Juho Kajanto

Sybil-hyökkäykset ja niiden havaitseminen ajoneuvojen langattomissa verkoissa (VANET)

Tietotekniikan kandidaatintutkielma

2. kesäkuuta 2022

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Juho Kajanto

Yhteystiedot: jukrkaja@student.jyu.fi

Ohjaaja: Tytti Saksa

Työn nimi: Sybil-hyökkäykset ja niiden havaitseminen ajoneuvojen langattomissa verkoissa (VANET)

Title in English: Sybil attacks and their detection in Vehicular Ad hoc Networks

Työ: Kandidaatintutkielma

Opintosuunta: Tietotekniikka

Sivumäärä: 23+0

Tiivistelmä: Ajoneuvojen langaton verkko on teknologia, jolla mahdollistetaan ajoneuvojen välinen tietoliikenne. Kuin mikä tahansa avoin verkko, myös ajoneuvojen langattomat verkot ovat alttiita tietoturvahyökkäyksille. Kaikkein vaarallisin hyökkäys on Sybil-hyökkäys, joka mahdollistaa kaikkien muiden hyökkäysten tekemisen verkossa. Sybil-hyökkäysten havaitsemiseksi on ehdotettu useita erilaisia ratkaisuja, kuten naapuriajoneuvojen tarkkailuun tai signaalien vahvuuksien analysointiin perustuvat mallit. Erilaisia ratkaisuja tulee vertailla runsaasti keskenään, jotta toimivimmat ratkaisut saadaan implementoitua älyliikenteeseen.

Avainsanat: VANET, väliaikaisverkko, Sybil-hyökkäys, tietoturva

Abstract: Vehicular Ad hoc Network (VANET) is a technology, which is used to enable inter-vehicular communication. Like any other open network, VANETs are vulnerable to cyberattacks. The most dangerous attack is the Sybil attack, which enables the attacker to perform all other types of attacks in the network. There have been multiple propositions for the detection of Sybil attacks, like models that are based on observing neighbouring vehicles or analyzing signal strengths. Different propositions should be compared with each other so that only the most effective solutions could be implemented in intelligent transport.

Keywords: VANET, ad-hoc network, Sybil attack, security

Kuviot

Sisällys

1 Johdanto

Suomen tilastokeskuksen mukaan vuonna 2020 Suomessa tapahtui 3608 tieliikenneonnettomuutta (“Tieliikenneonnettomuudet” 2022). Onnettomuuksissa loukkaantui 4411 ihmistä, ja 223 menehtyi. Vaikka näihin lukuihin on laskettu mukaan myös kaikki kevyen liikenteen onnettomuudet, suurimmassa osassa tieliikenneonnetomuuksia osallisena on ollut moottoroitu ajoneuvo.

Yhtenä ratkaisuna tieliikenneonnettomuuksien vähentämiseksi on ehdotettu älykkäitä toisiinsa yhdistettyjä ajoneuvoja. Yhdistetyillä ajoneuvoilla pyritään mahdollistamaan tieliikenneympäristö, jossa ajoneuvojen aiheuttamia tapaturmia ei tapahtuisi enää ollenkaan (Wang, Zeng ja Yang 2006). Ajoneuvoja, jotka on varustettu omaa ympäristöään skannaavilla sensoreilla, ovat tietoisia välittömästä ympäristöstään, mutta toistensa kanssa paikkatietoja jakavat ajoneuvot olisivat jatkuvasti tietoisia toistensa tarkoista sijainneista. Toistensa paikkatiedot tietävät ajoneuvot voivat varoittaa kuljettajaa tai itsenäisesti väistää kolaritilanteita. Yhdistetyt ajoneuvot voivat myös jakaa toisilleen tietoa liikennetapahtumista ja ilmoittaa toisilleen tapahtuneista onnettomuuksista (Sharma ja Kaushik 2019).

Älykäs tieliikenne tuo kuitenkin mukanaan omat ongelmansa. Mikään verkko ei ole turvassa hyökkäyksiltä, ja ajoneuvojen väliset verkot sisältävät useita tieturvallisuuteen vaikuttavia haavoittuvuuksia (Sharma ja Kaushik 2019). Charlie Miller (2019) kuvailee artikkelissaan koetta, jossa hän kolleegansa Chris Valasekin kanssa hakkeroivat ja kaappasivat 2015 vuosimallin Jeep Cherokeen. Hyökkäyksessä he ottivat etäyhteyden ajoneuvon keskipaneeliin, jonka he uudelleenohjelmoivat lähettämään viestejä ajoneuvon osiin, joihin keskipaneelilla ei olisi saanut olla mahdollisuutta. Tällä tavoin Miller ja Valasek pääsivät käsiksi ajoneuvon ohjausjärjestelmiin, jonka jälkeen he ohjasivat auton ojaan. Vaikka kyseinen hyökkäys kohdistettiin vain yhteen tietyn malliseen ajoneuvoon, kokeen tekijät löysivät saman haavoittuvuuden usean muun autovalmistajan autoista.

Tämän tutkielman tavoitteena on tutustuttaa lukija yhdistettyjen ajoneuvojen tietoturvaongelmiin ja selvittää erilaisia menetelmiä hyökkäysten estämiseksi. Tutkielmassa keskitytään yhteen ajoneuvojen langattoman yhdistämisen menetelmään, sekä yhtenä vakavimpana pi-

dettävään tietoturvahyökkäystyyppiin. Valintoihin vaikuttivat aiheista tehtyjen akateemisten tutkimusten määrät. Lopuksi tutkielmassa esitellään muutama puolustautumiskeino hyökkäystä vastaan. Tutkielma suoritetaan kirjallisuuskatsauksena.

2 Ajoneuvojen yhdistämisen menetelmät

Ajoneuvojen välinen tietoliikenne on älykkään liikenteen ja liikennetelematiikan (ITS, engl. Intelligent Transportation System) perusta. Ajoneuvojen yhdistämiseksi on kehitetty kaksi teknologiaa, jotka ovat ajoneuvojen langattomat verkot (VANET, engl. Vehicular ad-hoc Network) sekä ajoneuvojen internet (IoV, engl. Internet of Vehicles). VANETia on kehitetty 2000-luvun alusta lähtien, ja se on näistä teknologioista vanhempi. Ajoneuvojen internet on uudempi teknologia, jota on kehitetty yhdistämällä VANETin sekä esineiden internetin teknologioita.

Ajoneuvojen internet rakentuu VANETin päälle, joten se sisältää kaikki VANETin teknologiat ja standardit. Gasmin ja Aliouatin (2019) mukaan ajoneuvojen internet voidaankin nähdä VANETin laajennuksena. Artikkelin mukaan ajoneuvojen internetin laitteisiin kuuluvat VANETissa olevien ajoneuvojen ja tienvarsilaitteiden lisäksi ajoneuvojen sensorit sekä muut tietoteknilliset laitteet, esimerkiksi auton omistajan matkapuhelin. Ajoneuvojen välisten yhteyksien muodostamisessa ajoneuvojen internet hyödyntää internetin verkkoja käyttäen samalla VANETin yhteyden muodostuksen standardeja.

2.1 VANET

VANET on teknologia, jolla mahdollistetaan älykkäiden ajoneuvojen välinen tietoliikenne. Sen toiminta pohjautuu tilapäisverkkojen eli MANETin (engl. Mobile ad-hoc Network) periaatteisiin, mutta on lopulliselta toiminnaltaan poikkeavaa (Bariah ym. 2015). VANET on muiden tilapäisverkkojen tapaan hajautettu verkko, joka ei tarvitse valmiiksi olemassa olevia rakenteita toimiakseen, vaan laitteet, joita verkossa kutsutaan solmuiksi, luovat verkkoja spontaanisti toistensa kanssa. VANET voidaankin nähdä MANETin erikoistettuna ilmentymänä, jossa verkkoja luovat laitteet ovat yksinomaan ajoneuvoja ja tienvarsilaitteita (Abdessamed ja Samira 2014).

Verkoissa toimivien solmujen tyyppien lisäksi VANET ja MANET eroavat toisistaan useilla eri tavoilla, joita Saini, Alelaiwi ja El Saddik (2015) erittelevät artikkelissaan tarkemmin. Toisin kuin MANET, jonka solmut ovat harvoin nopeassa liikkeessä, älykkäät ajoneuvot tar-

vitsevat toimiakseen verkon, joka pystyy ylläpitämään solmujen välisiä yhteyksiä ajoneuvojen ajaessa suurillakin nopeuksilla. VANET on suunniteltu toimimaan verkkojen rakenteiden ollessa jatkuvassa muutoksessa, ja ajoneuvojen välisten yhteyksien ollessa hyvin hetkellisiä. VANET on myös varusteltu MANETia paremmin tietoturvasuojilla verkkoihin kohdistuvien hyökkäysten havaitsemiseksi ja estämiseksi.

Ominaista ajoneuvojen langattomille verkoille ovat myös ajoneuvojen kuljettajien tekemien päätösten vaikutukset verkkojen rakenteisiin. Verkossa välittyvät viestit ja ajoneuvojen antamat ilmoitukset voivat muokata kuljettajan liikennekäyttäytymistä, mikä voi aiheuttaa muutoksia solmujen rakeenteellisessa järjestyksessä eli verkon topologiassa (Jakubiak ja Koucheryavy 2008).

Gasmi ja Aliouat (2019) määrittelevät VANET-yhteyksille kolme eri kommunikaatioyhdistelmää. Ajoneuvojen välinen yhteys V2V (engl. vehicle-to-vehicle), ajoneuvojen ja tienvarsilaitteiden välinen yhteys V2R (engl. vehicle-to-roadside), sekä ajoneuvojen ja infrastruktuurin välinen yhteys V2I (engl. vehicle-to-infrastructure), jolla artikkelissa tarkoitetaan ajoneuvojen yhteyttä laajempaan internetiin. Muissa artikkeleissa ei kuitenkaan jaeta samaa ajatusta yhdistelmistä, vaan useassa artikkelissa olemassa olevia kommunikaatioyhdistelmiä tunnistetaan vain kaksi: ajoneuvojen välinen yhteys, sekä ajoneuvojen ja tienvarsilaitteiden välinen yhteys. Ajoneuvojen ja tienvarsilaitteiden välisestä yhteydestä käytetään artikkeleissa termejä V2R ja V2I samaa asiaa tarkoittaen, esimerkiksi Mejri, Ben-Othman ja Hamdi (2014) käyttävät lyhennettä V2I, Grover ym. (2011) käyttävät lyhennettä V2R, ja Sharma ja Kaushik (2019) käyttävät molempia lyhenteitä ajoneuvojen ja tienvarsilaitteiden välisen yhteyden kuvaamiseksi. Ajoneuvojen ja infrastruktuurin välisessä yhteydessä infrastruktuurilla tarkoitetaan yleisesti tieinfrastruktuuria ja siihen kuuluvia tienvarsilaitteita. Saini, Alelaiwi ja El Saddik (2015) mukaan tienvarsilaitteet voivat kuitenkin olla yhteydessä internetiin. Ajoneuvojen suora yhteys laajempaan internetiin nähdään ennemmin ajoneuvojen internetin kuin VANETin osana.

2.2 WAVE

Langaton yhteys ajoneuvoympäristössä (WAVE, engl. Wireless Access in Vehicular Environment) on ensimmäinen kahdesta VANETissa käytetyistä standardeista. WAVEn toiminta sen ylemmillä tasoilla on määritelty IEEE 1609 -standardeissa, ja sen fyysisen ja MAC-tasojen toiminta määritellään langattomien lähiverkkojen standardissa IEEE 802.11p (Gasmi ja Aliouat 2019). Verkkopalveluiden toiminnan määrittelevässä standardissa IEEE 1609.3 WAVE kuvataan radioviestintää käyttävänä järjestelmänä, jonka tarkoitus on tarjota ajoneuvojen käyttäjille saumaton yhteys infrastruktuuriin sekä muihin ajoneuvoihin (“IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Networking Services” 2021).

WAVE järjestelmät toimivat 5.850-5.925 GHz taajuuksilla ja datasiirron nopeus niissä on 6-27 Mb/s. WAVE laitteiden tyypillinen maksimikantama on 300 metriä, mutta parhaimmillaan kantama voi yltää 1000 metriin asti. WAVE järjestelmät toimivat ajoneuvojen liikkuessa suurillakin nopeuksilla. (Gasmi ja Aliouat 2019; Xiang ym. 2009)

2.3 CALM

Viestintäyhteys maaradioille (CALM, engl. Communications Access for Land Mobiles) on toinen VANETissa käytetyistä standardeista. CALM tunnetaan myös nimellä "pitkän ja keskipitkän kantaman jatkuva radioliitäntä" (engl. Continuous Air interface for Long and Medium range). Standardin kehitti kansainvälisen standardisointijärjestö ISO:n teknillisen komitean 204 työryhmä 16, ja se rakentuu WAVEN tavoin IEEE 802.11p:n päälle (“CALM Concept” 2011). CALM käyttää yhteyksien muodostamiseen matkapuhelinten verkkoja, infrapunaa, sekä 60 GHz taajuuksia (Jakubiak ja Koucheryavy 2008; Gasmi ja Aliouat 2019).

3 Sybil-hyökkäys

Kuten mikä tahansa verkko, joka sallii yhteyksien muodostumisen laitteiden välille, myös ajoneuvojen langattomat verkot ovat alttiita tietoturvahyökkäyksille. Ajoneuvoihin kohdistuvien hyökkäysten seuraukset voivat kuitenkin poiketa tyypillisiin tietokoneisiin kohdistuvista hyökkäyksistä, sillä hyökkäysten kohteena on liikkuva ajoneuvo. Tilapäisverkot ovat hyökkäyksille erityisen alttiita, sillä verkot ovat hajautettuja ja yhteydet muodostuvat laitteiden välille spontaanisti (Abusalah, Khokhar ja Guizani 2008). Tilapäisverkkojen erikoistumana VANET perii kaikki niiden turvallisuusheikkoudet (Lin ym. 2008).

Ajoneuvojen langattomia verkkoja uhkaavat joukko useita erilaisia hyökkäyksiä, jotka Sharma ja Kaushik (2019) jaottelevat artikkelissaan aktiivisiin ja passiivisiin hyökkäyksiin. Heidän mukaansa aktiivinen hyökkäys vaatii toimiakseen hyökkääjältä aktiivista osallistumista, sillä näissä hyökkäyksissä tietoa sekä kerätään että syötetään kohteena olevaan verkkoon. Passiivinen hyökkäys ei tarvitse aktiivista osallistumista, sillä niissä verkoista vain kerätään tietoa. Tässä tutkielmassa käsiteltävät Sybil-hyökkäykset ovat aktiivisia hyökkäyksiä.

Vakavimpia aktiivisia hyökkäyksiä Sybil-hyökkäysten ohella ovat palvelunestohyökkäykset, joiden tarkoituksena on estää todellisten ajoneuvojen yhdistyminen verkkoihin (Kumar ja Sinha 2014). Tavoite pyritään saavuttamaan tukkimalla kohteena oleva verkko, joko ruuhkauttamalla verkko roskaviesteillä, tai estämällä viestien kulku viestiliikennettä häiritsevällä signaalilla (Rawat, Sharma ja Sushil 2012). Palvelunestohyökkäyksen voi myös suorittaa pudottamalla viestipaketteja verkosta, kuten Musta Aukko -hyökkäyksessä, jossa hyökkääjä kaappaa kaikki verkossa kulkevat viestit itselleen, eivätkä viestit saavuta tarkoitettuja kohteitaan (Sharma ja Kaushik 2019). Hyökkäyksiä, joissa pahantahtoinen osapuoli tunkeutuu kahden solmun väliin ja kuuntelee näiden viestejä, kutsutaan väliintulohyökkäyksiksi.

Hyökkäystä, jonka tarkoituksena on häiritä ja provosoida kohteena olevan ajoneuvon kuljettajaa, kutsutaan sosiaaliseksi hyökkäykseksi. Hyökkäyksessä kohdeajoneuvoon lähetetään viestejä, joiden tarkoituksena on järkyttää tai raivostuttaa kuljettaja (Kumar ja Sinha 2014). Sosiaalista häirintää voi olla myös ajoneuvon laitteiston häiritsevä manipulointi, kuten WIRED (2015)-julkaisun videolla näytetään.

3.1 Hyökkäyksen tavoitteet

Sybil-hyökkäys on hyvin monipuolinen hyökkäys, ja sen avulla voidaan toteuttaa useita erilaisia verkkoa häiritseviä toimenpiteitä. Kaikkien muiden hyökkäystyyppien mahdollistamisen lisäksi Sybil-hyökkäyksellä voidaan muokata verkkojen rakenteita, sillä jokainen luotu Sybil-solmu on yksi ajoneuvo lisää verkossa. Sakiz ja Sen (2017) toteavatkin Sybil-hyökkäyksen päätavoitteen olevan verkon rakenteen muovaaminen hyökkääjien tarkoituksiin sopivaan muotoon.

Rabieh ym. (2015) esittävät artikkelissaan kaksi mahdollista hyökkäysskenaariota, joissa Sybil-hyökkäyksellä pyritään vaikuttamaan verkon rakenteen kautta todellisten ajoneuvojen käyttäytymiseen. Molemmissa esimerkeissä hyökkäyksen tavoitteena on tyhjentää tie todellisista ajoneuvoista. Ensimmäisessä skenaariossa Sybil-solmut lähettävät verkkoon valheellisia varoitusviestejä, joissa ilmoitetaan tiellä tapahtuneesta onnettomuudesta. Olematon onnettomuus näyttäytyy ajoneuvoille todellisena, ja vaarallisia tieolosuhteita välttävät ajoneuvot pyrkivät kiertämään onnettomuuspaikan suotuisimmilla ajoreiteillä. Toisessa skenaariossa usea yhtäaikainen Sybil-solmu luo illuusion liikenneruuhkasta, kuten kuvassa 1 esitetään. Tässäkin tapauksessa todelliset ajoneuvot pyrkivät kiertämään ilmoitetun liikennetukoksen, jolloin vapautunut tienpätkä olisi hyökkääjille vapaassa käytössä.

3.2 Hyökkäyksen toiminta

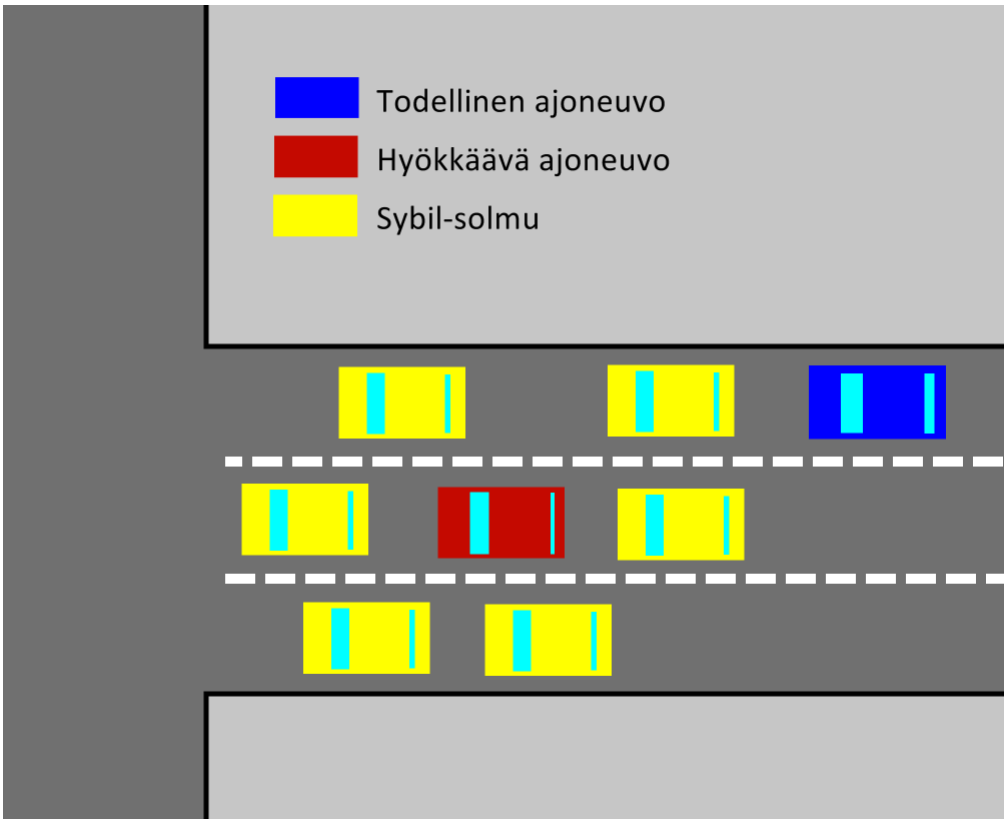
Sybil-hyökkäys on hyökkäys, jossa verkkoon liitetään solmu, jolla on useita identiteettejä (Douceur 2002). Ajoneuvojen langattomissa verkoissa ajoneuvot toimivat verkon solmuina, jolloin useita identiteettejä omistava solmu näyttäytyy verkossa useana ajoneuvona. Hyökkääjänä toimivan todellisen ajoneuvon luomia valheellisia solmuja kutsutaan Sybil-solmuiksi (Newsome ym. 2004). Nimi "Sybil"on peräisin samannimisestä kirjasta, joka kertoo dissosiatiivista identiteettihäiriötä sairastavasta potilaasta (Schreiber 1973).

Sybil-hyökkäystä pidetään yhtenä vakavimmista hyökkäyksistä, joita ajoneuvojen langattomia verkkoja kohtaan voidaan suorittaa (Hamed, Keshavarz-Haddad ja Haghighi 2018). Saman mielipiteen jakavat myös Grover ym. (2010), jotka täsmentävät Sybil-hyökkäysten vaarallisuutta sen mahdollistaessa kaikki muuntyyppiset hyökkäykset, kuten palvelunesto- ja

väliintulohyökkäykset. Sybil-hyökkäys on hyvin moniuloitteinen ja ominaisuuksiltaan laaja hyökkäystyyppi.

Newsome ym. (2004) loivat artikkelissaan luokittelun, jossa Sybil-hyökkäykset jaetaan ominaisuuksiensa perusteilla kolmeen eri kategoriaan, joita käsitellään ortogonaalisina ulottuvuuksina. Ensimmäinen näistä ulottuvuuksista määrittää Sybil-solmujen kyvyn kommunikoida: voivatko Sybil-solmut ja todelliset solmut kommunikoida verkossa keskenään. Toinen ulottuvuus määrittää Sybil-solmujen identiteettien perän: ovatko ne todellisilta ajoneuvoilta varastettuja vai kokonaan väärennettyjä. Kolmas ulottuvuus määrittää kuinka Sybil-solmut osallistuvat verkkoon: liittyvätkö kaikki identiteetit verkkoon useina solmuina (*yhtäaikainen hyökkäys*) , vai onko verkossa vain pieni määrä Sybil-solmuja kerrallaan, joiden identiteettejä hyökkääjä pystyy vaihtamaan (*eriaikainen hyökkäys*).

Sybil-hyökkäystä voi olla suorittamassa yksi tai useampi hyökkäävä solmu. Grover ym. (2010) tutkivat artikkelissaan hyökkääjien määrän vaikutusta verkoissa. He huomiovat verkossa liikkuvan viestinnän häiriintyvän enemmän mitä suurempi määrä hyökkääjiä verkossa on. Samassa artikkelissa he huomiovat myös kuinka hyökkääjien luomien Sybil-solmujen määrä vaikuttaa verkon toimivuuteen. Yhtäaikainen hyökkäys häiritsee verkon toimintaa enemmän kuin eriaikainen hyökkäys. He huomasivat myös kuinka hyökkäykset joissa Sybil-solmujen identiteetit ovat väärennettyjä ovat paljon tuhovoimaisempia kuin hyökkäykset joissa Sybil-solmujen identiteetit ovat todellisilta ajoneuvoilta varastettuja. Tämä johtuu siitä, että väärennetyillä identiteeteillä voidaan luoda uusia solmuja verkkoon, kun taas varastetut identiteetit eivät lisää uusien solmujen määrää. Tutkimuksessa (Grover ym. 2010) näin ollen todettiin väärennetyillä identiteeteillä suoritetun yhtäaikaisen hyökkäyksen olevan kaikkein vaarallisin Sybil-hyökkäyksen muoto.



Kuvio 1. Sybil-hyökkäyksessä simuloitu liikenneruuhka.

4 Sybil-hyökkäysten havaitseminen

Langattomien verkkojen sulavan toiminnan takaamiseksi on ehdotonta, että verkkoja uhkaavat hyökkäykset havaitaan ja eristetään verkoista mahdollisimman nopeasti. Newsomen ym. (2004) mukaan Sybil-hyökkäyksiltä suojautuminen perustuu vahvistukseen siitä, että jokaisella verkon fyysisellä solmulla on vain yksi identiteetti. Heidän mukaansa identiteetin vahvistuksen voi toteuttaa joko suorasti tai epäsuorasti. Suorassa vahvistuksessa verkon solmu testaa suoraan jollakin määritetyllä menetelmällä verkkoon liittyneen solmun validiuden. Epäsuorassa vahvistuksessa verkon valideiksi vahvistetut solmut voivat hyväksyä tai eristää epäilemänsä Sybil-solmut verkosta.

Newsome ym. (2004) esittävät artikkelissaan useita menetelmiä Sybil-hyökkäyksiltä suojautumiseksi, jotka Feng ym. (2017) kumoavat toimimattomiksi laajoissa ajoneuvojen langattomissa verkoissa. Ajoneuvojen langattomat verkot vaativat laajuutensa ja muuttuvuutensa takia nopeita ja tehokkaita tapoja havaita ja eristää hyökkääviä solmuja. Erilaisia menetelmiä on ehdotettu useita, joista tässä kirjoitelmassa käydään läpi muutama.

4.1 Naapuriajoneuvojen avulla

Grover ym. (2011) sekä Saggi ja Kaur (2015) ehdottavat Sybil-hyökkäysten havaitsemiseksi menetelmiä, joissa toistensa naapureina olevat ajoneuvot jakavat toisilleen tietoa itseään ympäröivistä ajoneuvoista. Vaikka menetelmät pohjautuvat samaan periaatteeseen, ne ovat toiminnaltaan hyvin erilaisia. Sybil-solmuja etsitään eri kriteereillä, ja verkoissa hyödynnetään eri laitteistoa.

Grover ym. (2011) kuvaa ajoneuvojen langattomissa verkoissa esiintyvän kahta erilaista naapuruutta, jotka ovat fyysinen naapuruus ja viestintänaapuruus. Fyysiset naapurit ovat solmuja, jotka sijaitsevat toistensa lähetysalueilla, ja voivat siten lähettää ja vastaanottaa toisilleen viestejä. Viestintänaapurit ovat solmuja, joiden lähetystehot ovat erisuuret, mistä johtuen viestien kulku on yksisuuntaista. Yksinkertaistetusti solmu 1 voi lähettää viestejä solmulle 2, mutta solmu 2 ei voi lähettää viestejä solmulle 1.

Saggin ja Kaurin 2015 esittelemä Sybil-hyökkäysten havainnointimenetelmä perustuu verkkoihin liittyvien solmujen vertaamiseen siinä jo oleviin todellisiksi vahvistettuihin solmuihin. Menetelmä hyödyntää laajasti tienvarsilaitteiden kykyä kerätä, analysoida ja tallentaa ajoneuvoilta kerättyä tietoa. Menetelmä vaatii myös, että ajoneuvot keräävät omista naapureistaan tietoa, jota ne jakavat eteenpäin tievarsilaitteille. Sybil-solmujen tunnistamiseen käytetään tienvarsilaitteiden keräämää tietoa, sekä ajoneuvojen vauhtiin pohjautuvaa kynnysarvoa.

Saggin ja Kaurin 2015 menetelmän alussa verkkoon saapuva solmu lähettää tienvarsilaitteille tervehdysviestin, jossa se kertoo oman tunnisteensa. Jos uuden solmun lähettämät tiedot ovat samat kuin jonkin uutta solmua naapuroivan solmun, uusi solmu eristetään Sybil-solmuna verkosta. Jos uuden solmun tiedot ovat ainutlaatuiset, sen nopeutta verrataan asetettuun kynnysarvoon. Jos kynnysarvo ylittyy, solmu todetaan Sybil-hyökkäykseksi ja eristetään verkosta. Muuten solmu merkitään verkossa todelliseksi ajoneuvoksi ja sen annetaan muodostaa yhteys muiden verkon solmujen kanssa.

Saggin ja Kaurin 2015 kuvaama menetelmä ei ole täydellinen. Tunnisteiden vertaamisella toisiinsa voidaan havaita Sybil-solmut, joiden identiteetti on todelliselta ajoneuvolta varastettu, mutta luotuja tunnisteita käyttävät solmut jäävät havaitsematta. Luotuja identiteettejä käyttävät solmut huomattaisiin vain, jos niiden vauhti olisi verkossa asetettua raja-arvoa suurempi. Solmujen vauhdin mittaaminen on kuitenkin jäänyt artikkelissa epäselväksi, eikä Sybil-solmujen epänormaalia vauhtia ole perusteltu.

Grover ym. (2011) esittävät artikkelissaan paljon vakuuttavamman menetelmän Sybil-hyökkäysten havaitsemiseksi. Toisin kuin Saggin ja Kaurin (2015) menetelmä, Groverin ym. menetelmä ei erottele varastettuja ja luotuja identiteettejä käyttäviä Sybil-solmuja toisistaan. Groverin ym. ehdottama Sybil-solmujen tunnistusalgoritmin toiminta on myös kuvattu ja selitetty tarkemmin. Heidän menetelmänsä perustuu oletukseen, jossa liikkuvassa liikenteessä todelliset ajoneuvot eivät viivy toistensa verkoissa pitkiä aikoja, vaan ajoneuvojen luontaisen liikehdinnän ja ajoneuvojen signaalivahvuuksien vaihteluiden takia ajoneuvojen naapurisolmut eivät pysy samoina pitkiä aikoja. Heidän menetelmänsä ei tarvitse tienvarsilaitteita toimiakseen, vaan ajoneuvot hoitavat naapureittensa seurannan itsenäisesti.

Groverin ym. ratkaisussa ajoneuvot lähettävät toisilleen säännöllisin väliajoin datapaketteja, jotka sisältävät sen lähettäneen solmun tiedot, sekä listan sen naapurisolmuista. Kun ajoneuvot ovat keränneet näitä datapaketteja tarpeeksi, pakettien sisältämät selvitykset naapurisolmuista ryhmitetään yhteen. Ajoneuvot jakavat ryhmitetyn tiedon naapurisolmuilleen, joita ajoneuvot vertaavat omiin havaintoihinsa omista naapureistaan. Jos naapurilistojen leikkauksessa ilmenee samoja solmuja pidemmän aikaa kuin annettu kynnysarvo, nämä solmut merkitään Sybil-solmuiksi.

Goverin ym. mukaan tällä menetelmällä pystytään havaitsemaan tehokkaasti samasta lähteestä tulevat hyökkäykset suurissa verkoissa, mutta pienemmissä verkoissa se tuottaa enemmän vääriä havaintoja. Feng ym. (2017) kritisoi menetelmää siitä, että ratkaisun toimivuus riippuu oletuksesta jossa verkon solmut lähettävät toisilleen luotettavaa dataa. Mikään ei estä Sybil-solmuja lähettämästä verkkoon valheellisia viestejä, joilla kaikkien solmujen löytämistä vaikeutetaan, tai joiden avulla hyökkääjä voi aloittaa uuden Sybil-hyökkäyksen.

4.2 Kerrosten välinen malli

Rabieh ym. (2015) esittävät artikkelissaan Sybil-hyökkäysten tunnistamisratkaisun, joka pohjautuu epäilyttävien solmujen ulosäänestämiseen haastepakettien avulla. He kritisoivat useita muita ratkaisuja siitä, että niissä oletetaan todellisten ajoneuvojen tunnisteiden olevan hakkerointivarmoja. Heidän ratkaisunsa on tehty toimimaan tilanteissa, joissa hyökkäävän solmun käyttämät identiteetit ovat todellisilta ajoneuvoilta varastettuja. Kerrosten välisyys tulee ajoneuvojen lähettämien haastepakettien luomisesta MAC tasolla ja lähetettämisestä fyysisellä tasolla.

Toimiakseen Rabiehin ym. ratkaisu vaatii verkon koostuvan neljästä osasta: ajoneuvoista, tienvarsilaitteista, Traficomiin verrattavissa olevasta valtiollisesta toimijasta, joka ylläpitää ajoneuvojen verkkojen toimivuutta ja turvallisuutta, sekä varmenneviranomaisesta, joka hallinnoi ajoneuvojen digitaalisia tunnisteita. Ajoneuvot lähettävät tienvarsilaitteille tasaisin väliajoin merkkivaloviestejä (engl. beacon packet), jotka sisältävät ajoneuvon uniikin varmenneviranomaisen myöntämän tunnisteen, aikaleiman viestin lähetyksestä, ajoneuvon vauhdin, sekä tieton omasta sijainnista. Tienvarsilaitteilla on suora yhteys liikenteen turvallisuusvi-

ranomaiseen.

Sybil-hyökkäysten käsittely tapahtuu Rabiehin ym. menetelmässä kolmessa osassa, jotka ovat hälytys, varmennus ja päätös. Kun verkossa havaitaan mahdollinen Sybil-hyökkäys (*hälytys*), havainnon tehnyt tienvarsilaite lähettää solmun vauhdista ja paikasta laskettuun solmun oletettuun uuteen sijaintiin haastepaketin (*varmennus*). Jotta syytetty solmu voisi ottaa sille lähetetyn haasteviestin vastaan, sen täytyy olla siirtynyt sille laskettuun uuteen sijaintiin. Haasteviestin vastaanottaneen ja siihen onnistuneesti vastanneen solmun syyte poistetaan. Jos solmua ei havaita sen oletetussa sijainnissa, solmu identifioidaan hyökkääväksi solmuksi. Tievarsilaite tähettää liikenteen turvallisuusviranomaiselle viestin, missä havaittua solmua syytetään Sybil-hyökkäyksen tekemisestä. Jos syytöksiä tulee tarpeksi paljon tietyssä ajassa, liikenteen turvallisuusviranomainen lähettää varmenneviranomaiselle pyynnön purkaa syytetyn ajoneuvon valtuudet (*päätös*).

Rabieh ym. (2015) luettelevat artikkelissaan myös muutamia tapoja Sybil-hyökkäysten tunnistamiseksi. Jos solmun ilmoitettu sijainti on kauempana kuin tienvarsilaitteen kantama, solmusta tehdään syytös. Jos kahden solmun ilmoittamat sijainnit ovat päällekkäisiä, molemmista ajoneuvoista tehdään syytös. Jos kahden tienvarsilaitteen välillä tielle ilmestyy uusia ajoneuvoja tyhjästä, näistä tehdään syytös. Jos solmun lähettämä viesti on lähetetty eri sijainnista mitä viestissä ilmoitetaan, solmusta tehdään syytös.

Rabiehin ym. esittämä ehdotus on suunniteltu tunnistamaan vain varastetuilla tunnisteilla tehtyjä hyökkäyksiä. Menetelmä kuitenkin huomioi kaikki epäilyttävästi käyttäytyvät solmut, ja varmenneviranomainen tekee väärennettyjen tunnisteiden käytöstä vaikeaa. Menetelmä hyödyntää vahvasti tienvarsilaitteita, jotka ovat kallis ja hyökkäyksille altis resurssi. Ratkaisun suunnittelijat haluaisivatkin luoda Sybil-hyökkäysten havainnointimenetelmän, jossa tienvarsilaitteita ei tarvittaisi ollenkaan.

4.3 Muutokset signaalien vahvuuksissa

Bouassida ym. (2009) ehdottama Sybil-hyökkäysten havainnointimenetelmä perustuu verkon solmujen paikallistamiseen niiden signaalinvoimakkuuksien avulla. Menetelmä vaatii toimiakseen verkon, jossa viestien lähetystehot on vakioitu, eli jokainen solmu lähettää vies-

tejä samalla teholla. Solmut joiden laskettu lähetysteho ei vastaa vakioitua tehoa identifioidaan epäilyttävinä solmuina. Menetelmä toimii kahdessa osassa, jonka ensimmäisessä osassa verkosta tunnistetaan epäilyttävät solmut, ja toisessa epäilyttävistä solmuista erotetaan Sybil-solmut ja ne luoneet hyökkäävät solmut.

Bouassidan ym. (2009) menetelmässä verkon solmut lähettävät verkossa tasaisin väliajoin merkkivaloviestejä, joista ilmenevät viestin lähettäjän digitaalinen tunniste sekä GPS-sijainti. Kun signaalin lähetysteho ja teho viestin saapuessa ovat tiedossa, voidaan näiden avulla laskea viestin lähettäneen solmun maksimietäisyys viestin vastaanottaneesta solmusta. Jos solmun ilmoittama sijainti ei vastaa laskettua maksimietäisyyttä, viestin lähettänyt solmu on käyttänyt vakiosta poikkeavaa tehoa, ja tämä solmu merkitään epäilyttäväksi solmuksi.

Bouassidan ym. (2009) menetelmässä hyökkäävien solmujen ja Sybil-solmujen erottamiseen käytetään geometrista analyysia. Analyysissä verrataan kahden epäilyttävän solmun ominaisuuksia keskenään, ja niistä lasketuista tuloksista selvitetään kumpi solmuista on hyökkäävä todellinen ajoneuvo ja kumpi Sybil-solmu. Bouassidan ym. suorittamien simulaatioiden perusteella menetelmä on tehokas, ja hyökkäävien solmujen ja Sybil-solmujen löytäminen on täsmällistä.

5 Yhteenveto

Tässä tutkielmassa tutustuttiin yhdistettyjen ajoneuvojen teknologioihin ja ajoneuvojen langattomiin verkkoihin kohdistuviin tietoturvahyökkäyksiin. Ajoneuvojen langattomia verkkoja kohtaan kohdistuvia hyökkäystyyppejä on monia, joista Sybil-hyökkäys todettiin kaikkein vaarallisimmaksi, sillä se mahdollistaa kaikki muut hyökkäystyypit. Tutkielmassa esiteltiin neljä eri Sybil-hyökkäysten havainnointimenetelmää, jotka kaikki poikkesivat toisistaan älyliikenteeseen liittyvien oletusten, sekä käytettyjen algoritmien ja teknologioiden osalta.

Tässä tutkielmassa käsiteltiin tarkemmin ajoneuvojen langattomia verkkoja, jotka ovat noussa olevan ajoneuvojen internetin perusta. Ajoneuvojen internet tuo mukanaan useita aikaisemmasta teknologiasta puuttuvia ominaisuuksia, jotka tuovat mukanaan omat tietoturvaongelmansa. Ajoneuvojen langattomissa verkoissa toimivat Sybil-hyökkäysten havainnointimenetelmät eivät välttämättä toimi ajoneuvojen internetissä. Useissa havainnointimenetelmissä käytetään myös toisistaan poikkeavia teknologioita, joten kaikkia niitä ei voida standardoidussa älyliikenteessä ottaa käyttöön. Uudet tulevat teknologiat mahdollistavat myös uusien hyökkäystapojen ja suojautumismenetelmien luonnin. Tässä tutkielmassa esiintuodut ratkaisut ovat toisistaan huomattavastikin eroavia ehdotuksia. Tulevaisuuden älyliikenteen laajempaa keskitettyä implementointia varten parhaimpien suojautumismenetelmien valitsemiseksi erilaisia suojautumismenetelmiä kannattaisi vertailla runsaasti keskenään.

Lähteet

Abdessamed, Derder, ja Moussaoui Samira. 2014. “Target Tracking in VANETs Using V2I and V2V Communication”. Teoksessa *2014 International Conference on Advanced Networking Distributed Systems and Applications,* 19–24. https://doi.org/10.1109/INDS.2014.11.

Abusalah, Loay, Ashfaq Khokhar ja Mohsen Guizani. 2008. “A survey of secure mobile Ad Hoc routing protocols”. *IEEE Communications Surveys Tutorials* 10 (4): 78–93. https://doi.org/10.1109/SURV.2008.080407.

Bariah, Lina, Dina Shehada, Ehab Salahat ja Chan Yeob Yeun. 2015. “Recent Advances in VANET Security: A Survey”. Teoksessa *2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall),* 1–7. https://doi.org/10.1109/VTCFall.2015.7391111.

Bouassida, Mohamed Salah, Giles Guette, Mohamed Shawky ja Bertrand Ducourthial. 2009. “Sybil Nodes Detection Based on Received Signal Strength Variations within VANET”. *International Journal of Network Security,* 9 (1): 22–33.

“CALM Concept”. 2011. Viitattu 15. heinäkuuta 2011. https://web.archive.org/web/20110715020929/http://www.isotc204wg16.org/concept.

Douceur, John. 2002. “The Sybil Attack”. Teoksessa *Peer-to-Peer Systems,* 251–260. https://doi.org/10.1007/3-540-45748-8_24.

Feng, Xia, Chun-yan Li, De-xin Chen ja Jin Tang. 2017. “A method for defensing against multi-source Sybil attacks in VANET”. *Peer-to-Peer Networking and Applications* 10 (2): 305–3014. https://doi.org/10.1007/s12083-016-0431-x.

Gasmi, Rim, ja Makhlouf Aliouat. 2019. “Vehicular Ad Hoc NETworks versus Internet of Vehicles - A Comparative View”. Teoksessa *2019 International Conference on Networking and Advanced Systems (ICNAS),* 1–6. Annaba, Algeria. https://doi.org/10.1109/ICNAS.2019.8807870.

Grover, Jyoti, Manoj Singh Gaur, Vijay Laxmi ja Nitesh Kumar Prajapati. 2011. “A Sybil Attack Detection Approach Using Neighboring Vehicles in VANET”. Teoksessa *Proceedings of the 4th International Conference on Security of Information and Networks,* 151–158. Sydney, Australia: Association for Computing Machinery. https://doi.org/10.1145/2070425.2070450.

Grover, Jyoti, Deepak Kumar, Sargurunathan Mohan, Manoj Gaur ja Vijay Laxmi. 2010. “Performance Evaluation and Detection of Sybil Attacks in Vehicular Ad-Hoc Networks”, 473–482. Heinäkuu. https://doi.org/10.1007/978-3-642-14478-3_47.

Hamed, Hamid, Alireza Keshavarz-Haddad ja Shapour Golbahar Haghighi. 2018. “Sybil Attack Detection in Urban VANETs Based on RSU Support”. Teoksessa *Iranian Conference on Electrical Engineering (ICEE),* 602–606. https://doi.org/10.1109/ICEE.2018.8472629.

“IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Networking Services”. 2021. *IEEE Std 1609.3-2020 (Revision of IEEE Std 1609.3-2016),* 1–210. https://doi.org/10.1109/IEEESTD.2021.9374154.

Jakubiak, Jakub, ja Yevgeni Koucheryavy. 2008. “State of the Art and Research Challenges for VANETs”. Teoksessa *2008 5th IEEE Consumer Communications and Networking Conference,* 912–916. https://doi.org/10.1109/ccnc08.2007.212.

Kumar, Ankit, ja Madhavi Sinha. 2014. “Overview on vehicular ad hoc network and its security issues”. Teoksessa *2014 International Conference on Computing for Sustainable Global Development (INDIACom),* 792–797. https://doi.org/10.1109/IndiaCom.2014.6828071.

Lin, Xiaodong, Rongxing Lu, Chenxi Zhang, Haojin Zhu, Pin-han Ho ja Xuemin Shen. 2008. “Security in vehicular ad hoc networks”. *IEEE Communications Magazine* 46 (4): 88–95. https://doi.org/10.1109/MCOM.2008.4481346.

Mejri, Mohamed, Jalel Ben-Othman ja Mohamed Hamdi. 2014. “Survey on VANET security challenges and possible cryptographic solutions”. *Vehicular Communications* 1 (2): 53–66. https://doi.org/https://doi.org/10.1016/j.vehcom.2014.05.001.

Miller, Charlie. 2019. “Lessons Learned from Hacking a Car”. *IEEE Design & Test* 36 (6). https://doi.org/10.1109/MDAT.2018.2863106.

Newsome, J., E. Shi, D. Song ja A. Perrig. 2004. “The Sybil attack in sensor networks: analysis amp; defenses”. Teoksessa *Third International Symposium on Information Processing in Sensor Networks, 2004. IPSN 2004,* 259–268. https://doi.org/10.1109/IPSN.2004.239019.

Rabieh, Khaled, Mohamed M. E. A. Mahmoud, Terry N. Guo ja Mohamed Younis. 2015. “Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs”. Teoksessa *2015 IEEE International Conference on Communications (ICC),* 7298–7303. https://doi.org/10.1109/ICC.2015.7249492.

Rawat, Ajay, Santosh Sharma ja Rama Sushil. 2012. “VANET: Security attacks and its possible solutions”. *Journal of Information and Operations Management* 3 (1): 301–304.

Saggi, Mandeep Kaur, ja Ranjeet Kaur. 2015. “Isolation of Sybil attack in VANET using neighboring information”. Teoksessa *2015 IEEE International Advance Computing Conference (IACC),* 46–51. https://doi.org/10.1109/IADCC.2015.7154666.

Saini, Mukesh, Abdulhameed Alelaiwi ja Abdulmotaleb El Saddik. 2015. “How close are we to realizing a pragmatic VANET solution? A meta-survey”. *ACM Computing Surveys* 48:1–40. https://doi.org/10.1145/2817552.

Sakiz, Fatih, ja Sevil Sen. 2017. “A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV”. *Ad Hoc Networks* 61 (maaliskuu). https://doi.org/10.1016/j.adhoc.2017.03.006.

Schreiber, Flora Rheta. 1973. *Sybil.* USA: Henry Regnery Company.

Sharma, Surbhi, ja Baijnath Kaushik. 2019. “A survey on internet of vehicles: Applications, security issues & solutions”. *Vehicular Communications* 20:100–182. https://doi.org/https://doi.org/10.1016/j.vehcom.2019.100182.

“Tieliikenneonnettomuudet”. 2022. Viitattu 18. huhtikuuta 2022. https://tieliikenneonnettomuudet.stat.fi/tieliikenneonnettomuudet_fi.html.

Wang, Fei-Yue, Daniel Zeng ja Liuqing Yang. 2006. “Smart Cars on Smart Roads: An IEEE Intelligent Transportation Systems Society Update”. *IEEE Pervasive Computing* 5 (4): 68–69. https://doi.org/10.1109/MPRV.2006.84.

WIRED. 2015. “Hackers Remotely Kill a Jeep on a Highway | WIRED”. Viitattu 3. toukokuuta 2015. https://www.youtube.com/watch?v=MK0SrxBC1xs.

Xiang, Weidong., Javier Gozalvez, Zhisheng Niu, Onur Altintas ja Eylem Ekici. 2009. “Wireless Access in Vehicular Environments”. *EURASIP Journal on Wireless Communications and Networking* 2009 (1). https://doi.org/https://doi.org/10.1155/2009/576217.