Tampereen ammattikorkeakoulu

Matkapuhelinohjaukset kulunvalvonnassa

Veeti Koski

OPINNÄYTETYÖ
Toukokuu 2023

Talotekniikka
Sähköinen talotekniikka

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Talotekniikan tutkinto-ohjelma
Sähköinen talotekniikka

KOSKI, VEETI:
Matkapuhelinohjaukset kulunvalvonnassa

Opinnäytetyö 28 sivua
Toukokuu 2023

Opinnäytetyön tarkoituksena oli tuottaa selkeä ja kattava tietopaketti puhelinliittymien avulla ohjattavista kulunvalvontalaitteista. Työssä perehdyttiin ensin olennaisilta osin puhelinstandardien historiaan ja niiden kehityksen luomiin mahdollisuuksiin IoT-laitteiden näkökulmasta. Lisäksi työhön tuotettiin käytännönläheinen selostus järjestelmien toteutuksesta, aina suunnittelusta käyttöön asti.

Puhelinliittymiä on käytetty etäohjausratkaisuissa jo vuosikymmeniä alkaen puhelinverkkojen digitalisoitumisesta ja GSM-teknologian yleistymisestä. Uusien matkapuhelinstandardisukupolvien säännöllinen ilmestyminen markkinoille on ajanut IoT-laitteiden kehitystä, ja ohjausmahdollisuudet ovat laajentuneet yksinkertaisista tekstiviestikomennoista pilvipalveluiden kautta tapahtuvaan laajaan hallintaan sekä monimuotoisiin järjestelmäintegraatioihin.

Kyseisen teknologian kehitys konkretisoituu muun muassa hajautetuissa ja itsenäisissä kulunvalvontalaitteissa, jotka ovat saavuttaneet laajaa suosiota viimeisen vuosikymmenen aikana. Kokonaisvaltaisia kulunvalvontajärjestelmiä edullisemmille ja erityisesti helppokäyttöisimmille ratkaisuille on tarvetta esimerkiksi taloyhtiöiden pysäköintihalleissa tai vuokratilakohteissa.

Puhelimien digitalisoitumisesta alkanut kehitys jatkuu toki tulevaisuudessakin, ja uusia standardeja ilmestyy jatkuvasti markkinoille. Tämän opinnäytetyön kirjoittamisen aikaan 5G:n käyttöönotto on jo alkanut kovalla vauhdilla, mikä saattaa tarkoittaa suurta mullistusta IoT-laitteiden maailmassa. Samaan tahtiin pyritään siivoamaan taajuusalueita poistamalla vanhoja standardeja käytöstä, mikä puolestaan luo uudenlaisia haasteita sekä uusien laitteiden suunnitteluun että käytössä olevien laitteiden päivittämiseen.

Asiasanat: kulunvalvonta, kulunhallinta, IoT, puhelinverkot, 2G, 3G, 4G

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Building Services Engineering
Electrical Systems

KOSKI, VEETI:
Cellular IoT Devices in Access Control Applications

Bachelor's thesis 28 pages
May 2023

The popularity of decentralized and inexpensive access control devices has been steadily rising since the inception of readily available cellular IoT. Regardless, most current instructional material only addresses extensive centralized access control systems. This can have the possible effect of hindering or even discouraging the implementation, and as an extension, the development of more practical systems.

The purpose of this thesis was to produce an information package, primarily to aid in designing and implementing modern decentralized access control systems, but also to further general awareness of the subject.

Information for the thesis was mainly gathered by conducting a broad literary review of mainly internet-based sources. This, combined with the author’s professional knowledge, created the theoretical framework of the thesis. Also, some amount of field research was conducted to gather information which was not readily available.

The primary objective for the thesis can safely be estimated to have been accomplished as the end result has the capability to function in the purpose that was set for it. The scope of the thesis was narrowed down on multiple occasions during the writing process, which resulted in some segments possibly being left incomplete. However, the result serves as a strong foundation for further efforts. This being said, the long-term and concrete benefit of the product cannot yet be evaluated at this stage, as it would require input from future readers.

Key words: access control, IoT, cellular networks, mobile networks, 2G, 3G, 4G

SISÄLLYS

LYHENTEET JA TERMIT

GSM (Global System for Mobile communications)	Toisen sukupolven käytetyin puhelinstandardi.
UMTS (Universal Mobile Communications System)	Kolmannen sukupolven käytetyin puhelinstandardi.
LTE (Long-Term Evolution)	Neljännen sukupolven käytetyin puhelinstandardi.
VoLTE (Voice over LTE)	LTE:n käyttämä puheensiirtotekniikka.
IoT	Internet of Things. Laitteiden kytkeminen internettiin.
LPWAN (Low-Power Wide Area Network)	Matalatehoinen pitkänmatkan langaton tiedonsiirtoverkko.
LTE-M / LTE-MTC (Long-Term Evolution-Machine Type Communication	LPWAN-teknologian standardi IoT käyttöön.
NB-IoT (Narrowband-Internet of Things)	LPWAN-teknologian standardi. Vielä vähätehoisempi kuin LTE-M.
Radiotaajuustunnistus (RFID)	Yksilöllisen radiosignaalin tuottava tunniste.

1 JOHDANTO

Tämän opinnäytetyön tarkoituksena on toimia kattavana tietopankkina ja suunnitteluapuna kevyiden puhelinliittymäohjattujen kulunvalvontajärjestelmien toteutuksessa. Kulunvalvontajärjestelmistä on helposti saatavilla runsaasti tietoa, mutta aiheen käsittely rajoittuu usein laajoihin ja korkean turvallisuustason järjestelmiin tai rikosilmoitusjärjestelmiin. Tämä jättää suuren aukon tietoisuuteen, sillä markkinoilla on paljon kysyntää edullisille, yhtä oviaukkoa ohjaaville laitteille, joiden tarkoituksena on sekä rajoittaa asiattomien kulkua että helpottaa loppukäyttäjien kulkemista. Työssä avataan laitteiden toiminnan mahdollistavaa tekniikkaa mahdollisimman helppolukuisesti ja tuodaan esille myös yleisimpiä kohdetyyppejä sekä kulunvalvontajärjestelmien suunnitteluperusteita.

Mobiiliohjatut IoT-laitteet alkavat olla arkipäivää lähes kaikkialla, eikä kulunvalvonta ole poikkeus. Etähallittavat ja reaaliaikaista valvontaa tarjoavat järjestelmät ovat viimeisen vuosikymmenen aikana lisääntyneet huomattavaa tahtia. Erityisesti itsenäiset, vain yhtä kulkuväylää vahtivat kulunvalvontalaitteet ovat muuttuneet yleiseksi ilmiöksi. Kyseiset laitteet mahdollistavat varteenotettavia ratkaisuja erityisesti väliin putoaviin kohteisiin, joissa on tarvetta perustason kulunhallinnalle, mutta ei ole perusteltua sijoittaa kalliisiin ja käyttökoulutusta vaativiin laitteisiin. Tässä työssä tullaan siis olennaisesti keskittymään yksinkertaisiin, lähinnä helppokäyttöisyyttä lisääviin järjestelmiin, eikä niinkään korkean turvallisuustason kulunvalvontajärjestelmiin.

2 MATKAPUHELINSTANDARDIT

Tässä kappaleessa käsitellään matkapuhelinstandardien kehitystä ja sen vaikutusta etenkin IoT-laitteisiin. Standardit jaetaan sukupolviin, joilla on tarkat vaatimukset standardien suorituskyvylle ja ominaisuuksille. Uuden sukupolven aloittavia standardeja on ilmestynyt markkinoille noin kymmenen vuoden välein alkaen ensimmäisen sukupolven järjestelmistä 1980-luvun alussa ja päättyen toistaiseksi viidenteen sukupolveen (Laine-Lassila 2018; Best 2014). Tässä opinnäytetyössä keskitytään erityisesti välille 2G-4G, sillä kyseiset sukupolvet ovat toistaiseksi olennaisimpia IoT-laitteiden näkökulmasta.

2.1 2G

2G on yleinen nimitys toisen sukupolven matkapuhelinstandardeille, joista ylivoimaisesti käytetyin on GSM. 2G on tärkeä vaihe puhelinteknologian kehityksessä, sillä se oli ensimmäinen täysin digitaalinen sukupolvi, joka korvasi aikaisemmat analogiset järjestelmät. Digitalisaatio on avannut mahdollisuudet tiedonsiirrolle, kuten tekstiviesteille ja sähköposteille. Myös internetin selailu on mahdollista 2G-liittymillä, mutta tiedonsiirtonopeudet ovat niin hitaita, että tämä ei ole kovin käytännöllistä. (Laine-Lassila 2018)

Toisen sukupolven standardit ovat vielä nykyäänkin hyvin laajalti käytössä, vaikka 3- ja 4G:n käyttö on kasvanut räjähdysmäisesti. 2G-liittymiä on luonnollisesti vielä huomattava määrä normaalissa matkapuhelinkäytössä, mutta niillä on myös mahdollista toteuttaa yksinkertaisia tekstiviesteillä tai puheluilla ohjattuja järjestelmiä. Tämä on nykyäänkin täysin riittävä ratkaisu esimerkiksi portin kulunhallintaan, jossa portti avataan soittajalle puhelinnumeron tunnistamiseen perustuvan kulkuluvan pohjalta. Tämä on kuitenkin hyvin rajoittunut ratkaisu ja koska nykyaikaisissa ohjainlaitteissa olevat modeemit tukevat useita sukupolvia, ei niissä tyypillisesti käytetä enää GSM-liittymiä.

2.2 3G

Maailmanlaajuisesti käytetyin kolmannen sukupolven teknologia on Universal Mobile Telecommunications System, UMTS. UMTS otettiin käyttöön 2000-luvun puolivälissä ja sen kehityksessä pyrittiin erityisesti lisäämään liittymiin käytännöllisen datansiirron, jollaista GSM ei tukenut (Laine-Lassila 2018). Vaikka internettiin yhdistäminen olikin mahdollista jo GSM-liittymillä, UMTS:in suuremmat tiedonsiirtonopeudet mahdollistivat käytännöllisemmän internetin selailun ja myös monimutkaisemmat etäohjausjärjestelmät.

IMT-2000-standardipaketti edellyttää 3G-verkkoilta seuraavia tiedonsiirtonopeuksia: 144 Kbps ajoneuvoympäristössä, 384 Kbps jalankulkuympäristössä ja 2048 Kbps rakennetussa ympäristössä (ITU-T 1999, 7, taulukko 1). Tämä on avannut huomattavia mahdollisuuksia IoT-laitteiden kehityksessä, ja samalla myös kulunvalvontalaitteiden etäohjaus on kehittynyt. Etäohjaukset eivät enää rajoitu yksinkertaisiin ja hitaisiin komentoihin, kuten tekstiviesteihin. Järjestelmät voivat olla jatkuvassa yhteydessä verkkoon ja ohjausta sekä valvontaa voidaan toteuttaa reaaliaikaisena, nyt myös monipuolisilla käyttöliittymillä.

2.3 4G

Neljättä sukupolvea ei ole määritetty samalla tavoin, kuin IMT-2000 määrittelee 3G:n, joten 4G:n nimellä markkinoidaan monenlaisia standardeja. Näistä käytetyimpänä standardina edustaa LTE eli Long-term Evolution, jota on yleisesti pidetty pikemminkin todellisten 4G-teknologioiden edeltäjänä. (ITU News 2022) Neljännen sukupolven kehitystä ajoi erityisesti ajatus mullistavista tiedonsiirtonopeuksista. 3G oli onnistunut nimittäin lisäämään 2G:stä puuttuneen tiedonsiirron, mutta ei tarpeeksi hyvin vastatakseen digitalisaation myötä jatkuvasti kasvaviin datamääriin. (Best 2014.)

LTE:in teoreettinen latausnopeus on 100 Mbps, mikä on huomattavasti enemmän, kuin IMT-2000:n 3G:ltä vaatimat nopeudet (European Telecommunications Standards Institute 2018). Todellisuudessa nopeudet ovat tyypillisesti kuitenkin paljon pienempiä, koska 4G:lle ei ole minkään standardipaketin vaatimia pienim-

piä tiedonsiirtonopeuksia. 4G-verkot ovat myös ruuhkautuneet valtavasti käyttäjämäärien räjähdysmäisen kasvun ja teleoperaattoreiden riittämättömien toimien myötä. Suomessa 4G-yhteyksien keskimääräinen huippunopeus on laskenut noin 7 Mbps. (West, Fagerström & Siironen 2020.) Esimerkiksi teleoperaattori Elisa arvioi LTE-liittymiensä miniminopeudeksi vain 5 Mbps, joten vaihteluväli on selkeästi valtava (Elisa Oyj 2013).

2.4 NB-IoT ja LTE-M

NB-IoT ja LTE-M ovat omia matkapuhelinpohjaisia LPWA-verkon standardeja. LPWA-verkko on yleinen nimitys pitkän matkan ja matalan datamäärän verkoille. Liittymät on tarkoitettu erityisesti vastaamaan kasvavaan IoT-laitemäärään, toisin kuin muut 3G-5G standardit, joissa on pyritty mahdollisimman korkeisiin tiedonsiirtonopeuksiin keskipitkillä ja jopa lyhyillä matkoilla. (Bagur 2023.) Matalien tiedonsiirtonopeuksien vuoksi liittymät säästävät energiaan ja ne ovat myös tavallisia liittymiä edullisempia, mikä mahdollistaa useiden erillisten IoT-laitteiden kustannustehokkaan liittämisen mobiiliverkkoihin.

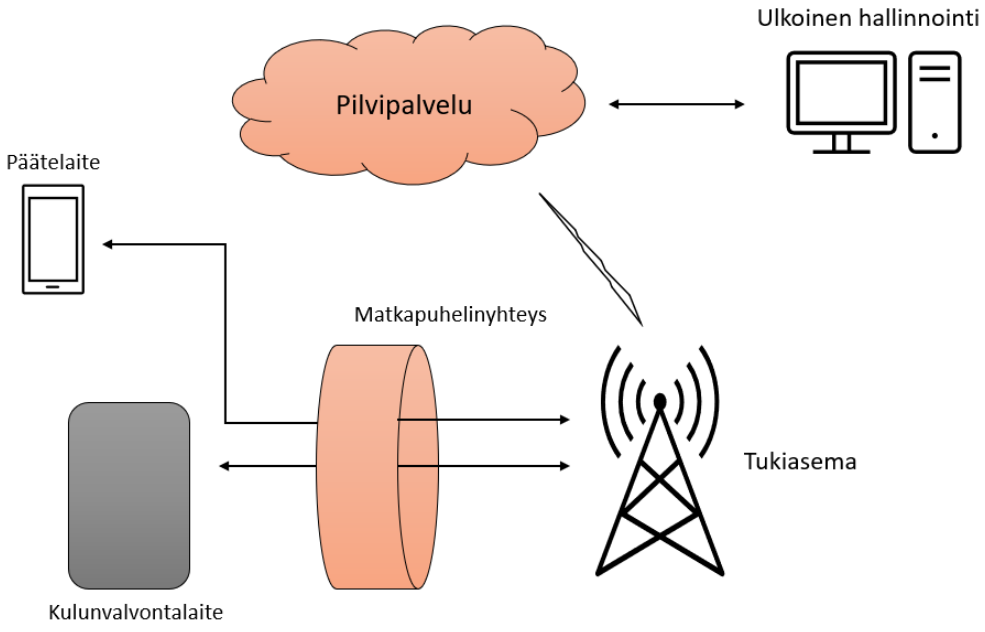
NB-IoT on optimoitu äärimmäisen pienille datamäärille ja se on soveltuvin lähinnä satunnaisesti pieniä datapaketteja lähettäville laitteille, kuten sensoreille. Akkukäyttöisten laitteiden toiminta-aikaa voidaan myös venyttää mahdollisimman pitkäksi NB-IoT:n mahdollistaman minimaalisen virrankulutuksen ansiosta. (Telia 2020.)

LTE-M on suunniteltu hieman suurempia datanopeuksia tarvitseville IoT-laitteille. Tällaisia laitteita ovat muun muassa jatkuvan verkkoyhteyden tarvitsevat ohjain- tai valvontalaitteet, matalaresoluutioiset kamerat tai puhelinsoittoja vastaanottavat laitteet. Käytössä on huomioitava, että LTE-M ja NB-IoT ovat viidennen sukupolven standardeja, joten vanhempien laitteiden modeemit eivät tue kyseisiä liittymiä. (Telia 2020.)

3 KULUNVALVONTAJÄRJESTELMÄ

Kulunvalvontajärjestelmät ovat perinteisesti olleet keskitettyjä järjestelmiä, joissa koko kiinteistön toimilaitteita hallitsee yksi keskus. Tiedonsiirto järjestelmän sisällä on tyypillisesti hoidettu verkkokaapeloinnilla ja hallinta on hoidettu paikallisella palvelimella. (ST 665.10 2016, 8) Keskitetyt järjestelmät ovat ylimitoitettuja pieniin 1–3 valvontapisteen kiinteistöihin ja niiden kustannustehokkuus paraneekin vasta suuremmissa kohteissa. IoT:n yleistyminen ja puhelinstandardien kehittyminen on mahdollistanut yksittäisten ohjainlaitteiden turvallisen ja edullisen yhdistämisen verkkoon. Tällaisten laitteiden tapauksessa hallinta on siirretty yleensä laitevalmistajien ylläpitämiin pilvipalveluihin. Tämä mahdollistaa laitteiden hallinnan reaaliaikaisesti ja erittäin turvallisesti.

Kuviossa 1 on esitetty yksinkertaistettu malli puhelinverkkoon liitetystä kulunvalvontalaitteesta. Laite yhdistetään verkkoon SIM-kortin avulla, kuten mikä tahansa muukin mobiililaite. Käyttäjien päätelaitteet luovat yhteyden kulunvalvontalaitteeseen suoraan puhelinverkon kautta ja kulunvalvontalaitteelle päivitetään aktiiviset kuluoikeudet esimerkiksi pilvipalvelun kautta. Pilvipalvelun käyttöliittymänä voi toimia tehtävään luotu internetsivu, jolloin kulunvalvontalaitetta voi hallita miltä tahansa internettiin yhdistetyltä päätelaitteelta.



KUVIO 1. Kulunvalvontalaitteen toiminta puhelinverkossa. (Veeti Koski 2023)

3.1 Tyypilliset käyttökohteet ja -tavat

Tyypillisimpiä kevyestä sekä etähallittavasta kulunvalvonnasta hyötyviä kohteita ovat matalan turvallisuustason tilat ja rakennukset, joiden käyttäjäryhmä on joko suuri tai kenties olennaisemmin, nopeasti muuttuva. Etähallitut järjestelmät mahdollistavat kulkuoikeuksien muuttamisen reaaliaikaisesti, jolloin uusien ja vanhenevien kulkulupien hallinta helpottuu suunnattomasti. Perinteinen fyysinen avainhallinta siirtyy esimerkiksi verkkoselaimen kautta tapahtuvaksi digitaaliseksi avainhallinnaksi. Kulkuluvat voidaan sitoa lähes mihin tahansa tunnisteeseen, mikä on digitaalisesti luettavissa. Tyypillisesti kulkulupia asetetaan puhelinnumeroille, rekisterinumeroille, RFID-tunnisteille, UHF-tunnisteille ja PIN-koodeille (ST-käsikirja 11 2016, 39). Näistä selkeästi turvallisin ratkaisu on puhelinnumerokohtainen kulkulupa, sillä se on yksilöllinen ja nauttii jo valmiiksi puhelinstandardien tietoturvasta. Toki tämän tasoista kulunvalvontaa hyödyntävissä kohteissa harvemmin on tarvetta erittäin korkeaan turvallisuustasoon, joten kaikki edellä mainitut metodit ovat täysin käyttökelpoisia. Etähallitut kulunvalvontajärjestelmät vain parantavat esimerkiksi PIN-koodien tehokkuutta, koska käyttäjäkohtaisia koodeja on helppo asettaa ja niitä voidaan myös vaihtaa kätevästi halutuin väliajoin. Eräs jatkuvasti yleistyvä ohjaustapa on puhelinsovellukset. Tyypillisesti kulunvalvontajärjestelmiin kuuluvaan pilvipalveluun on helppo integroida rajapinta loppukäyttäjän päätelaitteen kanssa, mikä mahdollistaa ovien avaamisen napin painalluksella, mutta kuitenkin puhelinstandardien turvallisuudella.

Tällaisen tekniikan luomista mahdollisuuksista hyötyvät tyypillisesti muun muassa seuraavanlaiset kohteet:

- Taloyhtiöt
- Vuokrapysäköintiyritykset ja muut pysäköintihallit
- Urheilu- ja kerhotilat
- Maan- ja lumenkaatopaikat
- Vuokratilayritykset
- Varastot
- Teollisuuslaitokset
- Tukut ja muut tavarantoimituksen solmukohdat
- Vuokramökit ja AirBnB -kohteet
- Joissakin tapauksissa myös Hotellit

Porttien ja ovien ohjaus tapahtuu yleensä yksinkertaisesti laitteen antamalla reletiedolla, joten järjestelmä on hyvin joustava. Tämän seurauksena ohjaaminen ei rajoitu vain kulkuväyliin, vaan järjestelmällä voidaan toteuttaa muutakin automaatiota. Lähes jokaisessa pysäköintihallissa on nykyään sähköautojen latausasemia ja esimerkiksi niiden käyttöä voidaan rajata tai rahastaa helposti samalla järjestelmällä.

3.2 Suunnittelu

3.2.1 Tarveselvitys

Ensimmäisenä askeleena järjestelmän suunnittelussa on tarveselvitys, jonka tarkoituksena on selvittää kohteeseen optimaalisin toteutus. Heti aluksi on järkevää tehdä tarkka rajaus vastaamalla esimerkiksi seuraaviin kysymyksiin:

Mihin järjestelmää on tarkoitus käyttää?
Käytetäänkö järjestelmää pääosin rikoksentorjuntaan, kulunrajoittamiseen vai halutaanko ensisijaisesti helpottaa kulkemista, jolloin esimerkiksi autosta ei tarvitsisi nousta nosto-oven avaamiseksi.

Mikä on vaadittava turvallisuustaso?

Turvallisuustason tarvetta voidaan arvioida kohteessa säilytettävän omaisuuden arvolla ja kohteen riskialttiudella joutua hyökkäyksen kohteeksi. Erityisesti suojauksen taso ja kohteen sijainti vaikuttavat riskialttiuteen.

Mitkä ovat kohteen kriittiset pisteet?

Kriittiset pisteet ovat heikkoja kohtia kuorisuojauksessa, kuten avoimia kulkuväyliä, jotka tulee tunnistaa ja lisätä kulunvalvonnan piiriin tai poistaa kokonaan käytöstä.

Mikä on valvontapisteiden määrä?

Valvontapisteet ovat kriittisiä pisteitä, jotta on päädytty sijoittamaan kulunvalvonnan piiriin. Suuri valvontapisteiden määrä nostaa kustannuksia ja järjestelmän monimutkaisuutta.

Mikä on odotettu käyttäjämäärä?

Hyvin pienillä ja muuttumattomilla käyttäjämäärillä ei yleensä ole tarvetta perinteisiä lukitusjärjestelmiä monimutkaisemmille ratkaisuille.

Kuinka usein käyttäjät ja kulkuluvat vaihtuvat?

Vaihtuvuus lisää tarvetta helposti hallittaville laitteille.

Miten järjestelmän hallinta hoidetaan?

Hallinta sisältää sekä järjestelmän toiminnan ylläpidon eli huollot ja päivitykset sekä avainhallinnan.

Mikä on järjestelmän budjetti?

Budjetoinnissa tulee ottaa huomioon järjestelmän hinnan lisäksi muun muassa asennuskustannukset ja mahdollisten ylläpitopalveluiden hinta.

3.2.2 Toteutussuunnittelu

Kevyet kulunvalvontajärjestelmät ovat luonnostaan helppo toteuttaa, ja ne eivät vaadi suuria valmisteluja kohteessa. Yksinkertaisimmillaan laitteet tarvitsevat vain sähkönsyötön, mikä saadaan portti- ja nosto-oviympäristöissä yleensä suoraan porttikoneikolta. Yksittäiset, puhelinverkon kautta toimivat laitteet, eivät tarvitse edes verkkokaapelointia. Näidenkin järjestelmien suunnittelussa on kuitenkin otettava huomioon muutamia yleispäteviä seikkoja.

Toimiva ja kustannustehokas kulunvalvonta tarvitsee aina perustakseen hyvän kuorisuojauksen. Kuorisuojauksella tarkoitetaan kohteen ”kuoren” eli ulkoreunan kykyä rajoittaa kulkua. Tämä sisältää siis kulkuväylien lukumäärän ja kuoren vahvuuden. Jokainen kulkuväylä on lisättävä kulunvalvontaan tai vapaa kulku ulkoa käsin on muuten estettävä. Mitä vähemmän valvottavia kulkuväyliä on, sitä edullisemmaksi kokonaisuus tulee. (ST-käsikirja 11 2016, 69)

Lisäksi langattomia yhteyksiä hyödyntävissä järjestelmissä signaalin kuuluvuus on erittäin kriittinen edellytys sulavalle toiminnalle. Signaalin vahvuuteen vaikuttavat erityisesti suuret betoniset tai metalliset massat antennin ympärillä. Näiden kriteerien pohjalta erityisesti pysäköintihallit ja tiiviisti rakennetut alueet voivat olla haastavia kohteita. Puhelinyhteyksiä hyödyntäessä myös tukiasemien etäisyys ja suuntaus suhteessa vastaanottavaan antenniin on suuri kuuluvuuteen vaikuttava tekijä. Tämän lisäksi tukiasemien kuuluvuus vaihtelee ympäristön olosuhteiden ja aseman kuormituksen mukaan, jonka seurauksena mobiililaitteet ovat alttiita hyppimään tukiasemien välillä parempaa kuuluvuutta etsiessään. (Traficom 2019, 4)

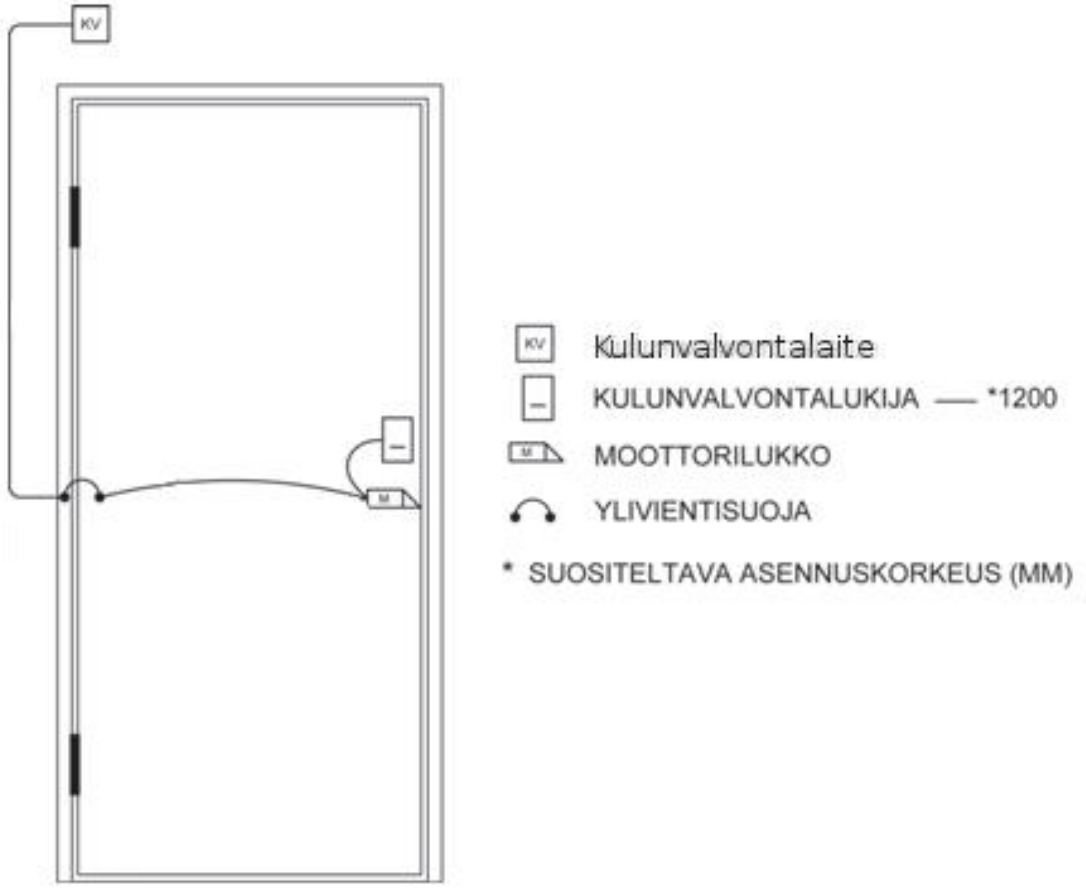
Suunnittelussa on otettava myös huomioon kulunvalvonnan vaikutus kohteeseen, eikä vain kohteen vaikutus kulunvalvontaan. Suomen rakentamismääräyskokoelmassa E1 määritellään seuraavasti: ”Uloskäytävien ja niihin johtavien tilojen ovien tulee olla hätätilanteessa helposti avattavissa” ja ” Kulunvalvonnan järjestelyt eivät saa estää turvallista poistumista rakennuksesta” (Ympäristöministeriö 2011, 32). Ovet on siis pystyttävä avaamaan sisäpuolelta ilman kulkuoikeuksiakin. Tämä on erittäin tärkeä huomio, mutta tyypillisesti vaatimus toteutuu

itsestäänkin, sillä harvassa kohteessa olisi muutenkaan tarvetta kaksisuuntaiselle kulunvalvonnalle. Ohjatut ovet toteutetaan pääsääntöisesti sähköisesti vapautettavilla vastaraudoilla, joten lukon avaus sisäpuolelta tapahtuu normaalisti sähkökatkonkin aikana. Mikäli lukon sähköiselle avaukselle on tarvetta myös sisäpuolelta, voidaan järjestelmään lisätä avausnappi tai jatkuvasti lukon tai vastaraudan auki pitävä avauskytkin. Pysäköintihalleissa nosto-ovien ja puomien sisäpuolisessa avauksessa käytetään tyypillisimmin joko ajoneuvon tunnistavaa tutkaa tai induktiosilmukkaa. Näissäkin tapauksissa ovi on toki saatava vian sattuessa avattua myös mekaanisesti.

3.3 Toteutus

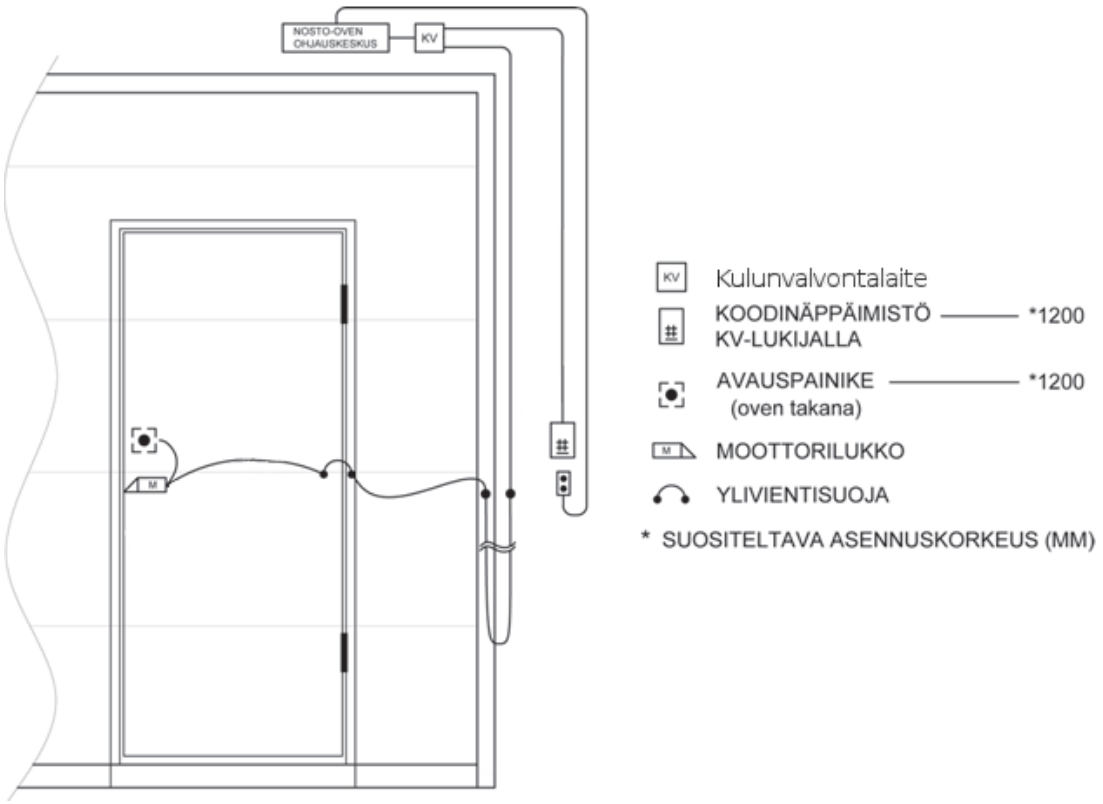
Suunnitteluvaiheen jälkeen alkaa järjestelmän toteutuksen käyttöön pano. Tämän opinnäytetyön käsittelemät järjestelmät ovat yleensä niin yksinkertaisia, että urakat eivät myöskään ole vaativia. Urakoitsijalla tulee tosin olla turvallisuusalan elinkeinolupa ja järjestelmän asentavilla työntekijöillä tulee olla turvasuojaajakortit (Laki yksityisistä turvallisuuspalveluista 2015, 60 §). Esimerkiksi tavallisilla sähköurakointiyrityksillä ei yleensä ole tarvittavia lupia kulunvalvontajärjestelmien asentamiseen. On kuitenkin hyvin yleistä, että laitetoimittajina tyypillisesti toimivat lukkoliikkeet järjestävät myös asennuksen ja tarvittaessa myös järjestelmän ylläpitopalvelut.

Kuviossa 2 on esitetty varsin tavanomainen moottorilukollinen oviympäristö. Toteutus on hyvin yksinkertainen, koska itsenäinen kulunvalvontalaite ei tarvitse muuta kuin virransyötön, mikä voidaan helpoimmassa tapauksessa ottaa vaikka läheiseltä pistorasialta. Kohteesta ja laitteesta riippuen erillisen antennin asentaminen voi tosin olla tarpeen.



KUVIO 2. Moottorilukollinen oviympäristö (ST-käsikirja 11. Kulunvalvonta- ja murtoilmaisujärjestelmät 2016, 62, muokattu).

Kuviossa 3 on esitetty tavallinen nosto-oviympäristö, joka on liitetty kulunvalvonnan piiriin. Nosto-ovessa on integroitu moottorilukollinen käyntiovi. Hyvin yleisesti käyntiovi löytyy nosto-oven vierestä, mutta toiminta on täysin sama. Tässä tapauksessa käyntioveen on myös suunniteltu avausnappi. Nosto-ovella on omat ohjausnappinsa, joilla ovea voidaan ohjata kulunvalvontajärjestelmästä riippumatta.



KUVIO 3. Nosto-ovi yhdistetyllä kulkuovella (ST-käsikirja 11. Kulunvalvonta- ja murtoilmaisujärjestelmät 2016, 63, muokattu).

Kuvassa 1 on esimerkki valmiista, kulunvalvonnan piirissä olevasta nosto-oviympäristöstä. Kuvaan on numeroimalla merkitty keskeisiä portti-/nosto-oviympäristöistä löytyviä laitteitta. Kuvan kohteessa on hyvin tyypillinen nosto-oviratkaisu, mikä löytyy varsin monesta paikasta. Kulunvalvontalaitteet ovat täysin itsenäisiä ja ne antavat vain yksinkertaisia avauskäskyjä nosto-oven ohjauskeskukselle.

KUVA 1. Erään pysäköintihallin lamellinosto-oven ohjainlaitteet. (Kuva: Veeti Koski 2023)

Kuvassa esitetyt laitteet:

1. Puhelinohjattu kulunvalvontalaite
2. Nosto-oven ohjauskeskus
3. Rekisteritunnistuskameran ohjainlaite
4. Rekisteritunnistuskamera
5. RF-lukija/PIN-koodinäppäimistö ja elektroninen avainpesä
6. Avainpesän ohjainlaite

Erikoisena ratkaisuna rekisteritunnistuskameralla on oma ohjainlaitteensa, vaikka yleensä tämä kaltaiset ratkaisut pystytään hoitamaan yhdellä laitteella. Kohteeseen on myös ajansaatossa kertynyt useampien eri valmistajien laitteita, jotka eivät ole keskenään yhteensopivia tai yhteensovitettuja, joten laitteita on kertynyt paljon seinälle.

3.4 Ylläpito

3.4.1 Pääkäyttäjä

Kaikki kulunvalvontajärjestelmät tarvitsevat aina vähintään yhden pääkäyttäjän. Pääkäyttäjän tehtävänä on järjestelmän käyttäjien kulkulupien hallinta eli avainhallinta. Ennen avainhallinnan on voinut hoitaa oikeastaan kuka tahansa luottohenkilö, mutta uuden lain johdosta yritysten harjoittama kulunvalvontajärjestelmän hallinta ja kulkuoikeuksien muokkaaminen on vaatinut vuodesta 2019 alkaen turvallisuusalan elinkeinoluvan ja turvasuojauskortin. Tämä voi vaikeuttaa esimerkiksi taloyhtiöiden toimintaa, joissa avainhallinnan hoitaa ammatti-isännöitsijä tai huoltoyhtiö, sillä kulunvalvontajärjestelmän digitaalinen avainhallinta on edellä mainittujen edellytyksien puuttuessa ulkoistettava turvallisuusalan elinkeinoluvan omaavalle toimijalle. (Laki yksityisistä turvallisuuspalveluista 2017, 60 §; Rasimus ym. 2019, 56; Poliisi 2020.)

3.4.2 Tietoturva

Tietoturva koostuu useasta eri kerroksesta, joihin sisältyy muutakin kuin tiedon suojaamista ulkoisilta uhilta. Tietoturva voidaan kiteyttää kolmeen ominaisuuteen: tiedon luottamuksellisuuteen, saatavuuteen ja eheyteen. Tiedon luottamuksellisuudella tarkoitetaan luvattomien tahojen pääsyn estämistä tietoihin. Tiedon saatavuus sen sijaan kuvaa luvan omaavien tahojen tietoihin käsiksi pääsyn varmistamista. Eheydellä tarkoitetaan tiedon tarkkuutta ja varmuutta. (SFS-EN ISO/IEC 27000:2020, 10 & 13) Tietoturva on siis paljon muutakin kuin pelkästään ulkoisilta uhilta suojautumista. Tässä kappaleessa tarkastellaan kulunvalvontalaitteiden ja osittain myös puhelinstandardien tietoturvaa.

Tietoturvasta ja sen toteuttamisesta on asetettu vaatimuksia muun muassa Tietosuojalaissa 5.12.2018/1050, Henkilötietolaissa 523/1999 ja EU:n verkko- ja tietoturvadirektiivissä 2016/1148 (ST 710.02 2019, 4). Säädöksistä huolimatta kulunvalvontalaitteiden tietoturva on varsin usein laiminlyöty kohteissa, joissa turvallisuustaso ei ole kovin korkea ja laitteista ei juuri välitetä. Esimerkiksi taloyhtiöt ovat hyvin alttiita kyseiselle kohtalolle, sillä isännöitsijöiden ja huoltoyhtiöiden nopean vaihtuvuuden vuoksi kulunvalvontajärjestelmien toiminnasta tai jopa olemassaolosta ei monesti ole tietoakaan. Puhelinliittymillä ohjatut järjestelmät ovat erinomainen ratkaisu tällaisten kohteiden kulunhallintaan, sillä puhelinstandardien tietoturvaominaisuudet sietävät huomattavasti paremmin säännöllisen ylläpidon puutetta kuin esimerkiksi taloyhtiöiden kellareista usein löytyvät tavalliset reitittimet, jotka tarvitsevat säännöllisiä tietoturvapäivityksiä pysyäkseen turvallisina. Yleinen ilmiö on myös se, että reitittimien ja yksinkertaisten IoT-laitteiden oletus salasanoja ei vaihdeta, mikä johtaa välittömästi verkon vaarantumiseen. Mitään luottamuksellista tietoa käsittelevää laitetta ei tulisi kytkeä yleisiin ja huonosti ylläpidettyihin verkkoihin. (Avast Software s.r.o 2019, 10.)

Vaikka yksittäisillä hyökkääjillä ei olisi motiivia satunnaisen taloyhtiön häiritsemiselle, esimerkiksi automatisoidut bottiverkot, eli yleisemmin botnetit, etsivät jatkuvasti heikkouksia käytännössä kaikista internettiin yhdistetyistä laitteista. Bottiverkot koostuvat lukuisista haittaohjelmien tartuttamista internettiin yhdistetyistä laitteista, jotka voidaan keskitetysti alistaa hyökkäävän tahon käyttöön.

Puhelinverkkojen käyttämät yhteydet nauttivat tarpeeksi hyvistä salauksista, joten vastaava toiminta ei ainakaan toistaiseksi ole käytännöllistä puhelinverkoissa. Tämän seurauksena jopa vanhemmilla puhelinstandardeilla on nykypäivänkin normeilla melko hyvät tietoturvaominaisuudet, ja yhdistettynä tiedon vähäiseen arkaluonteisuuteen tai haluttavuuteen, järjestelmät ovat yleensä erittäin hyvässä turvassa hyökkäyksiltä. (Pilkey 2016; F-secure 2017.)

GSM-teknologia käyttää verkon salauksessa A5-suvun algoritmeja. Aluksi käytössä oli pääasiallisesti A5/1-algoritmi, jonka murtaminen on jo monesti osoitettu helpoksi (Gendrullis, Novotný, & Rupp 2008, 1 & 16; Timberg 2013). Myöhemmin myös GSM-standardiin on lisätty kolmannen sukupolven standardien käyttämä vahvempi A5/3-algoritmi, joka perustuu monimutkaisempaan KASUMI-salaukseen. Vaikka A5/3 on selkeä parannus A5/1-algoritmiin verrattuna, on siitäkin jo löydetty teoreettisia heikkouksia, joilla salauksen murtaminen voi olla tietyissä olosuhteissa mahdollista (Dunkelman, Keller & Shamir 2010, 21). Salauksien purkaminen vaatii kuitenkin vaivaa, jolloin ne luovat kynnyksen hyökkääjille ja A5/3-salauksesta ei ole vielä osoitettu sellaisia heikkouksia, että niitä voitaisiin purkaa suuria määriä kerralla. 4G ja 5G standardeissa on edetty suuria hyppyjä tietoturvassa. 4G standardeja varten kehitetyt salausjärjestelmät AES-CTR, SNOW 3G ja ZUC ovat osoittautuneet varsin turvallisiksi ja niiden käyttöä onkin suoraan jatkettu 5G standardeissa. (Mattson, J., Comak, P. & Karakoç, F. 2021.)

Yksi puhelinteknologian tehokkaimmista tietoturvaominaisuuksista on kuitenkin alusta alkaen 2G:n käytössä ollut Subscriber Identity Module, eli tutummin SIM-kortti ja 3G-5G:n käytössä oleva USIM, eli Universal Subscriber identity Module. Yksinkertaistettuna, SIM- tai USIM-kortti sisältää yksilöllisen tunnisteen, jolla käyttäjä autentikoidaan aina tukiasemaan yhdistettäessä. (European Telecommunications Standards Institute 2020) Tätä ominaisuutta on hyödynnetty varsin tehokkaasti myös kulunvalvonnassa, sillä usein tunnisteena käytetty puhelinnumero on sidottu SIM-korttiin, joten se nauttii myös SIM-kortin luotettavuudesta ja yksilöllisyydestä.

3.4.3 Tietoturvan hallinta

Tietoturvan hallinta on tärkeä kulunvalvontajärjestelmän mukanaan tuoma tehtävä. Käyttäjien tiedot ja järjestelmän lokitiedot on säilytettävä asianmukaisella tavalla, jolloin ulkopuolisilla ei ole pääsyä tietoihin. Tietoturvan hallintaan vaikuttavat toimenpiteet on hyvä sopia jo suunnitteluvaiheessa tai viimeistäänkin toteutusvaiheessa. Järjestelmien fyysiset osat ja erityisesti niiden käyttämät etäyhteydet tulee suojata asianmukaisesti. (Rasimus ym. 2019, 33.)

4 TULEVAISUUS

Teknologian kehitys on edennyt kaikilla aloilla valtavina harppauksina viimeisen 150 vuoden aikana eivätkä puhelinteknologiat ole poikkeus. Ainoastaan kolmessakymmenessä vuodessa puhelinverkkojen digitalisoitumisen jälkeen elämme massiivisen IoT ”vallankumouksen” aikaa kun puhelinverkot kattavat jo syrjäseudutkin ja puhelinliittymiä on maailmassa enemmän kuin ihmisiä (International Telecommunications Union 2021a, 2021b). Ja vaikka nyt viidennen sukupolven kehityksen aikaan vaikuttaa siltä, että vihdoinkin on päästy melko tasapainoiseen tilaan puhelinstandardien kehityksessä, ei vauhti silti tule varmastikaan hidastumaan. On siis täysin sattumanvaraista mitä tulevaisuus tuo IoT:n kannalta, mutta tässä kappaleessa on tuotu esille muutamia lähitulevaisuuden olennaisia muutoksia.

4.1 3G-verkkojen lopettaminen

3G-verkkojen lopettamista on suunniteltu jo pitkään niiden jäädessä jatkuvasti vähemmälle käytölle. 3G:stä pyritään eroon pitkälti kustannussyistä, mutta myös siksi, että 3G-verkkojen taajuusalueet saataisiin 4G:n ja tulevaisuudessa myös 5G:n käyttöön (Lahtinen 2022). Tämän opinnäytetyön kirjoittamisen aikana 3G-verkkojen lopettaminen on jo kovassa vauhdissa ympäri maailmaa. Suomessa 3G-verkkoja ylläpitävät teleoperaattorit Elisa, Telia ja DNA, joista jokainen on ilmoittanut poistavansa 3G-verkkonsa käytöstä vuoden 2023 loppuun mennessä. (DNA Oyj 2021; Telia Company 2021; Elisa Oyj 2022.)

3G-verkkojen lopettaminen voi osoittautua ongelmalliseksi IoT-järjestelmien kannalta. Esimerkiksi laite, joka käyttää puhelinsoittoa ohjaukseen, on tehnyt sen 2G- tai 3G-verkkojen kautta, sillä 4G-verkot eivät tue perinteisiä piirikytkentäisiä puheluita. Puhelut siirtyvät 4G-verkon yli VoLTE-teknologialla, jota 3G-modeemit eivät tue (Oommen 2016). Seurauksena monia IoT-laitteita joudutaan joko kokonaan korvaamaan, tai tarvitaan laajoja ohjelmisto- ja komponenttipäivityksiä. Toisaalta 3G-modeemit tukevat tyypillisesti myös 2G-liikennettä, joten yksinkertaisemmat soitto- tai SMS-ohjaimet selviävät muutoksista siirtymällä 2G-verkkoon. Toki on huomioitava, että 2G-verkkojenkin sulkemista on suunniteltu jo hyvin pitkään, vaikka se ei näytäkään kovin todennäköiseltä lähitulevaisuudessa. GSM

on vuosikymmeniä toiminut pomminvarmana turvaverkkona uudempien standardien alla, ja sen poistuminen käytöstä on äärimmäisen epätodennäköistä ennen kuin 4G ja 5G ovat saavuttaneet GSM:n kattavuuden ja vakauden.

4.2 5G ja tulevat sukupolvet

Kovan kehityksen seurauksena näyttää siltä, että viidennen sukupolven standardeilla on mahdollista vihdoin saavuttaa tilanne, jossa puhelinverkko vastaa kaikkiin nykypäivän tarpeisiin. Teknologia kehittyy ja leviää tosin siihen tahtiin, että 5G voi edeltäjiensä tapaan jäädä alimitoitetuksi tulevaisuudessa. 5G mahdollistaa erittäin nopeat tiedonsiirtonopeudet ja se sisältää LPWAN-standardeja IoT-laitteiden tarpeisiin. Ongelmina ovat toistaiseksi verkon kattavuus Suomessa, verkon pieni kapasiteetti kasvaviin käyttäjämäärin nähden, ja IoT-näkökulmasta ennen kaikkea päätelaitteiden jäljessä laahaava kehitys.

5 POHDINTA

Opinnäytetyön ensisijaisena tarkoituksena oli lukijaystävällisen ja helposti ymmärrettävän tietopaketin kokoaminen, vastapainoksi varsin haastavasta aiheesta löytyville hajanaisille tiedonrippeille. Elämme tälläkin hetkellä niin kutsuttua IoT-vallankumousta, jonka seurauksena IoT-laitteita on maailmalla arviolta jo yli 15 miljardia ja määrän on arvioitu kaksinkertaistuvan vuoteen 2030 mennessä. Tästä huolimatta tietoisuus aiheesta seuraa kaukana perässä. Erityisesti kuluttajien keskuudessa tieto IoT-laitteiden hyödyistä on viime vuosina levinnyt nopeasti, mutta esimerkiksi ymmärrys haitoista ja vaaroista vaikuttaa paikoittain olevan jopa olematonta. Tämän vuoksi uusia teknologioita kehittäessä on äärimmäisen tärkeää pyrkiä myös lisäämään ymmärrystä aiheesta, tehtävä, johon myös tämä opinnäytetyö luotiin.

Työn voidaan sanoa pääosin onnistuneen, sillä se noudattelee pitkälti asetettuja tavoitteita. Ensisijaiseksi tavoitteeksi asetettiin yleishyödyllisen tietopaketin tekeminen, jonka on helppo arvioida onnistuneeksi, sillä työ saatiin kokonaisuudessaan vietyä maaliin asti. Toisaalta jälkikäteen tarkasteltuna, paikoittain melko suppeaksikin rajatun aiheen käsittelyssä ei välttämättä päästy toivotulle syvyydelle. Aihe on toki niin laaja, ettei sitä tässä työssä olisi voitukaan kokonaisuudessaan käsitellä, mutta kuitenkin herää kysymys; käytiinkö esimerkiksi ammattilaisen mielestä yksinkertaisissa asioissa tarpeeksi syvällä, jotta niin sanottu maallikkokin voisi sen ymmärtää? Tämä on ongelma, joka on seurausta melko kunnianhimoisesti rajatusta kohdeyleisöstä. Vaikka kohdeyleisö laajennettiin myös aiheesta täysin tietämättömiin, työtä tehdessä seurattiin hieman ristiriitaisesti oletusta, jonka mukaan lopullisen tuotteen lukijat omaisivat entuudestaan edes pienen ymmärryksen aiheen perusteista.

Työn lopullista hyötyä, muille kuin tekijälle itselle, on luonnollisesti vaikea arvioida. Onko tämänkaltaiselle tietopaketille arvioiden mukaisesti tarvetta? Entä onko työ helposti saavutettavissa? Tällaisille kysymyksille on vaikea löytää vastausta ilman ulkopuolista palautetta.

LÄHTEET

Avast Software s.r.o. 2019. Avast Threat Landscape Report. Viitattu 3.4.2023. https://cdn2.hubspot.net/hubfs/486579/Avast_Threat_Landscape_Report_2019.pdf

Bagur, J. 2023. LPWAN (Low-Power Wide-Area Networks) 101. Arduino Documentation 20.02.2023. Verkkosivu. Viitattu 28.2.2023. https://docs.arduino.cc/learn/communication/low-power-wide-area-networks-101

Best, J. 2014. The race to 5G: Inside the fight for the future of mobile as we know it. Verkkosivu. Viitattu 6.3.2023. https://www.techrepublic.com/article/does-the-world-really-need-5g/

DNA Oyj. 2017. Tietoliikennealan sanastoa. Verkkosivu. Viitattu 27.2.2023. https://corporate.dna.fi/talous/raportit/sanasto

DNA Oyj. 2021. DNA sulkee 3G-verkkonsa vuoden 2023 loppuun mennessä. Verkkosivu. Viitattu 25.1.2023. https://www.sttinfo.fi/tiedote/dna-sulkee-3g-verkkonsa-vuoden-2023-loppuun-mennessa?publisherId=1881&releaseId=69916236

Elisa Oyj. 2013. Elisan mobiiliverkon nopeudet. Verkkosivu. Viitattu 6.3.2023. https://elisa.fi/asiakaspalvelu/nettiliittymat/verkon-nopeudet/

Elisa Oyj. 2022. 3G poistuu käytöstä vuoden 2023 aikana - siirrymme kohti uudempaa teknologiaa. Verkkosivu. Viitattu 14.1.2023. https://elisa.fi/3g/

Mattson, J., Comak, P. & Karakoç, F. 2021. The evolution of cryptography in mobile networks and how to secure them in the future. Ericsson Blog 29.6.2021. Verkkosivu. Viitattu 3.4.2023. https://www.ericsson.com/en/blog/2021/6/evolution-of-cryptographic-algorithms

European Telecommunications Standards Institute. 2018. 4th Generation (LTE). Verkkosivu. Viitattu 6.3.2023. https://www.etsi.org/technologies/mobile/4g

European Telecommunications Standards Institute. 2020. SIM. Verkkosivu. Viitattu 3.4.2023. https://www.etsi.org/technologies/sim

F-secure Oyj. 2017. Botnet. Verkkosivu. Viitattu 17.3.2023. https://www.f-secure.com/v-descs/articles/botnet.shtml

Gendrullis, T., Novotný, M. & Rupp, A. 2008. A Real-World Attack Breaking A5/1 within Hours. Teoksessa Oswald, E. & Rohatgi, P. (toim.) Cryptographic Hardware and Embedded Systems – CHES 2008. CHES 2008. Lecture Notes in Computer Science, vol 5154. Springer, Berlin, Heidelberg. Viitattu 14.1.2023. https://doi.org/10.1007/978-3-540-85053-3_17

International Telecommunication Union. 1999. SERIES Q: SWITCHING AND SIGNALLING: Signalling requirements and protocols for IMT-2000. Teoksessa Framework for IMT-2000 networks. Sarja Q. Viitattu 23.1.2023. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Q.1701-199903-I!!PDF-E

International Telecommunication Union. 2021a. Subscriptions. Verkkosivu. Viitattu 30.3.2023. https://www.itu.int/itu-d/reports/statistics/2021/11/15/subscriptions/

International Telecommunication Union. 2021b. Mobile network coverage. Verkkosivu. Viitattu 30.3.2023. https://www.itu.int/itu-d/reports/statistics/2021/11/15/mobile-network-coverage/

ITU News. 2022. An inside look at mobile broadband standards development. International Telecommunication Union 2022. Verkkosivu. Viitattu 6.3.2023. https://www.itu.int/hub/2022/02/mobile-broadband-standards-imt-5g/

Kärkkäinen, H. 2021. Telia paljasti aikataulun 3g:n alasajolle – vaikuttaa peruspuhelimiin ja mökkikäyttöön. Ilta-Sanomat 1.2.2021. Luettu 14.1.2023. https://www.is.fi/digitoday/mobiili/art-2000007775217.html

Lahtinen, M. 2022. Suomen 3G-verkot suljetaan vuoden 2023 aikana, 2G lähivuosina. FiCom ry 12.12.2022. Verkkosivu. Viitattu 25.1.2023. https://ficom.fi/ajankohtaista/uutiset/suomen-3g-verkot-suljetaan-vuoden-2023-aikana-2g-lahivuosina/

Laine-Lassila, S. 2018. Langattomat sukupolvet 1G, 2G, 3G, 4G, 5G. FiCom ry 15.06.2018. Verkkosivu. Viitattu 14.1.2023. https://ficom.fi/ajankohtaista/uutiset/langattomat-sukupolvet-1g-2g-3g-4g-5g/

Laki yksityisistä turvallisuuspalveluista 21.8.2015/1085. Viitattu 9.3.2023. https://www.finlex.fi/fi/laki/ajantasa/2015/20151085#L5

Oommen, R. 2016. 3G and 4G – Voice calls on an LTE network – Implementation and Challenges. LinkedIn 2.5.2016. Verkkosivu. Viitattu 25.1.2023. https://www.linkedin.com/pulse/3g-4g-voice-calls-lte-network-implementation-richie-sam-oommen

Pilkey, A. 2016. What's a Mirai Botnet Doing With My Router? F-secure blog 30.11.2016. Verkkosivu. Viitattu 17.3.2023. https://blog.f-secure.com/whats-a-mirai-botnet-doing-with-my-router/

Poliisi. 2020. Turvallisuusalan elinkeinolupa. Verkkosivu. Viitattu 9.3.2023. https://poliisi.fi/turvallisuusalan-elinkeinolupa

Rasimus, T. (toim.), Rossi, A., Nuutinen, A., Hovatta, T., Hovinen, R. & Arenius, K. 2019. Turvaa oikein -opas. 2. uud. painos. Espoo: Turva-alan yrittäjät ry. Viitattu 9.3.2023.

SFS-EN ISO/IEC 27000:2020. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Suomen Standardoimisliitto SFS ry. 2. painos. Viitattu 14.3.2023.

ST 665.10. Kulunvalvonta- ja työajanseurantajärjestelmät. Suunnitteluohje. Sähkötieto ry. 2016. Espoo: Sähköinfo Oy. Viitattu 27.3.2023.

ST 710.02. Sähkö- ja tietoteknisten järjestelmien tietoturva. Sähkötieto ry. 2019. Espoo: Sähköinfo Oy. Viitattu 14.3.2023.

ST-käsikirja 11. Kulunvalvonta- ja murtoilmaisujärjestelmät. Arenius, K. (toim.), Syvälahti, P., Hovinen, R., Korkeavuori, T. & Kauppi, V. 2016. 5. uud. painos. Espoo: Sähköinfo Oy. Viitattu 1.2.2023.

Telia Company. 2020. Low Power Wide Area IoT. Verkkosivu. Viitattu 28.2.2023. https://business.teliacompany.com/internet-of-things/iot-connectivity/LPWA-IoT

Telia Company. 2021. 3G-verkko on siirtymässä historiaan. Verkkosivu. Viitattu 14.1.2023. https://www.telia.fi/3g

Timber, C. 2013. By cracking cellphone code, NSA has ability to decode private conversations. The Washington post 13.12.2013. Verkkosivu. Viitattu 14.3.2023. https://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html

Liikenne- ja viestintävirasto Traficom. 2019. Opas matkapuhelinverkkojen sisätilakuuluvuudesta. Viitattu 27.3.2023. https://www.traficom.fi/sites/default/files/media/publication/Opas-matkapuhelinverkkojen-sisatilakuuluvuudesta.pdf

Ympäristöministeriö. E1 Suomen rakentamismääräyskokoelma. Viitattu 8.3.2023.