Joel Helkala

Sotilaan monitorointi taistelukentällä hyödyntäen IoT-laitteita

Tietotekniikan kandidaatintutkielma

7. joulukuuta 2020

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Joel Helkala

Yhteystiedot: joel.helkala@gmail.com

Ohjaaja: Tytti Saksa

Työn nimi: Sotilaan monitorointi taistelukentällä hyödyntäen IoT-laitteita

Title in English: Soldier monitoring on the battlefield utilizing IoT devices

Työ: Kandidaatintutkielma

Opintosuunta: Tietotekniikka

Sivumäärä: 24+0

Tiivistelmä: Tässä tutkielmassa tutustutaan IoT-laitteisiin, sekä tapoihin ja teknologioihin joilla voitaisiin suorittaa sotilaan monitorointia taistelukentällä. Tutkielman tavoitteena on ollut perehtyä IoT-teknologiaan, IoT-monitorointiin ja sotilaiden monitorointiin taistelukentällä. Tutkielmassa käydään läpi optimaalisia kommunikaatioprotokollia sotilaan monitorointiin ja tämän hetkinen IoT:n tietoturvatilanne. IoT:n nopean kasvun on osoitettu aiheuttavan vakavia ongelmia tietoturvan alueella. Sotilaan monitorointiin on teknologiaa jo olemassa esimerkiksi terveydenhuollon alalla. Monitoroinnilla voidaan parantaa sotilaan turvallisuutta IoT-laitteiden keräämän datan avulla.

Avainsanat: IoT, monitorointi, sotilas, taistelukenttä

Abstract: In this thesis we will introduce IoT devices, methods and technologies that will enable us to perform monitoring of a soldier on the battlefield. The purpose of this thesis has been to get acquainted with IoT technology, IoT monitoring and soldier monitoring on the battlefield. In this thesis we will go over the optimal communication protocols and the current state of information security in the IoT. The rapid growth of IoT has been shown to increase the amount of security issues. The technology for soldier monitoring is already available, for example in the healthcare field. With monitoring we can enhance the safety of the soldiers with the help of the data collected by the IoT devices.

Keywords: IoT, monitoring, soldier, battlefield

Sisältö

1 Johdanto

Tämän tutkielman tarkoituksena on selvittää, miten IoT-laitteilla voidaan monitoroida sotilaita ja miten hyödyntää kerättyä tietoa sotilaan ja joukkueen eduksi. Tutkitaan minkälaisilla laitteilla tämä olisi mahdollista ja miten niitä voisi implementoida sotilaiden käyttöön. Internet of Things (IoT) tai esineiden internet tarkoittaa laitteiden sulautettua järjestelmää, jossa laitteet voivat kommunikoida keskenään ja prosessoida dataa ilman ihmisen vuorovaikutusta.

Data kerätään laitteisiin erilaisten sensoreiden, radiotaajuuksien kuten RFID ja Bluetooth ja paikannusjärjestelmän avulla. Laitteilla voidaan monitoroida sotilaan elintoimintoja ja varusteiden tilannetta. Tämä tieto voidaan näyttää sotilaalle itselleen, joukkueelle ja komentokeskukselle. Niillä voidaan myös tarkastella reaaliaikaisesti sotilaiden sijoittautumista taistelukentällä ja paikallistaa jopa mahdollisten uhkien sijaintia.

Sotilaiden monitoroinnista on vaikea löytää laadukkaita tutkimuksia, mikä vaikutti siihen, että kirjoittajan tarvitsi käyttää tutkielmassa enemmän pohdintaa. Luultavasti sotilaiden monitoroinnista on puolustusvoimilla tutkimusmateriaalia, mutta ei sitä ei ole paljoa julkisesti saatavilla. Tähän otetaan kantaa hieman tämän tutkielman lopussa. Näistä löydetyistä tutkimuksista kirjoittaja on ottanut ratkaisuja ja käytettyjä teknologioita. Niiden avulla on tehty johtopäätöksiä keskeisistä teknologioista. Tästä johtuu myös laaja lähteiden määrä.

Tutkielman rakenne on seuraava. Luvussa 2. käsitellään esineiden internet ja sen toimintaperiaatteet. Käydään myös hieman läpi LPWAN kommunikaatioteknologiaa ja tämän hetkistä IoT:n tietoturva tilannetta. Luvussa 3. pohditaan miksi on tärkeää monitoroida sotilasta ja annetaan esimerkkejä teknologioista, joilla monitorointia voitaisiin suorittaa. Luvussa 4. käsitellään sotilaan monitoroinnin hyödyt ja haitat, joita tulee IoT:n mukana. Viimeisenä lukuna on yhteenveto, johon tiivistetään tutkielman päätelmät ja ratkaisut monitoroinnin mahdollistamiseksi ja optimoimiseksi sotilaiden käyttöön.

2 Esineiden internet

Tässä luvussa tutustutetaan lukija IoT-laitteisiin ja niiden käyttötarkoituksiin. Tutkitaan oleellisia teknologioita ja IoT-infrastruktuurin rakenteita jotka mahdollistavat IoT:n. Tullaan käsittelemään myös, mitä tietoturvariskejä tämänhetkinen IoT-teknologia voi tuoda mukanaan. Esineiden internet (*Internet of Things*, IoT) termin toi ensimmäisenä esille Kevin Ashton vuonna 1999 (Ashton ym. 2009).

Esimerkkinä IoT-laitteesta voidaan antaa tunnetulla ilmalämpöpumppulla, jota voidaan monitoroida ja kontrolloida puhelimen avulla. Ilmalämpöpumppu kerää ympäristöstään tietoa sensoreilla kuten lämpötilaa ja jakaa tämän tiedon esimerkiksi Wi-Fi:n avulla internettiin. Tämä kerätty data esitetään käyttäjän puhelimessa applikaation avulla. Esineiden internetillä voidaan parantaa ihmisten elämää monilla eri aloilla, esimerkiksi julkisessa liikenteessä, terveydenhuollossa, teollisessa automaatiossa ja hätätapauksiin reagoimisessa (Al-Fuqaha ym. 2015). Viime vuosina IoT-laitteiden käyttö on yleistynyt myös julkisessa turvallisuudessa, älykkäässä kuljetuksessa, teollisuudessa, maantaloudessa ja myös armeijan käytössä (Cao, Zheng ja Shen 2016).

Esineiden internetin avulla fyysiset laitteet voivat nähdä, kuulla, ajatella ja suorittaa tehtäviä. Esineiden internet luo tavallisista laitteista älykkäitä hyödyntäen sulautettuja järjestelmiä, kommunikaatioteknologioita, sensoreita, internet-protokollia ja applikaatioita. (Al-Fuqaha ym. 2015) Termi IoT on määritelty monilla eri tavoilla, mutta näistä määritelmistä kaksi on kuitenkin saanut eniten suosiota tutkijoiden parissa. Ensimmäisenä määritelmänä IoT-laitteet voivat toimia ja kommunikoida keskenään ja kerätä dataa ympäristöstään. Ne myös reagoivat autonoomisesti fyysisen maailman tapahtumiin luoden palveluita ilman ihmisen interaktiota tai sen kanssa. Kiteytettynä se on fyysisen ja digitaalisen maailman interaktiota jossa digitaalinen maailma on vuorovaikutuksessa fyysiseen maailmaan sensoreiden ja muiden aktuaattoreiden avulla. (Vermesan ym. 2011). Toisessa määritelmässä IoT on paradigma jossa tietojenkäsittely ja tietoverkko kyvyt ovat sulautettuna johonkin kuviteltavissa olevaan objektiin. Näitä kykyjä käytetään kysyttäessä ja vaihtaessa objektin tilaa jos mahdollista. (Peña-López ym. 2005). IoT on yleisesti sanottuna uudenlainen maailma jossa melkein kaikki laitteet joita käytämme on kytkettynä verkkoon (Sethi ja Sarangi 2017).

Meulenin (2017) mukaan IoT käsitti vuonna 2017 noin 8.4 miljardia laitetta maailmanlaajuisesti, mikä tarkoitti 31 prosentin kasvua edellisestä vuodesta. Meulen (2017) ennusti laitteiden määrän kasvavan 20.4 miljardiin vuoteen 2020 mennessä. Burhan ym. (2018) puolestaan esittää artikkelissaan taulukon, jossa esitetään vuonna 2017 IoT-laitteita olevan 28.4 miljardia ja vuodelle 2020 ennustettu määrä on huimat 50.1 miljardia. Evans (2011) tukee Burhanin ennustamaa laitteiden määrää esittämällä taulukon, jossa osoitetaan 2015 vuonna IoT-laitteiden määrän olevan 25 miljardia ja vuonna 2020 vastaavat 50 miljardia. IoT-laitteiden todellista määrää on vaikea arvioida, jonka takia näiden arvioiden erot ovat suuret. Tämä voi osittain johtua myös pienistä eroista IoT-laitteiden määrittelyssä. Vaikka laitteiden todellista määrää on mahdoton tietää, näistä luvuista kuitenkin nähdään se, että IoT-laitteiden määrä kasvaa jatkuvasti suurta vauhtia. Näin nopean kasvun perässä on valitettavasti laitteiden tietoturvan vaikea pysyä mukana.

2.1 IoT:n toimintaperiaate

Esineiden internet -laitteet koostuvat sensoreista, prosessoinnista ja kommunikaatiosta. Laitteet kommunikoivat toistensa kanssa hyödyntäen erilaisia kommunikaatioprotokollia, jotka taas riippuvat laitteen käyttötarkoituksesta ja geologisesta sijainnista. Sotilaan monitorointiin voidaan käyttää useita erilaisia laitteita ja siksi on tärkeää, että IoT-järjestelmää luodessa hyödynnetään mahdollisimman kevyet kommunikaatioteknologiat niiden käyttötarkoituksiinsa. Tällä mahdollistetaan pienin mahdollinen energian kulutus ja luotettava tietoturva laitteiden muodostamassa esineiden internetissä.

Maksimovic (2017) kertoo esineiden internetin koostuvan miljardeista sensoreista. Sensorit keräävät tietoa ympäristöstään ja laitteet kommunikoivat muiden laitteiden kanssa, jotka ovat myös yhteydessä internetiin. IoT-teknologia vie eteenpäin monia elintärkeitä sektoreita, kuten terveydenhuoltoa, kuljetusta, teollisuutta, koulutusta, viljelyä, metsäteollisuutta ja vesiviljelyä. IoT-teknologia vie myös voimakkaasti maailmaa lähemmäs vihreää ja tehokasta tulevaisuutta. IoT:n on tunnistettu olevan yksi tulevaisuuden tärkeimmistä osa-alueista keräten huomiota koko ajan enemmän teollisuuden eri aloilta (Lee ja Lee 2015). Khanin ja Salahin (2018) mukaan tyypillisessä IoT-järjestelmässä on heterogeenisiä laitteita ja sulautettuja sensoreita jotka ovat yhteydessä internetin avulla. Laitteet ovat yksilöitävissä, vaativat

matalan määrän energiaa, niissä on pieni muisti ja rajoitetusti prosessointikykyä.

Esineiden internetin pitäisi pystyä yhdistämään miljardeja heterogeenisia objekteja internetin läpi. Tämän takia arkkitehtuurin on oltava joustavaa ja kerrostettua (Al-Fuqaha ym. 2015). Ei ole kuitenkaan yhtenäistä sopimusta siitä, mikä arkkitehtuuri on paras, vaan tutkijat ovat esittäneet erilaisia vaihtoehtoja. Sethin ja Sarangin (2017) mukaan kaikista yksinkertaisin on kolmen kerroksen arkkitehtuuri, joka koostuu havainnointikerroksesta, kuljetuskerroksesta ja sovelluskerroksesta. Viiden kerroksen arkkitehtuurissa tulee mukaan prosessointi- ja liiketoimintakerrokset. Tarkempia arkkitehtuureja löytyy eri tarpeisiin. Jos järjestelmä käyttää pilvi- tai sumupalveluita, käytettävän arkkitehtuurin tulee muuttua tätä tukevaksi.

Laitteet voivat kommunikoida useiden protokollien avulla, kuten Wi-Fin, Bluetoothin, 6LowPanin ja RFID:n (Al-Fuqaha ym. 2015). Tietyillä IoT-järjestelmillä on omat vaatimuksensa, kuten pitkä toimintamatka, alhainen datan määrä ja matala energiankulutus. Laajasti käytetyt lyhyen matkan radioteknologiat kuten ZigBee ja Bluetooth eivät sovellu pitkälle matkalle. Sellaiset ratkaisut joissa käytetään 2G-, 3G- tai 4G-yhteyksiä, voivat antaa laajemman kattavuuden, mutta vievät huomattavasti enemmän energiaa. Pitkän matkan kommunikaation tarpeet ovat tuoneet esille uuden langattoman kommunikaatioteknologian nimeltään LPWAN (*low power wide area network*). (Mekki ym. 2019)

IoT-kommunikaatiossa on useita hyödyllisiä langattomia teknologioita, joissa jokaisella on omia ominaisuuksia ja hyötyjä. Siksi on vaikea sanoa, mikä niistä on paras ja tämän vuoksi on käyttäjän itse mietittävä mikä vaihtoehdoista on hyödyllisin juuri omaan järjestelmään. (Al-Sarawi ym. 2017)

Sotilaiden monitoroinnin IoT-järjestelmiä voidaan toteuttaa usealla eri tavalla. Laitteet voivat kommunikoida suoraan internettiin itsenäisesti, jolloin laitteisiin tarvitaan LPWAN-tyylinen kommunikaatioteknologia, koska oletetaan sotilaan olevan sijainniltaan kaukana. Toinen vaihtoehto on käyttää yhdyskäytävää (*gateway*), jolla tarkoitetaan laitetta, jonka kautta IoT-laitteiden keräämä data viedään internetiin tai tarvittaessa muihin laitteisiin. Tällöin itse monitorointiin käytetyillä IoT-laitteilla voi olla yksinkertaisempi ja kevyempi kommunikaatioprotokolla käytössä, kuten ZigBee, joka kommunikoi yhdyskäytävän kanssa.

Gondalia ym. (2018) esittivät tutkielmassaan arkkitehtuurin jossa sotilailla on kevyempi

kommunikaatioprotokolla ja ryhmän johtajalla LoRa, joka kommunikoi operaatiokeskukseen. LoRa on yksi LPWAN-kommunikaatioteknologian suosituimmista vaihtoehdoista. Tällaisella toteutuksella voidaan tehdä yksinkertaisempia järjestelmiä ja kustannukseltaan halvempia IoT-laitteita ja kokonaisuuksia. Yhdyskäytävää voidaan käyttää myös datan kartoitukseen ja protokollien käännökseen erilaisten standardien välillä ja luoda yhteinen formaatti datalle (Johnsen, Zieliński ym. 2018b). Tätä yhdyskäytävä-arkkitehtuuria tukee artikkeli, jonka on luonut Pradhan, Fuchs ja Johnsen (2018). Kyseinen artikkeli esittää myös idean, jossa olisi eri tasoisia yhdyskäytäviä, jotka keräävät dataa eri tarkoituksiin (Pradhan, Fuchs ja Johnsen 2018). Näiden eri tasoisten yhdyskäytävien keräämä data prosessoidaan ja välitetään eri kohteisiin joilla on omat käyttötarkoituksensa.

2.2 LPWAN

Edellisessä alaluvussa mainittiin lyhyesti langaton kommunikaatioteknologia nimeltä LPWAN. LPWAN-teknologia syntyi ideasta, jossa laitteet voisivat keskustella keskenään ilman ihmisen interaktiota, nimeltä Machine-to-Machine (M2M) (Lukas Krupka, Lukas Vojtech ja Marek Neruda 2016; Ratasuk ym. 2016). M2M-teknologia on IoT:n yksi edeltäjistä. Näiden kahden eroavaisuutena on se, että M2M-teknologia keskittyy pelkästään laitteiden väliseen kommunikaatioon esimerkiksi RFID kommunikaatioteknologialla. M2M-teknologiaa käytetään todella paljon esimerkiksi teollisuudessa. Mobiililaajakaistaa on vaikea hyödyntää M2M-laitteisiin, koska ne ovat usein sijainniltaan kaukana, maan alla tai syvällä rakennuksissa. Näihin tilanteisiin kehitettiin kommunikaatioteknologioita, kuten Zigbee, Bluetooth ja RFID, mutta nämä kommunikaatioteknologiat eivät kuitenkaan sovellu pitkille matkoille. (Xiong ym. 2015)

M2M-teknologialle tarvittiinkin siis uusi pitkän matkan kommunikaatioteknologia ja tähän tarpeeseen kehitettiin LPWAN kommunikaatio. Naikin (2018) mukaan LPWAN-teknologia on ehdoton IoT:n tietoverkoston infrastruktuurin laajenemiseen ja kehittymiseen, koska LPWAN teknologia antaa mahdollisuuden kommunikaatiolle maaseudulla 10–40 kilometrin etäisyydelle ja kaupunkialueella 1–5 kilometrin etäisyydelle. Jethwa ym. (2020) tutkivat artikkelissaan sotilaille kohdistettua ympäristön ja elintoimintojen monitorointiin sopeutuvaa IoT-laitteistoa. Kommunikaatioteknologiaksi sotilaan ja tukikohdan välille valittiin LPWAN verk-

koarkkitehtuuri nimeltä LoRa, koska mobiililaajakaista yhteyksiä ei taistelukentällä välttämättä ole ja etäisyys tukikohtaan voi olla suuri.

Ison skaalan IoT-järjestelmiin kilpailee 3 johtavaa LPWAN teknologiaa, Sigfox, LoRa ja NB-IoT. Näissä kolmessa teknologiassa on monenlaisia teknisiä eroavaisuuksia, mutta näitä ei käydä tarkemmin tässä tutkielmassa lävitse. LPWAN teknologia on erittäin sopiva IoT-järjestelmiin joiden tarvitsee välittää pieni määrä dataa pitkän matkan yli (Mekki ym. 2019). L. Krupka, L. Vojtech ja M. Neruda (2016) suorittivat tutkimuksen mikä tukee näiden teknologioiden eroavaisuutta. Kyseisessä tutkimuksessa keskitytään kolmen LPWAN-teknologian eroavaisuuksiin ja mahdollisiin kommunikaatiotörmäyksiin käyttäen näitä teknologioita, joita havaittiin noin 876 MHz taajuudella.

Johnsen, Zieliński ym. (2018a) suorittivat tutkimuksen, jossa käytettiin IoT-laitteilla varustettuja simuloituja armeijajoukkoja Helsingissä. Helsinki oli tässä tutkimuksessa myös varustettu IoT-laitteilla, joka teki tästä kaupungista "älykkään". Älykkään kaupungin avulla sotilaat pystyivät kommunikoimaan kaupungissa sijaitsevien sensoreiden ja kameroiden kanssa. Tutkimuksessa pyrittiin käyttämään parhaita IoT tapoja ja siksi oli myös kommunikaatioteknologiaksi valittu LoRa, joka on yksi kilpailevista LPWAN teknologioista. Operaation tarkoituksena oli tutkia IoT:n käyttöä sotilasoperaatioissa älykkäässä kaupungissa. Tässä luvussa käsiteltyjen artikkeleiden perusteella voidaan päätellä, että LPWAN-teknologia on tähän tehtävään paras vaihtoehto. Sotilaiden geologinen sijainti voi olla mahdollisesti sellaisella alueella jossa ei ole mobiililaajakaistalle mahdollisuutta tai tarvitaan jostain muusta syystä pitkän matkan kommunikaatioteknologia. LPWAN-teknologia sopii todella hyvin myös kaupungissa sijaitseviin operaatioihin kuten tässä luvussa tuotiin esille. Älykkäässä kaupungissa sotilaat voivat saada IoT-laitteista vielä suuremman hyödyn, koska voivat olla kommunikaatiossa kaupungin sensoreiden ja kameroiden kanssa. Data, jota sotilaista ja kaupungeista välitetään on arkaluontoista ja siksi meidän on tutkittava hieman IoT-teknologian tämän hetkistä tietoturvatilannetta joka on yleisesti ollut iso huolenaihe.

2.3 Tietoturva

IoT-laitteiden räjähdysmainen yleistyminen tuo mukanaan tuntemattomia riskejä joita rikolliset voivat hyödyntää yllättävissäkin paikoissa (O'Neill ym. 2016). Arias ym. (2015) kertovat artikkelissaan sydämen tahdistimen haavoittuvuudesta, jota hyökkääjä pystyi käyttämään hyväkseen ja aiheuttamaan vahinkoa potilaalle. IoT-teknologian kyberturvallisuus on tämän takia iso huolenaihe, koska laitteet eivät saa aiheuttaa minkäänlaista vahinkoa käyttäjälleen. IoT-infrastruktuurit ja palvelut tuovat mukanaan valtavia turvallisuus haasteita, sillä niiden mukana tulee myös merkittävä kasvu hyökkäysalustoissa, kompleksisuudessa, heterogeenisyydessä ja resurssien määrässä (Pacheco ja Hariri 2016; Zhang ym. 2014). Jos IoT vallankumousta katsotaan tietoturvallisuuden perspektiivistä, se on täysi katastrofi. De Donnon (2017) mukaan tietoturvan heikkous ainakin kaupallisissa IoT-laitteissa johtaa juurensa yhtiöiden yritykseen pysyä IoT:n markkinoiden aallossa mukana tuomalla tuotteensa nopeasti markkinoille. Tätä tietoturvaongelman lähdettä tukee Zhangin ym. (2014) artikkeli, jossa tutkitaan IoT:n tietoturvahaasteita. Kyseisen tutkimuksen mukaan IoT:n tietoturvaongelmat johtuvat huonosta järjestelmän suunnittelusta, mutta myös IoT:n luomasta kompleksisuudesta. IoT:ssa käytetään useita erilaisia kommunikaatioprotokollia ja todella monia sensoreita ja laitteita, jotka luovat järjestelmästä monimutkaisen ja haavoittuvan.

Tietoturva koostuu kolmesta osa-alueesta ("Kyberturvallisuuskeskus" 2020; Lin ja Bergmann 2016).

- *Luottamuksellisuudesta*, eli keskitytään pitämään data yksityisenä, jotta vain valtuutetuilla laitteilla ja ihmisillä on siihen pääsy
- *Eheydestä*, eli verifioidaan, että dataa ei ole muutettu ja datan lähde on varmasti luotettava
- *Käytettävyydestä*, eli päästetään vain valtuutetut käyttäjät käsiksi dataan, kommunikaatio infrastruktuuriin ja tietojenkäsittely resursseihin

Khanin ja Salahin (2018) mukaan IoT:n data kulkee monien erilaisten tietoverkkojen ja laitteiden yli, siksi kunnollinen salaus mekanismi on oltava käytössä. Laajojen palveluiden, laitteiden ja tietoverkkojen integraatioiden takia data on altis yksityisyysloukkauksille. Hyökkääjät voivat vaikuttaa datan eheyteen muokkaamalla välitettävää dataa ilkeänmielisiin tar-

koituksiin. Jotta laitteiden välinen keskustelu on turvattua, tarvitaan laitteiden välille luoda lähteiden todentaminen. Hyökkäys voi kohdistua myös tietoliikenteen kerrokseen esimerkiksi palvelunesto (*Denial-of-service*, DoS) hyökkäyksellä, joka vaikuttaa datan liikkuvuuteen laitteiden välillä. Kuten aikaisemmin tuli ilmi, halutaan IoT-laitteiden virrankulutuksen olevan matala. IoT-laitteet jotka ovat hyökkäyksen kohteena vievät huomattavasti enemmän virtaa, josta voi seurata esimerkiksi laitteen sammuminen (Khan ja Salah 2018). Tietoturvan ollessa IoT-järjestelmien yksi isoimmista huolenaiheista, on sen suunnittelu ja vahvuus oltava yksi järjestelmän suunnittelun pääkohdista.

Luvussa 2.1 tuotiin esille yhdyskäytävä. Yhdyskäytävällä voidaan myös parantaa laitteiden välisen datan salausta ja yleistä tietoturvan vahvuutta huomattavasti (Johnsen, Zieliński ym. 2018b). Jotta tuntemattomat laitteet eivät pääse kommunikoimaan muiden laitteiden kanssa, voidaan hyödyntää julkisen avaimen infrastruktuurin (*Public Key Infrastructure*, PKI) sertifikaattia (Tuecke ym. 2004). Tähän infrastruktuuriin ei mennä syvällisesti sisälle, mutta lyhyesti tarkoittaa sitä, että on käytössä sertifikaatti auktoriteetti (*Certificate Authority*, CA) joka varmistaa, että laite on luotettava. Tämän jälkeen osapuolet jakavat avaimet, joiden avulla heidän välisensä datanvaihto voidaan salata. Avaimen generoimiseen on monia työkaluja, kuten Diffie-Hellman avaimen vaihto (Diffie ja Hellman 1976; Rescorla ym. 1999), jonka avulla generoidaan erittäin suojattu avain jota on todella vaikea murtaa. Erilaisille kommunikaatioprotokollille on erilaisia tietoturvamenetelmiä ja niitä protokollia käytettäessä on tiedettävä miten niiden kommunikaatio salataan. Edellä mainitut salausmenetelmät ovat yleisimpiä lähiverkoissa (*local area network, LAN*).

3 Sotilaan monitoroinnin tarpeet ja tavat

Sensoreilla voidaan kerätä dataa melkein mistä vain. Tässä luvussa tullaan keskittymään alueisiin, jotka voisivat parantaa sotilaan toimintakykyä ja turvallisuutta taistelukentällä. Pohditaan hieman myös miksi olisi tärkeää monitoroida sotilaita ja miten elintoimintojen monitorointi on suoritettu esimerkiksi terveydenhuollossa. Tutkimme terveydenhuollon käyttämiä IoT-toteutuksia, koska terveydenhuollon käyttämä monitorointi on tavoitteiltaan lähellä sotilaan monitoroinnin tavoitteita. Terveydeynhuolto oli myös yksi ensimmäisistä toimialoista, joka otti käyttöönsä IoT-teknologian (Lampropoulos, Siakas ja Anastasiadis 2018). Terveydenhuolto on yksi maailman nopeiten kasvimimmista toimialoista, se on myös maailman tarvituin ja käytetyin palvelu (Titi, Elhadj ja Chaari 2019). Näistä kahdesta väittämästä voidaan päätellä, että terveydenhuollon toimiala on myös yksi maailman parhaista ja isoimmista IoT-teknologian kehittäjistä. Sotilaiden monitoroinnin teknologian edistyksillä voitaisiin myös edistää terveydenhuollon monitoroinnin teknologiaa ja tämä nostaisi nopeasti IoT-monitoroinnin kehitystä, kun molempien alojen teknologinen kehitys tukee toisiaan.

Tämän tutkielman kirjoittajan mielestä sotilaan monitoroinnissa painottuu pieni datan määrä ja pitkän matkan kantavuus. Sotilaita voi olla monia, joista jokaisesta kerätään dataa. Jotta data saataisiin nopeasti analysoitavaksi ja esitettäväksi niin sotilaille kuin operaatiokeskukselleki, sen olisi hyvä olla valmiiksi prosessoitu mahdollisimman yksinkertaiseen muotoon ennen lähettämistä. Tähän voitaisiin käyttää esimerkiksi JSON-formaattia, jota käytettiin esimerkiksi Johnsenin (Johnsen, Zieliński ym. 2018a) artikkelin operaatiossa. Data prosessoitaisiin jo valmiiksi datan keräämässä laitteessa tai viimeistään ennen datan lähettämistä ja lähetettäisiin kevyessä formaatissa jota ihminenkin voi lukea.

Esineiden internetin-laitteet vaihtelevat yksinkertaisista puettavista lisävarusteista isoihin koneisiin ja esimerkiksi sotilaiden käyttämiin ajoneuvoihin, mutta sotilaan monitoroinnissa keskitytään elintoimintojen tarkkailuun, paikannukseen ja varusteiden tilaan. Suurin osa näistä monitoroinneista voidaan suorittaa puettavilla laitteilla, joita käydään tarkemmin läpi tämän luvun ensimmäisessä aliluvussa. IoT-laitteiden mahdollistama terveyden monitorointi on yleistymässä myös kuluttajien keskuudessa. Lenovon älykkäissä kengissä on esimerkiksi siru, joka laskee ja analysoi kuntoiluun liittyvää dataa (Khan ja Salah 2018), jota kuluttaja

voi tarkkailla puhelimessaan sijaitsevan applikaation avulla. Pelkästään näin yksinkertaisella toiminnolla voidaan normaalin kansalaisen elintasoa nostaa ja kehittää heidän kykyään oman terveyden huoltamisessa.

3.1 Puettavat laitteet

Sotilaalla informaatio omasta tilastaan ja taistelukentästä olisi kriittistä, jotta operaatiot voidaan suorittaa turvallisesti ja tehokkaasti. Tämä informaatio täytyisi kuitenkin olla sotilaalle helposti ja nopeasti saatavilla ja siten esitetty, että sotilas saisi nopealla toiminnalla kaiken tarvittavan tiedon. Puettavilla laitteilla voi käyttäjä tehdä monenlaisia toimintoja vaivattomasti, kuten katsoa puhelimeen tulleen viestin ranteessa olevasta laitteestaan tai esimerkiksi älykkäistä silmälaseistaan. Ensimmäinen älykäs vaate kehitettiin 1990-luvun lopulla Georgian teknillisen yliopiston toimesta (Fernández-Caramés ja Fraga-Lamas 2018; Gopalsamy ym. 1999). Tämä puettava emolevy oli kehitetty paidaksi, joka mittaisi käyttäjän elintoimintoja huomaamattomasti, terveydenhuollon ja taistelukentän applikaatioihin.

Seneviratnen (Seneviratne ym. 2017) mukaan puettavat laitteet voidaan jakaa kolmeen kategoriaan: varusteisiin, sähköisiin tekstiileihin ja sähköisiin laastareihin. Varuste kategoriaan kuuluvat esimerkiksi älykkäät kellot tai rannenauhat, jotka keräävät henkilön terveystietoja. Tekstiili kategoriaan kuuluvat laitteet joita käytetään myös vaatteina, kuten paidat, housut ja alusvaatteet. Käsissä ja jaloissa pidettävät asusteet kuuluvat myös tähän kategoriaan. Viimeisenä kategoriana on laastarit, joihin kuuluvat sensori laastarit ja e-tatuoinnit. Puettavat laitteet ovat arkkitehtuuriltaan samanlaisia kuin IoT-laitteet, mutta niillä on yleensä vähemmän laskentatehoa ja rajoitettu kommunikaatiorajapinta. Nämä laitteet kuitenkin keräävät yhtä paljon, ellei enemmän dataa verrattuna normaaleihin IoT-laitteisiin. Tämän takia on tärkeää saada puettavien laitteiden virrankäyttö mahdollisimman alhaiseksi sotilaan monitoroinnissa. Laitteissa voi olla myös kiihtyvyyssensoreita, gyroskooppeja ja sähkömagneettikenttä sensoreita (Majumder, Mondal ja Deen 2017). Puettavat laitteet voivat kuitenkin johtaa turvallisuusongelmiin käyttäjille, kuten luvussa 2.3 esitetty tapaus.

Puettaville laitteille on yleistä se, että niiden komponentit ovat kytketty yhteisen verkkotopologian kautta jolle on ominaista tarjota todella lyhyt kantama. Tätä verkkoa kutsutaan

nimellä Body Area Network tai lyhenteenä BAN. Tämä nimike on kuitenkin yleistys kyseiselle verkolle, koska puettaville laitteille käytetään tarkemmin nimikettä WBAN (*Wearable BAN*). IBAN (*Implantable BAN*) nimikettä käytetään verkosta, jonka laitteet keräävät tietoa ihmisen kehon sisäpuolelta. WBAN:n on oltava energia tehokas, koska yleisesti puettavat laitteet saavat virtansa paristoista. (Fernández-Caramés ja Fraga-Lamas 2018)

3.2 Elintoiminnot

Sotilaan elintoimintojen monitorointi olisi erittäin tärkeää, koska sillä voidaan antaa sotilaalle tietoa omasta tilastaan, josta sotilas voi tehdä johdettuja ratkaisuja. Sotilaan ollessa haastavassa tilanteessa, laite pystyisi myös nopeasti hälyttämään lähellä olevan lääkintämiehen sotilaan luokse tai suorittamaan muita asetettuja hätätilanteen toimintoja. Laitteiden keräämän datan analyysi sijaitsee luultavasti operaatio- tai komentokeskuksessa, jossa on terveydenhuollon ammattilaisia tarkkailemassa sotilaiden elintoimintoja ja tietyssä tilanteessa ammattilainen pystyisi antamaan sotilaalle tarkasti neuvoja. Tätä pohdintaa tukee artikkeli, jonka on luonut Titi, Elhadj ja Chaari (2019). Kyseisessä artikkelissa kerrotaan, että potilaan monitoroinnissa käytetyt laitteet kommunikoivat internetiin, josta terveydenhuollon ammattilaiset pääsevät tarkastelemaan kerättyä dataa ja tekemään tästä harkittuja päätöksiä.

Laitteiden sensorit pystyvät mittaamaan fysioloogisia attribuutteja, kuten elektrokardiokrammia (ECG), elektromyografiaa (EMG), sykettä (HR), kehon lämpötilaa, elektrodermaalista aktiviteettia (EDA), valtimoiden happisaturaatiota (Sp02), verenpainetta (BP) ja hengitysnopeutta (RR) (Majumder, Mondal ja Deen 2017). Izumi ym. (2014) suunnittelivat tutkimuksessaan matalavirtaisen ihoon kiinnitettävän pietsosähköisen painesensorin, jolla mitataan käyttäjän sydämen sykettä. Laite pystyy mittaamaan sykkeen tarkasti meluisassakin ympäristössä, hyödyntäen STAC algoritmia. Taistelukenttä voi olla meluisa ympäristö ja siksi on tärkeää ottaa tämä huomioon. Sotilaan monitorointi on tärkeää, mutta kirjoittajan mielestä kerätyn datan tarkkuus on tärkeämpää. Tämä painottuu huomattavasti, jos datan tarkkuus voi heitellä paljon meluisan ympäristön takia.

IoT-laitteiden matalat virrankulutus vaatimukset voivat esittää myös haasteita laadukkaiden datojen keräämiseen varsinkin meluisissa ympäristöissä (Hassanalieragh ym. 2015). Tämän

takia on tärkeää keskittää virrankulutus niihin komponentteihin, joissa se on tärkeintä. Tätä voidaan edistää käyttämällä mahdollisimman kevyitä teknologioita monitoroinnin mahdollistavissa laitteissa. Virran generoimiseen voitaisiin käyttää myös muitakin keinoja kuin paristot ja akut. Torfsin (Torfs ym. 2006) suorittamassa tutkimuksessa he kehittivät laitteen, jolla voidaan generoida virtaa käyttäjän kehonlämmöstä. Laite mittasi käyttäjän pulssia ja generoi käyttäjän kehonlämpötilasta itselleen virtaa ja laitteella oli täysi energia autonomisuus.

3.3 Paikannus

Paikannuksen todentamiseen hyödynnettään satelliittejä, mikä on tämän hetkisen paikannuksen ja navigaation kulmakivi. Satelliittisignaalien perusteella voi sijainnin määrittää noin muutaman metrin tarkkuudella missä vain maapallolla. Avustepalveluita käyttämällä tarkkuus voidaan parantaa jopa senttimetreihin. GPS (*global positioning system*) on vain tunnetuin satelliittipaikannus järjestelmä. Kenen tahansa käytettävissä on myös paikannusjärjestelmät kuten venäläinen GLONASS, eurooppalainen Galileo ja kiinalainen BeiDou. Tämän takia nykyään viitataan paikannusjärjestelmään termillä GNSS (*global navigation satellite system*). (“Maanmittauslaitos” 2020)

Tutkimuksien yhtenäisenä vaatimuksena on sotilaan monitoroinnissa käyttää paikannusjärjestelmää. Paikannusjärjestelmä on sotilaan monitoroinnin kulmakiviä, jolla operaatiokeskus voi tarkkailla sotilaiden sijaintia ja helposti tarkkailla tietyn sektorin sotilaiden tilaa. Erityisoperaatioissa sotilaat voivat joutua poikkeamaan suunnitellulta polultaan. Paikannusjärjestelmän avulla kuitenkin voidaan lähettää sotilaan leveys- ja pituusaste operaatiokeskukseen, josta voidaan antaa ohjeita operaation jatkamiseen (Gondalia ym. 2018). Sotilaiden laitteissa voi olla paikannuksen lisäksi myös kiihtyvyyssensorit, kuten luvussa 3.1 mainittiin. Paikannuksen ja kiihtyvyyssensoreiden yhteystyöllä voidaan räjähdyksen sattuessa laskea räjähdyksen voima ja räjähdyspaikka (Lim ym. 2010). Näihin tietoihin voidaan implementoida matemaattisia kaavoja ja luoda visualisointeja räjähdyksen vaikutusalasta ja sotilaiden sijainnista räjähdysalueella.

4 Sotilaan monitoroinnin hyödyt ja haitat

Tässä luvussa pohditaan mitä hyötyjä ja haittoja IoT-teknologia toisi mukanaan sotilaan monitorointiin. Sotilaan monitoroinnissa on erittäin tärkeää, että monitoroinnilla kerätty data on aitoa, sitä voi tarkastella vain ne joilla on siihen valtuudet ja laitteet eivät voi aiheuttaa sotilaalle minkäänlaista vahinkoa. Laitteet joita käytettäisiin sotilaiden monitorointiin, on testatava mahdollisten tietoturva aukkojen varalta. Laitteissa ei saisi olla vanhentuneita kommunikaatioteknologioita ja data jota välitetään laitteiden ja tukikohdan välillä, on salattava. Armeija ei voisi siis turvautua kaupallisiin monitorointi laitteisiin, vaan laitteiden tietoturvan testaus ja muokkaus olisi suoritettava sisäisesti. Rikolliset pystyvät itse rakentamaan IoT-laitteita ja testaamaan tietoturva haavoittuvuuksia. Siksi on myös tärkeää, että sotilaiden monitorointiin käytettävien laitteiden tarkkoja tietoja ei ole julkisuudessa. Tämän perusteella voidaan ymmärtää miksi sotilaiden monitoroinnista ei löydy julkisesti paljolti tutkimuksia.

4.1 Monitoroinnin hyödyt

Sotilaan monitoroinnin hyödyistä painavin on selvästi sotilaan turvallisuus. Ihmishengille ei voi asettaa arvoa tai hintaa ja tämän takia on valtion ja armeijan tehtävä kaikkensa, jotta sotilaiden turvallisuus taataan. Monitoroinnilla voitaisiin suorittaa paljon turvallisempia ja suunnitellumpia operaatioita sen mukana tulevien ominaisuuksien ansiosta. Teknologialla saataisiin tarkkaa tietoa taistelukentän tilanteista ja sitä voitaisiin analysoida myös jälkikäteen. Hyvin suunnitellulla operaatiolla voitaisiin taata sotilaiden maksimaalinen turvallisuus ja kotiinpaluu. Sotilaiden joutuessa haastavaan tilanteeseen, voitaisiin operaatiokeskuksesta tehdä nopeita strategisia ratkaisuja taistelun edistämiseksi.

Kuten luvussa 3.2 tuli ilmi, sotilaan elintoimintojen monitorointiin on tarvittava teknologia jo valmiina. Elintoimintoja mittaavan teknologian implementointi sotilaan monitorointiin edistäisi huomattavasti sotilaan turvallisuutta, mahdollisten hätätilanteiden reaktionopeutta ja suoritettavan ensiavun hyödyn maksimoimista. Laitteet voisivat antaa sotilaalle ensiapu ohjeita haavoittuneen toverin hoitamiseen tai ne voisivat antaa sotilaalle ohjeita oman tilan kohentamiseen tarvittavalla ensiavulla tai lääkkeillä.

Puettavilla laitteilla voidaan helposti havaita räjähdyksiä, niiden voimakkuuttaa ja räjähdyksen sijaintia. Näistä tilanteista voidaan luoda visualisointeja operaatiokeskuksessa, jossa saadaan erittäin hyvää kokonaiskuvaa taistelukentän tilanteesta. Voitaisiin räjähdyksien sattuessa tarkasti tehdä strategisia päätöksiä siitä, minkälainen määrä on sotilaita mahdollisesti loukkaantunut ja minkälaista apua taistelukentän räjähdys sektorissa tarvittaisiin. Räjähdysten lisäksi voitaisiin laitteisiin liittää mukaan myrkyllisten kaasujen tunnistimia, jotka havaitessaan myrkyllisen kaasun, ilmoittaisivat siitä sotilaille ja operaatiokeskukselle. Puettavien laitteiden avulla saataisiin monitorointia mahdollistavat laitteet asetettua sotilaaseen siten, että se ei tule aiheuttamaan sotilaan liikkuvuuteen esteitä.

Useammalla yhdyskäytävällä voitaisiin luoda laadukkaampaa kuvaa taistelukentästä ja hyödyntää esimerkiksi tekoälyjen avulla saatua dataa strategioiden luomiseen. Useamman yhdyskäytävän avulla voidaan keventää kommunikaatiokuormaa ja luoda entistä tarkempaa kuvaa taistelukentästä hyvin prosessoidun ja analysoidun datan avulla.

IoT:n rajoja on vaikea tietää, mutta sen mahdollisuudet ovat kuitenkin suuret. Sotilaiden monitoroinnissa on paljon haasteita, mutta pelkästään ihmishenkien pelastaminen ja haavoittuvuuksien vähentäminen luo motivaation monitoroinnin suorittamiselle. Ottamalla vastaan monitoroinnin tuomat haasteet, voimme kehittyä turvallisemmaksi ja rauhallisemmaksi maailmaksi.

4.2 Monitoroinnin haitat

IoT-monitorointi on virrallisesti rajattua, eikä sotilaasta voitaisi monitoroida mitä vain attribuuttia tämän takia. Kuten luvussa 3.2 mainittiin, laitteista on mahdollista tehdä virrantuottoltaan ja kulutukseltaan autonomisia, mutta se teknologia tällä hetkellä koskee vain yksinkertaisia laitteita, rajatuilla toiminnoilla. Liiallista virrankulutusta voidaan ehkäistä mahdollisimman kevyillä kommunikaatioteknologioilla ja hyvällä arkkitehtuurilla. Virrankulutukseen voi vaikuttaa myös mahdollinen kyberhyökkäys laitetta kohtaan.

Luvussa 2.3 kävimme lyhyesti IoT:n tietoturvaa läpi. Luvusta voitaisiin päätellä, että IoT:n tietoturvatilanne ei ole tällä hetkellä hyvä. Hyökkäyksellä pahamielinen tekijä voisi saada arkaluontoista tietoa ja vaarantaa sotilaiden turvallisuutta. Tietoturvan kehittämisen olisi siksi

oltava ensisijaisia tavoitteita sotilaan monitoroinnin suunnittelussa ja toteutuksessa. Tietoturvaongelma kuitenkin tietyiltä osilta on kaupallisen kilpailun syytä. Tähän voitaisiin vaikuttaa sillä, että sotilaan monitorointiin käytettävät laitteet kehitettäisiin ja ylläpidettäisiin armeijan toimesta. Pelkästään hyvällä suunnittelulla ja toteutuksella voidaan IoT-laitteista saada tietoturvaltaan paljon vahvempia.

Laitteet eivät saa aiheuttaa sotilaille minkäänlaista vahinkoa, kuten luvussa 2.3 esitetty sydämentahdistin. Monitoroinnissa käytettävien laitteiden tietoturva on oltava koko ajan ajantasalla ja tämä vaatii sitä, että asiantuntijat ovat perillä niissä käytetyistä teknologioista, haavoittuvuuksista ja myös laitteita olisi testattava jatkuvasti. IoT:n luoman laajan alustan takia hyökkääjät voivat suorittaa hyökkäyksiä yllättävissäkin paikoissa. Siksi on tärkeää, että sotilaiden monitorointiin käytettävät laitteet ja protokollat eivät ole julkisesti tiedossa. Julkisesti saatavilla olevat tutkimukset sotilaan monitoroinnista voisi nopeuttaa teknologian kehitystä, mutta altistaa sotilaat ja laitteet suuremmalle kyberhyökkäys riskille.

Haittoja sotilaan monitoroinnissa ei ole paljoa, mutta tämän hetkiset haitat ovat erittäin vakavia. Suurin osa haitoista on minimoitavissa kunnollisella suunnittelulla ja toteutuksella.

5 Yhteenveto

Tässä kirjallisuuskatsauksessa tutkittiin sotilaan monitorointia taistelukentällä hyödyntäen IoT-laitteita. Ensimmäisessä sisältöluvussa käsiteltiin mitä esineiden internet tarkoittaa, sen toimintaperiaatteet ja käytiin lyhyesti läpi LPWAN kommunikaatioteknologiaa ja tämän hetkistä tietoturva tilannetta. Toisessa sisältöluvussa käsiteltiin monitoroinnin tarpeita ja esimerkkejä erilaisista teknologioista, joita voidaan käyttää sotilaan monitorointiin. Kolmannessa sisältöluvussa käytiin läpi kirjoittajan pohdintaa sotilaan monitoroinnin hyödyistä ja haitoista löydetyn kirjallisuuden perusteella.

Tutkimuskysymyksinä toimi: "*Miten sotilaita voidaan monitoroida taistelukentällä hyödyntäen IoT-laitteita*" ja "*Mitä hyötyjä ja haittoja sotilaan monitorointi toisi mukanaan*". Ensimmäiseen tutkimuskysymykseen löytyi kirjallisuuskatsauksella vastauksia ja valmiina olevia teknologioita varsinkin terveydenhuollon alalta. Monitoroinnin hyötyihin ja haittoihin kirjoittaja käytti omia johtopäätöksiään ja mielipiteitään kirjallisuuskatsauksen avulla. Hyötyihin kuului sotilaan yleinen turvallisuuden parantaminen ja haittoihin kuului esimerkiksi IoT-teknologian nykyiset tietoturva haasteet ja sen mukana tulevat ongelmat.

Tätä kirjallisuuskatsautta tehdessä kirjoittaja on lukenut todella monia tutkimuksia ja artikkeleita sotilaan tai terveydenhuollon monitoroinnista. Harvoissa artikkeleissa oli edes kuvauksia yleisesti siitä, mitä arkkitehtuuria kyseiseen teknologiaan käytetään tai olisi hyvä käyttää. Kuitenkin kaikista huolestuttavinta oli, että kirjallisuuskatsausta tehdessä vastaan tuli vain muutama tutkimus jonka infrastruktuurikuvassa oli kyberturvallisuus otettu mukaan. Tämä voi johtua julkisten sotilaan monitorointiin kohdistuneiden tutkimuksien pienestä määrästä. Tutkimukset joita kirjoittaja löysi olivat enemmänkin kokonaiskuvausta monitoroinnista eikä menty yksityiskohtaisuuksiin.

Lähteet

Arias, Orlando, Jacob Wurm, Khoa Hoang ja Yier Jin. 2015. “Privacy and security in internet of things and wearable devices”. *IEEE Transactions on Multi-Scale Computing Systems* 1 (2): 99–109.

Ashton, Kevin, ym. 2009. “That ‘internet of things’ thing”. *RFID journal* 22 (7): 97–114.

Burhan, Muhammad, Rana Asif Rehman, Byung-Seo Kim ja Bilal Khan. 2018. “IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey”. *Sensors* 18 (elokuu). doi:10.3390/s18092796.

Cao, Liang, Guo Zheng ja Yong Shen. 2016. “Research on design of military ammunition container monitoring system based on IoT”. Teoksessa *2016 Prognostics and System Health Management Conference (PHM-Chengdu),* 1–4. IEEE.

De Donno, Michele, Nicola Dragoni, Alberto Giaretta ja Angelo Spognardi. 2017. “Analysis of DDoS-capable IoT malwares”. Teoksessa *2017 Federated Conference on Computer Science and Information Systems (FedCSIS),* 807–816. IEEE.

Diffie, Whitfield, ja Martin Hellman. 1976. “New directions in cryptography”. *IEEE transactions on Information Theory* 22 (6): 644–654.

Evans, D. 2011. “How the Next Evolution of the Internet Is Changing Everything”. https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

Fernández-Caramés, Tiago M, ja Paula Fraga-Lamas. 2018. “Towards the Internet of smart clothing: A review on IoT wearables and garments for creating intelligent connected e-textiles”. *Electronics* 7 (12): 405.

Al-Fuqaha, Ala, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari ja Moussa Ayyash. 2015. “Internet of things: A survey on enabling technologies, protocols, and applications”. *IEEE communications surveys & tutorials* 17 (4): 2347–2376.

Gondalia, Aashay, Dhruv Dixit, Shubham Parashar, Vijayanand Raghava, Animesh Sengupta ja Vergin Raja Sarobin. 2018. “IoT-based healthcare monitoring system for war soldiers using machine learning”. *Procedia computer science* 133:1005–1013.

Gopalsamy, Chandramohan, Sungmee Park, Rangaswamy Rajamanickam ja Sundaresan Jayaraman. 1999. “The Wearable Motherboard^{TM}: The first generation of adaptive and responsive textile structures (ARTS) for medical applications”. *Virtual Reality* 4 (3): 152–168.

Hassanalieragh, M., A. Page, T. Soyata, G. Sharma, M. Aktas, G. Mateos, B. Kantarci ja S. Andreescu. 2015. “Health Monitoring and Management Using Internet-of-Things (IoT) Sensing with Cloud-Based Processing: Opportunities and Challenges”. Teoksessa *2015 IEEE International Conference on Services Computing,* 285–292. doi:10.1109/SCC.2015.47.

Izumi, Shintaro, Ken Yamashita, Masanao Nakano, Hiroshi Kawaguchi, Hiromitsu Kimura, Kyoji Marumoto, Takaaki Fuchikami, Yoshikazu Fujimori, Hiroshi Nakajima, Toshikazu Shiga ym. 2014. “A Wearable Healthcare System with a 13.7 μ A Noise Tolerant ECG Processor”. *IEEE Transactions on Biomedical Circuits and Systems* 9 (5): 733–742.

Jethwa, B., M. Panchasara, A. Zanzarukiya ja R. Parekh. 2020. “Realtime Wireless Embedded Electronics for Soldier Security”. Teoksessa *2020 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT),* 1–6. doi:10.1109/CONECCT50063.2020.9198537.

Johnsen, F. T., Z. Zieliński, K. Wrona, N. Suri, C. Fuchs, M. Pradhan, J. Furtak ym. 2018a. “Application of IoT in military operations in a smart city”. Teoksessa *2018 International Conference on Military Communications and Information Systems (ICMCIS),* 1–8. doi:10.1109/ICMCIS.2018.8398690.

Johnsen, Frank T, Zbigniew Zieliński, Konrad Wrona, Niranjan Suri, Christoph Fuchs, Manas Pradhan, Janusz Furtak, Bogdan Vasilache, Vincenzo Pellegrini, Michał Dyk ym. 2018b. “Application of IoT in military operations in a smart city”. Teoksessa *2018 International Conference on Military Communications and Information Systems (ICMCIS),* 1–8. IEEE.

Khan, Minhaj Ahmad, ja Khaled Salah. 2018. “IoT security: Review, blockchain solutions, and open challenges”. *Future Generation Computer Systems* 82:395–411.

Krupka, L., L. Vojtech ja M. Neruda. 2016. “The issue of LPWAN technology coexistence in IoT environment”. Teoksessa *2016 17th International Conference on Mechatronics - Mechatronika (ME),* 1–8.

Krupka, Lukas, Lukas Vojtech ja Marek Neruda. 2016. “The issue of LPWAN technology coexistence in IoT environment”. Teoksessa *2016 17th International Conference on Mechatronics-Mechatronika (ME),* 1–8. IEEE.

“Kyberturvallisuuskeskus”. 2020. Viitattu 27. lokakuuta 2020. `https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva`.

Lampropoulos, Georgios, Kerstin Siakas ja Theofylaktos Anastasiadis. 2018. “Internet of Things (IoT) in Industry: Contemporary Application Domains, Innovative Technologies and Intelligent Manufacturing”. *people* 6:7.

Lee, In, ja Kyoochun Lee. 2015. “The Internet of Things (IoT): Applications, investments, and challenges for enterprises”. *Business Horizons* 58 (4): 431–440.

Lim, H. B., D. Ma, B. Wang, Z. Kalbarczyk, R. K. Iyer ja K. L. Watkin. 2010. “A Soldier Health Monitoring System for Military Applications”. Teoksessa *2010 International Conference on Body Sensor Networks,* 246–249. doi:`10.1109/BSN.2010.58`.

Lin, Huichen, ja Neil W Bergmann. 2016. “IoT privacy and security challenges for smart home environments”. *Information* 7 (3): 44.

“Maanmittauslaitos”. 2020. `https://www.maanmittauslaitos.fi/tutkimus/teematietoa/satelliittipaikannus`.

Majumder, Sumit, Tapas Mondal ja M Jamal Deen. 2017. “Wearable sensors for remote health monitoring”. *Sensors* 17 (1): 130.

Maksimovic, Mirjana. 2017. “The role of green internet of things (G-IoT) and big data in making cities smarter, safer and more sustainable”. *International Journal of Computing and Digital Systems* 6 (04): 175–184.

Mekki, Kais, Eddy Bajic, Frederic Chaxel ja Fernand Meyer. 2019. “A comparative study of LPWAN technologies for large-scale IoT deployment”. *ICT express* 5 (1): 1–7.

Meulen, Rob van der. 2017. “Gartner Says 8.4 Billion Connected "Things"Will Be in Use in 2017, Up 31 Percent From 2016”. Viitattu 7. helmikuuta 2017. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016.

Naik, Nitin. 2018. “LPWAN technologies for IoT systems: choice between ultra narrow band and spread spectrum”. Teoksessa *2018 IEEE International Systems Engineering Symposium (ISSE),* 1–8. IEEE.

O’Neill, Maire, ym. 2016. “Insecurity by design: Today’s IoT device security problem”. *Engineering* 2 (1): 48–49.

Pacheco, J., ja S. Hariri. 2016. “IoT Security Framework for Smart Cyber Infrastructures”. Teoksessa *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W),* 242–247. doi:10.1109/FAS-W.2016.58.

Peña-López, Ismael, ym. 2005. “ITU Internet report 2005: the internet of things”.

Pradhan, Manas, Christoph Fuchs ja Frank T Johnsen. 2018. “A survey of applicability of military data model architectures for smart city data consumption and integration”. Teoksessa *2018 IEEE 4th World Forum on Internet of Things (WF-IoT),* 129–134. IEEE.

Ratasuk, R., B. Vejlgaard, N. Mangalvedhe ja A. Ghosh. 2016. “NB-IoT system for M2M communication”. Teoksessa *2016 IEEE Wireless Communications and Networking Conference,* 1–5. doi:10.1109/WCNC.2016.7564708.

Rescorla, Eric, ym. 1999. *Diffie-hellman key agreement method.* Tekninen raportti. RFC 2631, June.

Al-Sarawi, Shadi, Mohammed Anbar, Kamal Alieyan ja Mahmood Alzubaidi. 2017. “Internet of Things (IoT) communication protocols”. Teoksessa *2017 8th International conference on information technology (ICIT),* 685–690. IEEE.

Seneviratne, Suranga, Yining Hu, Tham Nguyen, Guohao Lan, Sara Khalifa, Kanchana Thilakarathna, Mahbub Hassan ja Aruna Seneviratne. 2017. “A survey of wearable devices and challenges”. *IEEE Communications Surveys & Tutorials* 19 (4): 2573–2620.

Sethi, Pallavi, ja Smruti R Sarangi. 2017. “Internet of things: architectures, protocols, and applications”. *Journal of Electrical and Computer Engineering* 2017.

Titi, S., H. B. Elhadj ja L. Chaari. 2019. “An ontology-based healthcare monitoring system in the Internet of Things”. Teoksessa *2019 15th International Wireless Communications Mobile Computing Conference (IWCMC),* 319–324. doi:10.1109/IWCMC.2019.8766510.

Torfs, Tom, Vladimir Leonov, Chris Van Hoof ja Bert Gyselinckx. 2006. “Body-heat powered autonomous pulse oximeter”. Teoksessa *SENSORS, 2006 IEEE,* 427–430. IEEE.

Tuecke, Steven, Von Welch, Doug Engert, Laura Pearlman, Mary Thompson ym. 2004. *Internet X. 509 public key infrastructure (PKI) proxy certificate profile.* Tekninen raportti. RFC 3820 (Proposed Standard).

Vermesan, Ovidiu, Peter Friess, Patrick Guillemin, Sergio Gusmeroli, Harald Sundmaeker, Alessandro Bassi, Ignacio Soler Jubert, Margaretha Mazura, Mark Harrison, Markus Eisenhauer ym. 2011. “Internet of things strategic research roadmap”. *Internet of things-global technological and societal trends* 1 (2011): 9–52.

Xiong, X., K. Zheng, R. Xu, W. Xiang ja P. Chatzimisios. 2015. “Low power wide area machine-to-machine networks: key techniques and prototype”. *IEEE Communications Magazine* 53 (9): 64–71.

Zhang, Z., M. C. Y. Cho, C. Wang, C. Hsu, C. Chen ja S. Shieh. 2014. “IoT Security: Ongoing Challenges and Research Opportunities”. Teoksessa *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications,* 230–234. doi:10.1109/SOCA.2014.58.