuksellisuus määrää, että tietoon on pääsy ainoastaan asianomaisilla osapuolilla. Toisena on eheys (engl. Integrity, I), joka määrää että tietoa ei pidä pystyä muuttamaan luvatta tai ilman, että siitä jää jälki. Kolmantena osa-alueena on saatavuus (engl. Availability, A), joka määrää, että tieto tulee aina olla saatavilla asianomaisille tahoille. **hajautetut**



Kuva 3.1: CIA-kolmio

3.1 Haavoittuvuudet

Yksi merkittävimmistä turvallisuusriskeistä on autentikoinnin eli todennuksen puute. Todentamisella tarkoitetaan prosessia, jossa viestin lähettäjän identiteetti ja viestin alkuperä varmistetaan luotettavasti. Perinteisissä tietoverkoissa solmu voi todentaa itsensä esimerkiksi digitaalisen allekirjoituksen tai salausavainten avulla ennen tiedon välittämistä. CAN-verkosta tällainen sisäänrakennettu todentamismekanismi puuttuu kokonaan. Tämä puute altistaa verkon identiteettivarkauksille (engl. spoofing), joissa pahanlaatuinen tai kompromisoitu ohjausyksikkö voi tekeytyä toiseksi, luotetuksi yksiköksi. Koska viestin todellista lähettäjää ei voida varmistaa, väylään kytketty yksikkö voi luvatta lähettää väärennettyjä ohjauskomentoja tai lukea tietoa, johon sillä ei tulisi olla pääsyä.

Seuraava olennainen haavoittuvuus on salauksen puute. Salauksen tavoitteena on varmistaa tiedon luottamuksellisuus. Tiedon salaaminen tapahtuu kryptografisilla algoritmeilla, joilla selkokielinen teksti (engl. plain text) sekoitetaan lukukelvottomaan muotoon (engl. cipher). Asianomaisten on mahdollista purkaa salaus ja

täten päästä käsiksi alkuperäiseen selkokieliseen tekstiin. Ilman salausta on tieto esillä kaikille kanavan kuuntelijoille, joka rikkoo eheyttä ja luottamuksellisuutta.

Seuraavana haavoittuvuuksien listalla on CANin tapa määrittää prioriteetti kommunikaatiossa. Kuten luvussa 2 käsiteltiin, korkeimman prioriteetin saavat ne joiden ID on alhaisin. Tämä aiheuttaa ongelmia kun identiteettiä ei varmisteta, jonka totesimme jo aikaisemmin. Tämä altistaa hyökkäyksille, jossa hyökkääjä lähettää viestejä alhaisella IDllä, joka estää oikeasti tärkeiden viestin perille pääsyn. Tämä siis aiheuttaa ongelmia saatavuuden kanssa.

Viimeisenä listalla on CANin tapa lähettää viestejä eli jo ennestään tuttu yleislähetys. Tämä yhdistettynä salauksen ja todentamisen puutteen kanssa tekee koko kanavan viestinnästä julkista tietoa kaikille sen jäsenille, joka puolestaan suoraan rikkoo luottamuksellisuutta.

3.2 Hyökkäykset

CAN-verkko on alttiina monille eri hyökkäyksille johtuen sen yleisestä huonosta turvallisuudesta. Hyökkäyksien tavoitteena on usein joko varkaus, vakoilu, hallinta, tai jopa terrorismi. Hyökkäykset voidaan luokitella kahteen yläluokkaan: Paikallis- ja etähyökkäyksiin. Paikallishyökkäykset vaativat fyysisen, joko suoran tai epäsuoran pääsyn CAN-verkkoon. Suora pääsy saadaan OBD-portin kautta. Epäsuora pääsy taas voi olla USB-portin tai DVD-soittimen kautta. [15]Etähyökkäyket suoritetaan ilman fyysistä pääsyä CAN-verkkoon ja ne ovat joko lyhyen ja pitkän matkan hyökkäyksiä. Lyhyen matkan hyökkäykset tehdään Bluetoothin ja Wifin kautta. Pitkän matkan hyökkäyspinta-aloihin lukeutuvat 5G ja GNSS. [9]

Tekeytymishyökkäys (engl. spoofing) on aktiivinen hyökkäys, jossa hyökkääjä lähettää CAN-väylään viestejä esiintyen jonkin toisen, luotetun ohjausyksikön nimissä. Kuten alaluvussa 3.1 todettiin verkko luottaa sokeasti viestien sisältämään ID-tunnisteeseen. Hyökkääjä voi siis esimerkiksi syöttää väylään väärennettyjä jarrutus-

tai ohjauskomentoja korkealla prioriteetilla, ja vastaanottavat ohjausyksiköt käsittelevät ne täysin aitoina komentoina.

Toistohyökkäys (engl. replay attack on puolestaan menetelmä, jossa hyökkääjä ensin salakuuntelee ja tallentaa väylän liikennettä, ja lähettää tallentamansa viestit myöhemmin takaisin verkkoon sellaisenaan. Tämän hyökkäyksen onnistuminen perustuu siihen, että perinteisissä CAN-viestissä ei ole sisäänrakennettua tuoreusarvoa, kuten aikaleimaa tai juoksevaa järjestysnumeroa. Vaikka viestin hyötykuorma olisi suojattu, hyökkääjän ei tarvitse ymmärtää sen sisältöä. Riittää, että hän tallentaa esimerkiksi auton ovien avauskomennon ja toistaa sen myöhemmin, jolloin vastaanottava järjestelmä luulee komentoa uudeksi ja reagoi siihen.

Palvelunestohyökkäys (engl. Denial-of-service, DoS) on hyökkäys, jonka tarkoituksena on nimensä mukaisesti estää jonkin palvelun toiminta lähettämällä sinne valtava määrä dataa. CAN-protokollassa tämä onnistuu lähettämällä suuri määrä korkeimman prioriteetin viestejä kanavaan, jolloin mikään muu alhaisemman prioriteetin omaava solmu ei pysty lähettämään viestejä, täten lamauttaen kaiken oikean viestinnän väylän sisällä. [15]

Salakuuntelu (engl. eavesdropping) on passiivinen hyökkäys, jossa pyritään keräämään tietoa. Viestintäkanavilla on yleensä salaus tämän estämiseksi, jota tietenkään CAN ei omaa. Nykyautoissa CAN-väylä vastaanottaa ja välittää tietoa ei pelkästään auton sisäisten ohjausyksiköiden välillä vaan myös ulkomaailman kanssa (engl. Vehicle to everything, V2X) yhdistyy CAN-väylään yhdyskäytävän kanssa ja se välittää tietoa muihin auton verkkoihin ja järjestelmiin. CAN-väylän altistuessa se altistaa myös kaiken muun kommunikoinnin autossa, jonka välikätenä se toimii.

4 Modernit puolustusmekanismit

Aikaisemmissa luvuissa käsiteltiin haavoittuvuuksia ja mahdollisia hyökkäyksiä CAN-verkkoa vastaan. Tämän johdosta CAN-verkkoa varten on kehitelty paljon eri keinoja puolustautua niitä vastaan. Nämä puolustusmekanismit jakautuvat pääasiallisesti todentamiseen, salaukseen, ja tunkeutumisen havaitsemisjärjestelmiin (engl. Intrusion Detection System, IDS). Salauksen ja todennuksen lisäämisen haasteita on useita. Kaksi pääasiallista ongelmaa ovat rajattu laskentateho sekä viestien koko, joka on vain 8 tavua. Rajatun koon vuoksi digitaalisten allekirjoitusten ja muiden turvatunnisteiden lisääminen on hankalaa, sillä kommunikaation on pysyttävä reaaliaikaisena auton kriittisissä osissa. Tämä asettaa lisärajoitteita, sillä salauksen ja todentamisen toteutukset lisäävät välttämättömästi viivettä, joka voi olla kriittinen esimerkiksi jarrujen ohjauksessa. Tämän vuoksi tunkeutumisen havaitsemisjärjestelmät ovat nousseet suosituksi vaihtoehdoksi ongelman ratkaisemiseksi, sillä ne voivat tarkkailla verkossa tapahtuvaa liikennettä vaikuttamatta siihen itse.

Ilmeinen ratkaisu näihin ongelmiin olisi siirtyä uudempaan CAN-FD-teknologiaan, joka hyödyntää sen suurempaa hyötykuormaa (64 tavua) erilaisten salausalgoritmien kuten AES-128, SHE, HSM ja autentikointikoodien (engl. Message Authentication Codes, MAC) käyttämiseen. Käytännössä tämä ei ole kuitenkaan mahdollista jo olemassa olevissa autoissa ilman auton elektroniikan laajamittaista uudelleenrakentamista. Uudet autot luonnollisesti käyttävät näitä uudempia teknologioita, mutta liikenteessä jo olevat autot ovat yhä haavoittuvaisia. Seuraavissa

alaluvuissa käsitellään keinoja, joilla näiden autojen turvallisuutta voidaan parantaa olemassa olevan CAN-arkkitehtuurin puitteissa. [16]

4.1 Autentikointi

Kuten aikaisemmin todettiin autentikoinnilla eli todentamisella tarkoitetaan viestin lähettäjän identiteetin varmistamista. Tähän on useita keinoja, joista yleisimpiä ovat viestien todennuskoodit, digitaaliset allekirjoitukset ja sertifikaatit. Perinteiset todennusmenetelmät törmäävät CAN-protokollan kanssa kuitenkin samaan 8 tavun ongelmaan. Esimerkiksi HMAC-SHA256 tuottaa 32 tavun pituisen tunnisteen, joka on yksinään nelinkertainen CAN-kehyksen maksimikokoon nähden. Tämä tarkoittaa, että jo pelkän tunnisteen lähettäminen vaatisi neljä erillistä kehystä, eli yksittäinen todennettu viesti pilkkoutuisi vähintään viideksi kehykseksi.

Tämän päivän autoalan de facto -todentamisstandardina on AUTOSARin SecOC (Seucre Onboard Communication), joka tarjoaa ratkaisun viestien autentikointiin ja toisohyökkäyksien estämiseen varmentamalla datan tuoreuden. Se on kuitenkin suunniteltu ensisijaisesti uudemille verkkoarkkitehtuureille, kuten CAN-FDlle, joissa hyötykuorman koko ei muodosta pullonkaulaa. Kun SecOC-standardi yritetään pakottaa vanhaan CAN CC -arkkitehtuuriin, törmätään välittömästi väylän 8 tavun rajoitteeseen. Jotta standardi saadaan toimimaan, on tehtävä kompromisseja joko turvallisuuden tai nopeuden kustannuksella. Yleisin ratkaisu on typistää (engl. truncation) todennuskoodia ja tuoreusarvoa voimakkaasti. Tämä kuitenkin heikentää turvallisuustasoa ja tekee protokollasta haavoittuvaisemman esimerkiksi väsytyshyökkäyksille (brute-force). [17]

Toinen yleinen lähestymistapa CANin kaltaisille verkoille on ryhmäavainten käyttö, jossa kaikki verkon jäsenet jakavat yhteisen avaimen. Tämä tekee avainten hallinnasta helpompaa, mutta tuo mukanaan uuden ongelman. Ohjausyksikkö pitää avaimen talletettuna muistissaan, jos laitteeseen saadaan fyysinen pääsy, on se luettavis-

sa ja täten koko verkon viestintä on vaarantunut. On siis selvää, etteivät perinteiset lähestymistavat ole sopivia sellaisenaan vaan ne täytyy mukauttaa CAN-verkkoa varten sopiviksi.

Lai et al. [16] ehdottivat todentamis- ja avaimenvaihtoprotokollaa, jossa ennen kuin ohjausyksikkö saa luvan lähettää kriittistä dataa, sen identiteetti varmennetaan. Tämä tehdään hyödyntäen kevyttä kryptografiaa, joka pitää viiveet minimaalisina, jotta ajoneuvon reaaliaikainen toiminta ei häiriintyisi. Avaimenvaihto tapahtuu kun laite on todennettu. Osapuolet muodostavat turvallisen, salatun yhteyden luomalla yhteisen väliaikaisen istuntoavaimen (engl. session key). Avainta päivitetään dynaamisesti, mikä takaa sen, ettei hyökkääjä voi käyttää vanhaa, kaapattua liikennettä hyväkseen. [16] Tällaisen protokollan merkittävin etu on se, että se torjuu tehokkaasti identiteettivarkaudet, väliintulohyökkäykset sekä toistohyökkäykset.

4.2 Salaus

Salauksen tavoitteena on muuntaa data ymmärrettävästä muodosta salattuun muotoon, jonka salauksen vain asianomainen voi purkaa. Haasteena on kuitenkin se, että ajoneuvojen elektroniset ohjausyksiköt ovat laskentateholtaan, muistiltaan ja energiankulutukseltaan erittäin rajallisia. Perinteiset salausalgoritmit, kuten laajasti käytetty AES (Advanced Encryption Standard), ovat usein liian raskaita CAN-väylässä käytettäväksi. Tämän vuoksi on täytynyt kehittää uusia salausalgoritmeja, jotka on suunniteltu juuri CANia varten.

Hediyal et al. [18] esittävät tähän ratkaisuksi kevennettyn SCAN-C -salausalgoritmin (Secured Controller Area Network for Communications), joka on optimoitu erityisesti ajoneuvojen resurssirajoitteisille ohjausyksiköille. Menetelmän keskeinen vahvuus piilee siinä, että se käyttää 64-bittistä lohkosalausta.

Perinteisten, raskaiden laskentaoperaatioiden sijaan SCAN-C hyödyntää kevennettyä hybridirakennetta. Laitteistotason resurssivaatimuksia ja fyysistä pinta-alaa

mittaavana porttiekvivalenttina (engl. Gate Equivalent, GE) SCAN-C vaatii ainoastaan 1197 yksikköä. Laajasti käytetty AES-salaus vaatisi kymmeniä tuhansia yksiköitä, mikä on CAN-verkon solmuille liikaa. Tällaisen kevennetyn salauksen avulla väylän viestinnän luottamuksellisuus ja eheys pystytään varmistamaan tehokkaasti ilman, että ohjausjärjestelmien vaatima reaaliaikaisuus kärsii. Tämä samalla suojaa ajoneuvon verkkoa muun muuassa salakuuntelulta sekä toistohyökkäyksiltä.

4.3 Tunkeutumisen havaitsemisjärjestelmät

Tunkeutumisen havaitsemisjärjestelmä valvoo järjestelmää hyökkäyksien tai haitallisen toiminnan tai muun poikkeaman varalta, josta se ilmoittaa järjestelmän ylläpitäjälle. IDS toimii perinteisesti signatuurien eli niin sanottuja digitaalisten sormenjälkien tai poikkeuksien pohjalta. [19] Tunnetuista haittaohjelmista on olemassa signatuureja, joiden avulla muut vastaavat haittaohjelmat voidaan tunnistaa. Tällaisen järjestelmän heikkoutena ovat uudet ennestään tuntemattomat metodit ja ohjelmat. Lisäksi haasteena on nykyisen tietokannan jatkuva ajan tasalla pitäminen. [20] Näiden haasteiden myötä nykyaikainen tutkimus keskittyy yhä enemmän kone- ja syväoppimiseen perustuviin malleihin. Syväoppimisen avulla järjestelmät pystyvät analysoimaan CAN-väylän datavirtaa ja oppimaan verkkoliikenteen normaalitilat ilman, että jokaista mahdollista hyökkäystä tarvitsee tuntea ennalta.[21]

Javed et al. [22] esittävät syväoppimista hyödyntävän CANintelliIDS-mallin, joka analysoi liikennettä konvoluutio- ja aikasarjaneuroverkkojen avulla. Järjestelmä oppii tunnistamaan verkkoliikenteen normaalin rytmin ja rakenteen. Tämän kontekstiymmärryksen ansiosta malli kykenee havaitsemaan väylään kohdistuvat poikkeavuudet, kuten fuzzing- ja palvelunestohyökkäykset, yli 93 prosentin tarkkuudella.

Korkean tunnistustarkkuuden lisäksi syväoppimiseen pohjautuvien IDS-järjestelmien elineheto autoalalla on niiden nopeus. Viivet kommunikoinnissas voivat olla kohtalokkaita, minkä vuoksi analysoinnin on taphduttava reaaliajassa. Yang et

al. [23] kehittämä tunkeutumisenhavaitsemisjärjestelmä MTH-IDS-järjestelmä käsittelee yhden datapaketin keskimäärin alle 0,6 millisekunnissa. Tämä alittaa selkeästi ajoneuvojen turvallisuuspalveluiden vaatiman 10 millisekunnin enimmäisviiven, mikä osoittaa neuroverkkojen soveltuvuuden myös reaaliaikaiseen tunnistamiseen.

Tunkeutumisen havaitsemisjärjestelmät ovat lupaava suojautumiskeino CAN Classic -arkkitehtuurille. Koska IDS toimii passiivisesti vain tarkkailemalla liikennettä, se ei vaadi muutoksia itse CAN-viestien 8 tavun kokoon tai rakenteeseen, eikä se hidasta väylän normaalia viestintää toisin kuin raskaat salaus- ja autentikointimenetelmät.

5 Pohdinta

CAN Classic -teknologia on alkuperäisen suunnittelunsa vuoksi rakenteellisesti haavoittuvainen, ja huolimatta tietoisuuden lisääntymisestä, se on edelleen käytössä lähes poikkeuksetta kaikissa tämän päivän henkilöautoissa. Autoalan ensisijaisena suuntana kuitenkin on siirtyminen uudempiin teknologioihin, kuten CAN-FDhen, jonka suurempi hyötykuorma mahdollistaa raskaampien turvaominaisuuksien käyttöönoton luonnollisemmin. Tästä huolimatta jo olemassa olevan autokannan turvaaminen vaatii yhä ratkaisuja.

Turvallisuustutkijat ovat ehdottaneet useita eri tapoja puolustautua hyökkäyksiä vastaan. Tässä työssä keskityttiin käsittelemään salausta, autentikointia ja tunkeutumisen havaitsemisjärjestelmiä. Rajauksen vuoksi, on mahdollista, että näiden keinojen lisäksi on tehokkaampia tai parempia tapoja paikata CANin haavoittuvuuksia. Kirjallisuudessa todetaan useaan kertaan CAN Classicin kohtaamat rajoitteet, jotka käsiteltiin luvussa 4. Nämä rajoitteet tekevät perinteisistä salauksen ja autentikoinnin keinoista käyttökelvottomia

Yksittäiset menetelmät eivät itsessään tarjoa täysvaltaista ratkaisua ilman omia pulmiaan, ja ne joutuvat tasapainottelemaan turvallisuuden ja nopeuden välillä. Kevyellä viesti autentikoinnilla saadaan estettyä tekeytymis- ja toistohyökkäyksiä, mutta ne väistämättäkin vaikuttavat väylällä tapahtuvan kommunikaation nopeuteen. [24]. Tunkeutumisen havaitsemisjärjestelmät puolestaan, erityisesti neuroverkkoihin pohjautuvat mallit, kykenevät havaitsemaan monimutkaisempia ja ennestään

tuntemattomia uhkia täysin passiivisesti. Tämä mahdollistaa elintärkeän nopeuden säilyttämisen viestinnässä. Näiden mallien tarkkuus testidatalla on vaikuttava, mutta ne tarjoavat vain osan ratkaisusta.

Merkittävin haaste ei olekaan uhkien havaitseminen, vaan niihin reagoiminen tavalla, joka ei vaaranna ajoneuvon matkustajia tai muuta liikennettä. Perinteisissä tietoverkoissa saastunut laite tai hyökkäyksen kohteena oleva yhteys voidaan eristää verkosta. Autossa tämä ei kuitenkaan ole mahdollista, sillä auton eri ohjausyksiköiden eristäminen tai estäminen voisi aiheuttaa vaaratilanteita. Vaikka koneoppimismallit olisivat erittäin tarkkoja, yksikin väärä hälytys voisi johtaa vakaviin seurauksiin.

6 Yhteenveto

Tässä tutkielmassa tarkasteltiin CAN Classic -tiedonsiirtoprotokollan tietoturvaa, keskittyen sen rakenteellisiin haavoittuvuuksiin sekä näiden torjumiseksi kehitettyihin moderneihin suojautumismenetelmiin. Työn tutkimuskysymykset jakautuivat kahteen osaan: ensimmäisessä kartoitettiin protokollan heikkouksia ja toisessa etsittiin ratkaisuja havaittujen uhkien torjumiseksi.

Vaikka CAN-väylä on nopea ja häiriösietoinen, sen alkuperäisessä suunnittelussa ei huomioitu nykypäivän tietoturvavaatimuksia. Tutkielmassa havaittiin, että protokollan suurimmat uhat johtuvat sisäänrakennetun salauksen ja autentikoinnin puutteesta yhdistettynä sen yleislähetyspohjaiseen rakenteeseen. Nämä ominaisuudet rikkovat suoraan tietoturvan CIA-mallin luottamuksellisuuden, eheyden ja saatavuuden periaatteita. Nämä haavoittuvuudet mahdollistavat esimerkiksi salakuuntelua ja palvelunestohyökkäyksiä.

Suojautumiskeinojen osalta tarkastelu rajattiin salaukseen, autentikointiin ja tunkeutumisen havaitsemisjärjestelmiin. Perinteisten kryptografisten menetelmien soveltaminen CAN Classic -verkkoon sen rajallisen laskentatehon ja tiukan kahdeksan tavun viestikoon vuoksi. Raskaat suojausmekanismit hidastavat aikakriittistä kommunikaatiota ajoneuvon ohjausyksiköiden välillä. Näiden rajoitteiden myötä erityisesti kone- ja syväoppimiseen, perustuvat IDS-järjestelmät nousivat esiin tehokkaimpina ratkaisuina, koska ne kykenevät havaitsemaan poikkeavuuksia passiivisesti lisäämättä verkkoon viivettä.

Luvussa 5 pohdittiin myös kuinka ajoneuvon tulisi käytännössä reagoida IDS-järjestelmän havaitsemaan uhkaan liikenteessä. Koska yksittäisten ohjausyksiköiden eristäminen verkosta tai niiden välisen kommunikaation estäminen voisi olla ajotilanteessa hengenvaarallista, pelkkä uhkien havaitseminen ei riitä, vaan rinnalle tarvitaan turvallisia reagointimekanismeja.

Lähdeluettelo

[1] A. S. Tanenbaum ja M. v. Steen, *Distributed systems: principles and paradigms*, 2nd ed. Upper Saddle RIiver, NJ: Pearson Prentice Hall, 2007, ISBN: 978-0-13-239227-3.

[2] T. Andreica, C.-D. Curiac, C. Jichici ja B. Groza, "Android Head Units vs. In-Vehicle ECUs: Performance Assessment for Deploying In-Vehicle Intrusion Detection Systems for the CAN Bus", *IEEE Access*, vol. 10, s. 95 161–95 178, 2022, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2022.3204746.

[3] S. Rajapaksha et al., "AI-Based Intrusion Detection Systems for In-Vehicle Networks: A Survey", *ACM Computing Surveys*, vol. 55, nro 11, s. 1–40, helmikuu 2023. DOI: 10.1145/3570954.

[4] Uttarakhand Technical University, G. Bora, S. Bora, S. Singh ja S. M. Arsalan, "OSI Reference Model: An Overview", *International Journal of Computer Trends and Technology*, vol. 7, nro 4, s. 214–218, tammikuu 2014, ISSN: 22312803. DOI: 10.14445/22312803/IJCTT-V7P151.

[5] CAN in Automation (CiA), *CAN CC*. viitattu 20. maaliskuuta 2026. url: https://www.can-cia.org/can-knowledge/can-cc.

[6] T. Chowdhury et al., "Safe and Secure Automotive Over-the-Air Updates", teoksessa *Computer Safety, Reliability, and Security*, B. Gallina, A. Skavhaug ja F. Bitsch, toim., Cham: Springer International Publishing, 2018, s. 172–187, ISBN: 978-3-319-99130-6. DOI: 10.1007/978-3-319-99130-6_12.

[7] O. Avatefipour ja H. Malik, *State-of-the-Art Survey on In-Vehicle Network Communication (CAN-Bus) Security and Vulnerabilities*, 5. helmikuuta 2018. DOI: 10.48550/arXiv.1802.01725. arXiv: 1802.01725[cs].

[8] P. Jing et al., "Revisiting Automotive Attack Surfaces: a Practitioners' Perspective", teoksessa *2024 IEEE Symposium on Security and Privacy (SP)*, ISSN: 2375-1207, toukokuu 2024, s. 2348–2365. DOI: 10.1109/SP54263.2024.00080.

[9] M. Bozdal, M. Samie ja I. Jennions, "A Survey on CAN Bus Protocol: Attacks, Challenges, and Potential Solutions", teoksessa *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*, s. 201–205. DOI: 10.1109/iCCECOME.2018.8658720.

[10] CAN in Automation (CiA), *History of CAN technology*. viitattu 19. maaliskuuta 2026. url: https://www.can-cia.org/can-knowledge/history-of-can-technology.

[11] D. Oladimeji, A. Rasheed, C. Varol, M. Baza, H. Alshahrani ja A. Baz, "CANAttack: Assessing Vulnerabilities within Controller Area Network", en, *Sensors*, vol. 23, nro 19, s. 8223, tammikuu 2023, ISSN: 1424-8220. DOI: 10.3390/s23198223. viitattu 29. maaliskuuta 2026. url: https://www.mdpi.com/1424-8220/23/19/8223.

[12] J. Liu, S. Zhang, W. Sun ja Y. Shi, "In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions", *IEEE Network*, vol. 31, nro 5, s. 50–58, 2017, ISSN: 1558-156X. DOI: 10.1109/MNET.2017.1600257.

[13] W. Voss, *A Comprehensible Guide to Controller Area Network*. Copperhill Media, 2008, Google-Books-ID: PU6ppO3XbUwC, ISBN: 978-0-9765116-0-1.

[14] Z. Wang ja F. A. Ghaleb, ”An Attention-Based Convolutional Neural Network for Intrusion Detection Model”, *IEEE Access*, vol. 11, s. 43 116–43 127, 2023, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2023.3271408.

[15] F. Fakhfakh, M. Tounsi ja M. Mosbah, ”Cybersecurity attacks on CAN bus based vehicles: a review and open challenges”, *Library Hi Tech*, vol. 40, nro 5, s. 1179–1203, marraskuu 2022, ISSN: 0737-8831. DOI: 10.1108/LHT-01-2021-0013.

[16] C. Lai, J. Ma, X. Wang, H. Zhou ja D. Zheng, ”A Novel Authentication and Key Agreement Scheme for In-Vehicle Networks”, *Ieee Transactions on Vehicular Technology*, vol. 74, nro 6, s. 9630–9644, kesäkuu 2025, Num Pages: 15 Web of Science ID: WOS:001512538000026, ISSN: 0018-9545, 1939-9359. DOI: 10.1109/TVT.2025.3540442.

[17] AUTOSAR, *Specification of Secure Onboard Communication*, 654, AUTOSAR Classic Platform, Standard Release R19-11, AUTOSAR, marraskuu 2019.

[18] N. Hediyal, B. P. Divakar ja K. Narayanaswamy, ”SCAN-C: a lightweight cryptographic algorithm to secure CAN communications in modern vehicles”, *Cybersecurity*, vol. 8, nro 1, s. 49, heinäkuu 2025, Num Pages: 30 Web of Science ID: WOS:001536522600001, ISSN: 2523-3246. DOI: 10.1186/s42400-024-00291-z.

[19] M. Müter ja N. Asaj, ”Entropy-based anomaly detection for in-vehicle networks”, teoksessa *2011 IEEE Intelligent Vehicles Symposium (IV)*, ISSN: 1931-0587, kesäkuu 2011, s. 1110–1115. DOI: 10.1109/IVS.2011.5940552.

[20] R. A. Kemmerer ja G. Vigna, ”Intrusion detection: a brief history and overview”, *Computer*, vol. 35, nro 4, s. 27–30, huhtikuu 2002, ISSN: 0018-9162. DOI: 10.1109/MC.2002.1012428.

[21] F. Oberti, S. Di Carlo ja A. Savino, ”CANDoSA: A Hardware Performance Counter-Based Intrusion Detection System for DoS Attacks on Automotive CAN Bus”, teoksessa *2025 IEEE 31st International Symposium on On-Line Testing and Robust System Design (IOLTS)*, ISSN: 1942-9401, heinäkuu 2025, s. 1–5. DOI: 10.1109/IOLTS65288.2025.11116886.

[22] A. R. Javed, S. U. Rehman, M. U. Khan, M. Alazab ja T. G. Reddy, ”CANintelliIDS: Detecting In-Vehicle Intrusion Attacks on a Controller Area Network Using CNN and Attention-Based GRU”, *Ieee Transactions on Network Science and Engineering*, vol. 8, nro 2, s. 1456–1466, kesäkuu 2021, Num Pages: 11 Web of Science ID: WOS:000680892400055, ISSN: 2327-4697. DOI: 10.1109/TNSE.2021.3059881.

[23] L. Yang, A. Moubayed ja A. Shami, ”MTH-IDS: A Multitiered Hybrid Intrusion Detection System for Internet of Vehicles”, *IEEE Internet of Things Journal*, vol. 9, nro 1, s. 616–632, tammikuu 2022, ISSN: 2327-4662. DOI: 10.1109/JIOT.2021.3084796.

[24] R. Rai, J. Grover, P. Sharma ja A. Pareek, ”Securing the CAN bus using deep learning for intrusion detection in vehicles”, *Scientific Reports*, vol. 15, nro 1, s. 13 820, huhtikuu 2025, Num Pages: 22 Web of Science ID: WOS:001471857800002, ISSN: 2045-2322. DOI: 10.1038/s41598-025-98433-x.