Jan Karvonen

Älykotiratkaisujen tietoliikenne ja tietoturva

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

27.4.2018

Metropolia

Tekijä Otsikko Sivumäärä Aika	Jan Karvonen Älykotiratkaisujen tietoliikenne ja tietoturva 28 sivua + 3 liitettä 27.4.2018
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoliikenne
Ohjaaja	Yliopettaja Janne Salonen

Insinöörityön tarkoituksena oli perehtyä kuluttajille suunnattuihin halpoihin älykotiratkaisuihin ja siihen, kuinka hyvin valmistajien lupaukset vastaavat todellisuutta.

Työssä perehdyttiin älykotiratkaisujen käyttämiin tekniikoihin ja niiden radiotaajuuksiin, sekä kilpailevien standardien tietoturvan toteutukseen ja tunnettuihin haavoittuvaisuuksiin. Pelkästään tekniikoihin perehtymällä saatiin hyvä käsitys siitä, kuinka hyvää tietoturvan tasoa voi odottaa eri tekniikoita käyttämällä.

Työssä testattiin kolmen eri valmistajan älykotiratkaisuja. Ratkaisujen tietoliikennettä tutkittiin liikennekaappausten avulla. Testien tarkoituksena oli tutkia eri valmistajien omien toteutusten eroja. Testeissä havaittiin suuria eroja toteutusten välillä, erityisesti siinä, miten laitteet kommunikoivat palvelimen kanssa. Testeissä kiinnitettiin huomiota myös laitteiden tietoturvaan ja arvioitiin sen ongelmakohtia. Tietoturvaa tutkittiin ensisijaisesti teknisen toteutuksen kannalta, mutta unohtamatta käyttäjärajapintaa.

Todettiin, että tietoturvallisen älykodin rakentaminen on tekniikkaan perehtymättömälle käyttäjälle lähes mahdoton tehtävä. Standardien tunteminen on hyvä alku, mutta standardien eri sukupolvien ja harhaan johtavien tuotemerkintöjen kanssa on vaikea varmistua suojauksen tasosta. Standardit eivät myöskään kata sitä, miten älykotiratkaisujen keskusyksiköt kommunikoivat valmistajan palvelimien kanssa, ja tämän toteutuksen luotettavuuden arvioinnissa kuluttaja on täysin valmistajan lupausten varassa.

Vaikka työn tarkoitus ei ollutkaan vertailla valmistajia toisiinsa, löytyi työn aikana selviä eroja eri valmistajien välillä.

Avainsanat	älykoti, IoT, Zigbee, Z-Wave

Author Title Number of Pages Date	Jan Karvonen Smart home systems' security and networking 28 pages + 3 appendices 27 April 2017
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialization Option	Telecommunications
Instructor	Janne Salonen, Principal Lecturer

The goal of this thesis work was to examine some cheap Smart Home solutions, which are widely available to the consumer market and see how well the manufacturers' promises resonate with reality.

The technologies and radio frequencies used by Smart Home systems were examined, as well as the security level of competing standards and their known vulnerabilities. By examining the technologies, a baseline of expected security levels was formed.

The Smart Home solutions from three different manufacturers were tested and the communication of the devices was analysed using traffic captures. The main purpose of the tests was to find the differences in implementation between the different manufacturers solutions. Major differences were found. The second purpose of the tests was to identify any security issues or vulnerabilities in the devices themselves, but also to examine the user interface from a security perspective.

It was found, that building a secure Smart Home is nearly impossible for a consumer that is not technically oriented. Knowing the common standards is a good start, but the differences between different generations of said standards and misleading package markings, makes it hard to be sure of the level of security achieved. The standards do not cover the communication between the Smart Home controller and the manufacturers cloud servers, and for the consumer to estimate the trustworthiness of this communication, he has to rely on the information provided by the manufacturer, if any.

While the main purpose of this work was not to directly compare different manufacturers, it came evident during the work, that there are big differences between their solutions.

Keywords	Smart Home, IoT, Zigbee, Z-Wave

Sisällys

Lyhenteet

IoT	*Internet of Things*. Esineiden internet.
kontrolleri	Älykotiratkaisun keskuslaite, joka ohjaa ja valvoo älykodin muita laitteita.
ISM	ISM-taajuusalueet (Industrial, Scientific and Medical) ovat teolliseen, tieteelliseen ja lääketieteelliseen käyttöön tarkoitettuja lisenssivapaita taajuusalueita.
ITU	*International Telecommunication Union*. Kansainvälinen televiestintäliitto.
ITU-R	Kansainvälisen televiestintäliiton radiokommunikaatiosta vastaava osasto.
WLAN	*Wireless Local Area Network*. Langaton lähiverkko.
Bluetooth	Lyhyen kantaman radiotekniikka, joka toimii 2,4 GHz:n taajuudella.
IEEE	*Institute of Electrical and Electronics Engineers.* Järjestö, joka muun muassa luo elektroniikkastandardeja.
OSI-malli	*Open Systems Interconnection Reference Model*. Standardoitu malli, jolla havainnollistetaan tietoliikenteen eri tasoja.
IP-osoite	Internetin protokollaosoite. Tunniste, jolla laite kommunikoi *Internet Protocol* -pohjaisissa verkoissa.
AES128	128-bittinen *Advanced Encryption Standard* -salaus.
Z/IP	*Z-Wave over IP*. Z-Waven protokolla *Internet Protocol* -protokollan käyttämiseen Z-Wave-verkossa.
kbps	Kilobittiä sekunnissa.
Mbps	Megabittiä sekunnissa.

SSID *Service Set Identifier.* WLAN-verkon tunnus, käytännössä langattoman verkon nimi.

IFTTT *If This Then That.* <ifttt.com>. Internetissä toimiva palvelu, jossa käyttäjä voi luoda ketjun ehdollisia lauseita palvelua tukevien ohjelmien tai laitteiden välisen toiminnan automatisoimiseksi.

TCP *Transmission Control Protocol*. Yleinen protokolla IP-verkkoon liitettyjen laitteiden väliseen kommunikointiin, jossa vastaanottaja kuittaa paketit vastaanotetuiksi.

UDP *User Datagram Protocol*. Yleinen protokolla IP-verkkoon liitettyjen laitteiden väliseen kommunikointiin, jossa paketteja ei kuitata vastaanotetuiksi.

TLS *Transport Layer Security.* Yleisesti käytössä oleva salausprotokolla. Käytetään mm. HTTPS-liikenteen salaukseen.

SSH *Secure Shell*. Protokolla, jota käytetään yleisesti muun muassa suojatun yhteyden luomiseen laitteen komentoriville tai konsoliin.

HTTP *Hypertext Transfer Protocol.* Protokolla web-sivujen näyttämiseen.

ONVIF *Open Network Video Interface Forum.* Järjestö, jonka tavoitteena on standardoida IP-pohjaisten videovalvontalaitteiden tietoliikennerajapinta.

GDPR *General Data Protection Regulation*. EU:n tietosuojauudistus, joka astuu voimaan 25.5.2018 [37].

1 Johdanto

Esineiden internet (Internet of Things, IoT) ja älykoti ovat trendikkäitä termejä, joilla kuvataan nykyistä tietoteknistä kehitystä. IoT:llä tarkoitetaan sitä, että lähes jokaisella laitteella on yhteys verkkoon, myös sähkölaitteilla ja kodinkoneilla, joilla ei yhteyttä ole aiemmin ollut. Älykoti on tästä puolestaan askeleen pidemmälle viety käsite, jossa näitä laitteita ja muuta kotiautomaatiota voidaan ohjata tietokoneella tai matkapuhelimella ja tarvittaessa myös etäältä. Älykodin ratkaisuissa tyypillisiä ovat fyysisen ympäristön tarkkailuun ja ohjaamiseen liittyvät toteutukset, kuten valo-ohjaus sekä kulun-, lämpötilan- ja kosteudenvalvonta. Pisimmälle vietynä älykodissa kaikkia toimintoja lukituksesta lähtien voidaan ohjata matkapuhelimella.

Työssä testataan kolmen älykotituotteisiin keskittyvän valmistajan älykodin aloituspaketteja. Testeissä tutkitaan liikennekaappauksien avulla, miten laitteet kommunikoivat keskenään ja mitä mahdollisia tietoturvaongelmia laitteissa esiintyy. Osana testejä arvioin käyttäjäkokemusta, sillä hienoinkin ratkaisu jää käyttämättä, mikäli se on käyttäjälle liian hankala ottaa käyttöön.

Insinöörityön tarkoituksena on selvittää, minkälaisia älykodin laitteita kuluttajille on nykyään tarjolla ja onko tekniikka valmista siihen, että aina vain kasvava kuluttajajoukko ottaa laitteita käyttöön tuntematta tekniikkaa niiden taustalla.

2 Älykodin tekniikat

Yleisesti ottaen älykodissa ohjataan sähkölaitteita verkon kautta, mikä mahdollistaa omien automaatioiden tekemisen, ja toinen yleinen termi älykodin tekniikalle onkin kotiautomaatio. Älykoti on samalla aika laaja markkinointitermi, jonka alla myydään monenlaisia elämää helpottavia tuotteita. Esimerkiksi langattomasti ohjattavia pistorasioita myydään älykotituotteina, vaikka niissä ei mitään verkkoyhteyttä olekaan. Tässä työssä keskityn älykotiratkaisuihin, joita voidaan ohjata etäältä. Kaikissa testatuissa paketeissa on kontrolleri, eli keskuslaite, joka ohjaa muita laitteita ja jota käyttäjä voi sitten itse ohjata vaikka matkapuhelimella.

Kaikissa testatuissa älykotipaketeissa edellytetään, että kodissa on jo toimiva Internet-yhteys ja kontrolleri pitää saada liitettyä lähiverkkoon johdolla. Lähes poikkeuksetta kaikki älykodin ohjaimet ja sensorit toimivat langattomasti. Ratkaisujen välillä on suuria eroja siinä, miten langaton kommunikointi tapahtuu kontrollerin kanssa.

Älykotilaitteet voidaan jakaa karkeasti eri kategorioihin sen mukaan, mitä langatonta tekniikkaa ne käyttävät. Älykotiratkaisuissa käytetään muitakin tekniikoita, kuin mitä tässä luetellaan, ja monien valmistajien kontrollerit tukevat useaa tekniikkaa, mutta kontrolleriin liitettävien älykotilaitteiden ja -sensorien osalta seuraavat käsiteltävät tekniikat ovat yleisimmät:

2.1 Standardoimattomat ISM-taajuudet

ISM-taajuusalueet (Industrial, Scientific and Medical) ovat teolliseen, tieteelliseen ja lääketieteelliseen käyttöön tarkoitettuja lisenssivapaita taajuusalueita. Yleisesti käytettyjä lisenssivapaita taajuusalueita Euroopassa ovat muun muassa 433:n, 868:n ja 2400 MHz:n alueet. Moni älykotilaite käyttää näitä taajuuksia hyväkseen, mutta kommunikointiin käytetään valmistajan omaa tai muuten standardoimatonta tekniikkaa.

433 MHz

Taajuusaluetta 433,05–434,79 MHz (jonka keskitaajuus on 433,92 MHz) voidaan ITU-R:n määrityksen mukaan käyttää vapaasti alueella 1 (muutamia maita lukuun ottamatta) [1]. Suomessakin tämä taajuusalue on tietyin edellytyksin lupavapaa. Suurin sallittu lähetysteho Suomessa 433,92 MHz:n taajuudella on 25 mW. [2, s. 7.]

Taajuutta 433,92 MHz (josta yleisesti käytetään vain lyhyttä nimeä ”433 MHz”) käytetään yleisesti kodin langattomissa laitteissa, kuten langattomissa ovikelloissa, langattomissa valokaukosäätimissä ja muissa vastaavissa sovelluksissa. Taajuusalueen etuna on, että sillä ei ole kovin paljon muuta liikennettä verrattuna esimerkiksi 2,4 GHz:n taajuusalueeseen, jolla toimii suuri osa langattomista kotiverkoista ja Bluetooth-laitteet. Radiotekniikan perusoppien mukaisesti, mitä pienempi taajuus, sen parempi kantama ja mitä pienempi taajuus, sitä paremmin radiosignaali läpäisee seiniä, jolloin suhteellisen matalataajuuksinen 433 MHz soveltuu erinomaisesti älykotikäyttöön.

433 MHz:n taajuusaluetta käyttävillä laitteilla ei ole yhteistä ohjelmistorajapintaa tai standardointia. Vaikka taajuutta käyttävien eri valmistajien laitteiden yhteensopivuuden pitäisi olla olematonta, ovat valmistajat itse lisänneet tukia muiden valmistajien tuotteille. Esimerkiksi testattu Cozifyn kontrolleri yhdistää Telldusin (Prooven) ja Nexan valmistamiin 433 MHz:n laitteisiin [3].

868 MHz

800–1000 MHz:n välillä on useita ISM-taajuuksia, ja niistä yleisimmin älykotikäytössä Euroopassa on 868 MHz. 868 MHz kantaa kohtuullisen pitkälle ja läpäisee seiniä hyvin verrattuna 2,4 GHz:n taajuusalueeseen. Moni valmistaja käyttää taajuutta hyväkseen omissa standardoimattomissa ratkaisuissaan ja taajuutta käytetään myös standardoiduissa Z-Wave- ja Zigbee-tekniikoissa. Suurin sallittu lähetysteho Suomessa 868 MHz:n taajuusalueella on 25 mW. [2, s. 8.]

2,4 GHz

2,4 GHz:n taajuusalue on ISM-taajuuksista eniten käytetty. Taajuusalueella toimivat WLAN-tukiasemat, Bluetooth, monet langattomat hiiret, näppäimistöt jne. 2,4 GHz:n taajuusalueen ruuhkaisuus on sen suurin ongelma. Todennäköisesti siksi, että 2,4 GHz:n taajuusalueelle on niin monta standardia (mm. WLAN, Bluetooth, Zigbee), ei markkinoilla ole juurikaan laitteita, jotka käyttäisivät taajuutta standardoimattomasti.

2,4 GHz:n kantama ja seinien läpäisykyky on heikompi kuin edellä mainittujen matalampien taajuuksien. Vaikka suurin sallittu lähetysteho on melko suuri (100 mW [2, s. 10]), se ei välttämättä riitä kompensoimaan häiriöiden ja radioteknisten ominaisuuksien aiheuttamaa kuuluvuusongelmaa. Lisäksi suuremman lähetystehon käyttäminen tarkoittaa suurempaa virrankulutusta lähettävällä laitteella, ja koska moni älykotisensori on paristokäyttöinen, ei virrankulutusta ole juuri varaa kasvattaa.

2.2 Langaton lähiverkko (WLAN)

Osa älykotilaitteista käyttää IEEE 802.11:n määritysten mukaista WLAN-verkkoa. WLAN-verkon käyttämisen etuna on, että voidaan käyttää jo kodista löytyvää langatonta verkkoa, eikä uutta verkkoa tarvitse luoda. Tämä mahdollistaisi myös älykotilaitteiden

käytön itsenäisesti ilman keskitettyä kontrolleria, joskin kaikki tässä työssä testatut ratkaisut ovat keskitetysti hallittuja. Älykotikäyttöä ajatellen on myös huomattava, että IEEE:n 802.11-työryhmä kehittää standardeja raskasta tiedonsiirtoa varten, jolloin esimerkiksi tiedonsiirtonopeus on tärkeämpi kriteeri kuin sähkönkulutus.

IEEE:n 802.11-2016-standardi on varsin kattava ja, riippuen siitä mitä siinä määriteltyjä tekniikoita käytetään, siirtonopeudet vaihtelevat suuresti. Koska älykotilaitteille on tärkeää olla yhteensopivia olemassa olevan verkon kanssa, ne käyttävät todennäköisesti 2,4 GHz:n taajuusaluetta 20 MHz:n kaistanleveydellä. Tällöin, riippuen samanaikaisten datavoiden määrästä (jota rajoittaa antennien määrä), suurin saavutettu datanopeus on 6,5–288,8 Mbps. [14.]

2.3 Z-Wave-tekniikka

Z-Wave on alun perin tanskalaisen Zensysin kehittämä tekniikka älykotien tiedonsiirtoon. Vuoden 2008 lopulla Zensysin osti yhdysvaltalainen Sigma Designs [4], mutta tuotemerkki Z-Wave on säilynyt käytössä. Z-Wave oli alun perin suljettu standardi, mutta sitä on avattu julkiseksi hiljalleen. Vuonna 2012 Z-Waven OSI-mallin fyysisen (L1) ja siirtokerroksen (L2) toimintaperiaatteet lisättiin osaksi ITU:n suositusta G.9959 [8; 9]. Elokuussa 2016 Sigma Designs julkisti Z-Waven ”yhteensopivuuskerroksen” eli OSI-mallin ylempiä kerroksia koskevat määritykset laitteiden välisestä kommunikaatiosta, joita G.9959 ei kattanut [10]. Nykyisellään kuka vain voi siis luoda Z-Wavea käyttävän laitteen, mutta Z-Waven virallisen logon käyttäminen ja sertifioinnin saaminen on maksullista.

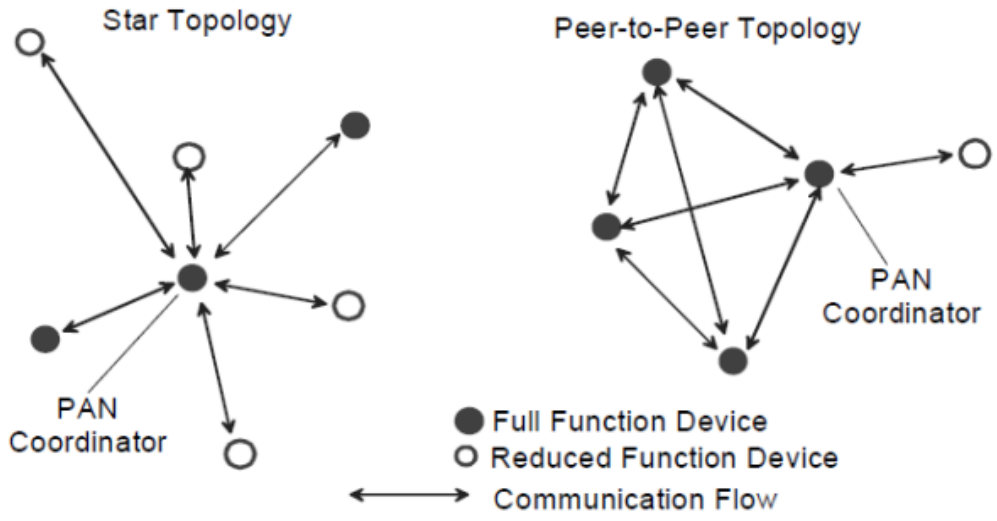
Tekniikka käyttää lupavapaita taajuuksia 800–1000 MHz:n alueella, joskin, aluekohtaisten rajoitusten vuoksi, käytetty taajuus vaihtelee alueittain. Euroopan unionissa käytetään taajuuksia 868,40 MHz ja 869,85 MHz. [6.] Z-Waven tiedonsiirtonopeus on korkeintaan 100 kbps [9, s. 17]. Suurinta sallittua lähetystehoa ei ole G.9959:n puitteissa määritetty, mutta siinä mainitaan, että lähetystehon tulisi olla paikallisviranomaisten määrittämissä rajoissa [9, s.19]. Suomessa näiden taajuusalueiden suurin sallittu lähetysteho on 25 mW [2, s. 8].

Yleensä Z-Wave-verkossa vain kontrollerilla on IP-osoite ja muut laitteet liitetään kontrolleriin sisäisiä tunnisteita käyttäen, mutta perusprotokollaa laajentavan Z-Wave over IP

(Z/IP) -protokollan avulla myös muille Z-Wave-verkon laitteille voidaan määrittää IP-osoite. Testatuissa laitteissa ei Z/IP-ominaisuutta ole.

Z-Wave-verkossa voi olla useampi kontrolleri eri rooleissa (esim. varakontrollerina, mobiilikontrollerina), mutta verkossa voi olla vain yksi aktiivinen pääkontrolleri, joka ylläpitää verkon topologiatietoja [13, s. 9]. Uutta verkkoa luotaessa pääkontrolleri luo verkolle HomeID-tunnisteen, joka on käytännössä 32-bittinen satunnaisluku (luku väliltä 0–4 294 967 295). Jokaiselle laitteelle tässä verkossa määritetään tämän lisäksi NodeID-tunniste, joka on käytännössä juokseva 8-bittinen numero. Koska osa NodeID-tunnisteista on varattu sisäiseen käyttöön, Z-Wave-verkossa voi olla korkeintaan 232 laitetta. [11.]

Z-Wave osaa toimia perinteisellä tähtitopologialla tai mesh-topologialla. Tähtitopologiassa kaikki laitteet ottavat suoraan yhteyden vain keskuslaitteeseen, kun taas meshissä laitteet ottavat yhteyden suoraan lähimpiin naapureihinsa. Mesh-topologia tunnetaan myös nimellä Peer-to-Peer. Kuva 1 havainnollistaa tähti- ja mesh-topologioiden eroa.



Kuva 1. Esimerkki laitteiden toiminnasta tähti- ja mesh-topologiassa. Mustat ympyrät ovat tässä esimerkissä meshin osaavia laitteita ja valkoiset laitteita, joista mesh-tuki puuttuu. [17.]

Kantamaksi laitteille luvataan 100 metriä, kun ne yhdistetään suoraan kontrolleriin, ja 200 metriä, kun yhteys kulkee ketjussa muiden laitteiden kautta. Peräkkäisten hyppyjen määrä ketjussa on kuitenkin rajoitettu neljään. [7.] Mainitut luvut ovat kuitenkin markkinointiosaston värittämiä ja erään käyttäjän tekemä käytännön testi osoitti todellisen kantaman olevan korkeintaan 27 metriä (kontrollerista lähimpään laitteeseen) [22]. Z-

Wavella on myös oma sisäinen reititysprotokolla, jolla se etsii nopeimman reitin jokaiseen laitteeseen mittaamalla laitteiden väliset viiveet. Protokolla tukee kolmea varareittiä laitetta kohti. [11.]

Z-Wavella on kaksi selkeää tuotesukupolvea, vanha Z-Wave ja uusi Z-Wave Plus. Suurin ero sukupolvilla on tietoturva. Suurimmassa osassa vanhoista Z-Wave-laitteista, liikenne laitteiden välillä ei ole salattua. Laitteilla on tunnisteisiin pohjautuva varmennus, jonka pitäisi estää muita kontrollereita hallitsemasta niille kuulumattomia laitteita, mutta sitä vastaan on jo hyökkäysmenetelmä [15]. Salaus (AES128) on osa uutta Z-Wave Plus -standardia, ja se on myös saatavilla osaan vanhoista Z-Wave-laitteista. [7.] Tilanteen tekee hankalaksi se, että vaikka Z-Wave Plus -standardiin on sisäänkirjoitettu tuki salaukselle, salausta ei ole pakko ottaa käyttöön saadakseen Z-Wave Plus -sertifioinnin [30]. Kuluttajalle on siis hyvin vähän takeita siitä, että Z-Wave-yhteys on salattu, ja jää laitevalmistajan harteille informoida kuluttajaa salauksen saatavuudesta.

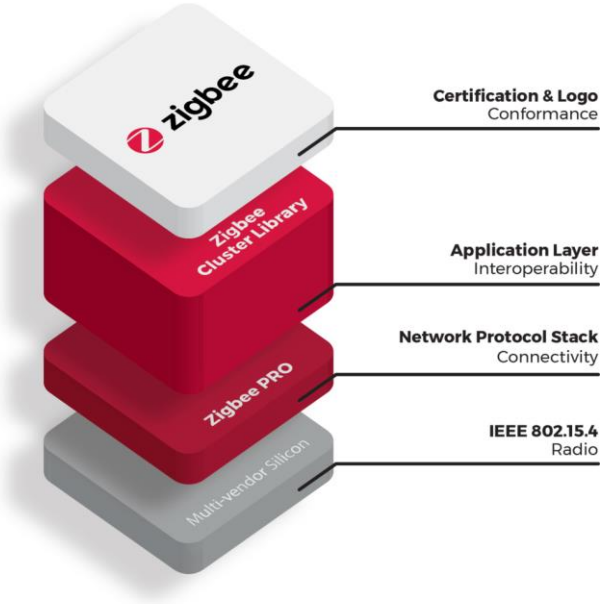
Z-Waven sertifiointiohjelmien ansiosta Z-Wave-laitteiden keskinäinen yhteensopivuus on hyvä [7]. Yhteensopivuutta kuitenkin rajaavat hieman edellä mainitut alueelliset taajuusrajoitukset ja puutteet salauksessa.

2.4 Zigbee-tekniikka

Zigbee on markkinointinimi laitteille, jotka pohjautuvat IEEE:n 802.15.4-standardiin. Zigbee on avointa tekniikkaa, sitä ei siis omista mikään yksityinen taho. Zigbeen kehityksestä ja laitteiden sertifioinnista vastaa vuonna 2002 perustettu voittoa tavoittelematon ZigBee Alliance. [16.]

Kuten kilpailevalla Z-Wavellakin, avoinstandardi, tässä tapauksessa IEEE 802.15.4, kattaa vain OSI-mallin fyysisen (L1) ja siirtokerroksen (L2) toiminnan [17]. Tätä standardia on laajennettu Zigbee PRO -kokonaisuudella, joka tuo mukanaan OSI-mallin verkkokerroksen (L3) toimintoja, kuten laitteiden välisen salauksen (AES128) ja mesh-yhteydet [18]. Uusin versio, Zigbee 3.0, tuo mukanaan Zigbree PRO:n toiminnot ja yhdistää aiemmin erillään olleita Zigbeen alaisia kehityslinjoja saman kokonaisuuden alle. Zigbee 3.0 lisää esimerkiksi ”Green Power” -toiminnon, joka antaa yhteensopivien vähävirtaisten laitteiden ottaa tarvitsemansa käyttövirran suoraan radioaalloista. [19.] Kuva 2 esittää

Zigbeen 3.0:n eri osioita. Kaikkien Zigbee-versioiden pitäisi olla keskenään yhteensopivia [18].



Kuva 2. Zigbee 3.0:n osiot [18].

Zigbee käyttää sekä 2,4 GHz:n taajuutta maailmanlaajuisesti että alle gigahertsin taajuusalueita paikallisesti, ja tarkat taajuudet vaihtelevat alueittain [20]. Euroopassa Zigbee käyttää yleisesti 2,4 GHz:n lisäksi 868 MHz:n taajuutta [18]. Vaikka IEEE 802.15.4-standardin lisäyksessä 5 vuodelta 2017 (802.15.4v-2017) määritellään myös taajuusalue 915–921 MHz käytettäväksi Euroopassa [20], tämä taajuusalue oli Euroopassa varattu radiopuhelinkäyttöön jo vuonna 2004 [21]. Vaikka Zigbee käyttääkin 2,4 GHz:n taajuutta, se ei tue IEEE 802.11-standardia, eli se ei ole yhteensopiva WLAN-verkkojen kanssa, ja saman taajuusalueen takia tekniikat häiritsevät toisiaan.

Zigbeen käytännön lähetystehoista on vaikea saada luotettavaa tietoa, sillä lähetystehojen rajoja ei ole määritelty 802.15.4-standardissa. Onkin oletettava, että valmistajat käyttävät taajuusalueiden suurimpia sallittuja lähetystehoja, jotka ovat 100 mW 2,4 GHz:n alueella ja 25 mW 868 MHz:n alueella [2]. Zigbeen kantama on käytännön testeissä osoittautunut lyhyemmäksi kuin Z-Waven: Zigbeen kantama oli alle 12 metriä sisätiloissa [23]. Edellä mainittu testi oli tehty 2,4 GHz:n taajuudella, joka selittää hyvin miksi kantama on Z-Wavea lyhyempi, joka käyttää matalampaa taajuutta. Toki 2,4 GHz:n taajuudella suurin sallittu lähetysteho on korkeampi kuin 868 MHz:llä, mutta tämä ei riitä kompensoimaan taajuudesta johtuvaa kantaman pienentymistä ja seinissä tapahtuvaa

häviötä. Radioteknisesti Z-Waven ja Zigbeen kantaman pitäisi olla samalla tasolla 868 MHz:n taajuudella, mutta todennäköisesti suurin osa Zigbee-laitteista toimii vain 2,4 GHz:n taajuudella, joka on käytössä globaalisti ilman alue-eroja.

IEEE 802.15.4-standardi tukee monia eri modulaatiotekniikoita ja taajuuksia. Zigbeen suurin mahdollinen siirtonopeus riippuu käytetyistä taajuuksista ja modulaatioista. Suomessa käytetyillä taajuuksilla Zigbeen suurin mahdollinen siirtonopeus on 250 kbps. [17]. Laitteiden osoitteet Zigbeessä ovat 16-bittisiä [17, s.154], minkä perusteella yhdessä Zigbee-verkossa voi olla 2^{16} (65 536) laitetta. Siirtotien häiriöt ja käytettävissä olevan kaistanleveys rajoittavat laitteiden määrän käytännössä paljon pienemmäksi, mutta on epätodennäköistä, että tavallisessa kotiverkossa olisi edes sataa laitetta.

Tietoturvan kannalta Zigbee on varsin hyvällä mallilla, ainakin uusimman Zigbee 3.0 -sukupolven myötä. Alkuperäisessä Zigbee-versiossa oli kuitenkin merkittäviä tietoturvapuutteita. Zigbeen salausta varten on käytössä kaksi salausavainta: verkkoavain (Network Key), joka on koko verkolle yhteinen avain, ja linkkiavain (Link Key), joka on jokaisen langattoman hypyn avain. Uuden ennestään tuntemattoman laitteen liittyessä verkkoon Zigbee lähetti verkkoavaimen käyttäen linkkiavaimella suojattua yhteyttä. Mutta koska uusi laite ei ollut vielä liittynyt verkkoon, eikä yhteistä luotettua linkkiavainta keskuksen kanssa ollut vielä muodostettu, verkkoavaimen lähetykseen käytettävä linkkiavain oli aina sama: ”ZigBeeAlliance09”. Uuden laitteen liittyessä verkkoon oli siis mahdollista kaapata langatonta liikennettä kuuntelemalla koko verkon salausavain. Todellista riskiä pienensi se, että kaappaus piti tehdä juuri sillä hetkellä, kun uusi laite oli liittymässä verkkoon. [24; 25.]

Zigbee 3.0:n myötä lisättiin vaatimus laitekohtaisesta asennusta varten käytettävästä linkkiavaimesta (Install Code), jonka tulee olla tulostettuna laitteen pakettiin tai dokumentaatioon ja olla luettavissa helposti älypuhelimella, esimerkiksi QR-koodin muodossa [26]. Tämä laitekohtainen avain poistaa riskin, joka esiintyi aiemmin uutta laitetta liitettäessä, mutta lisää laitetta käyttöönottavalle kuluttajalle yhden työvaiheen.

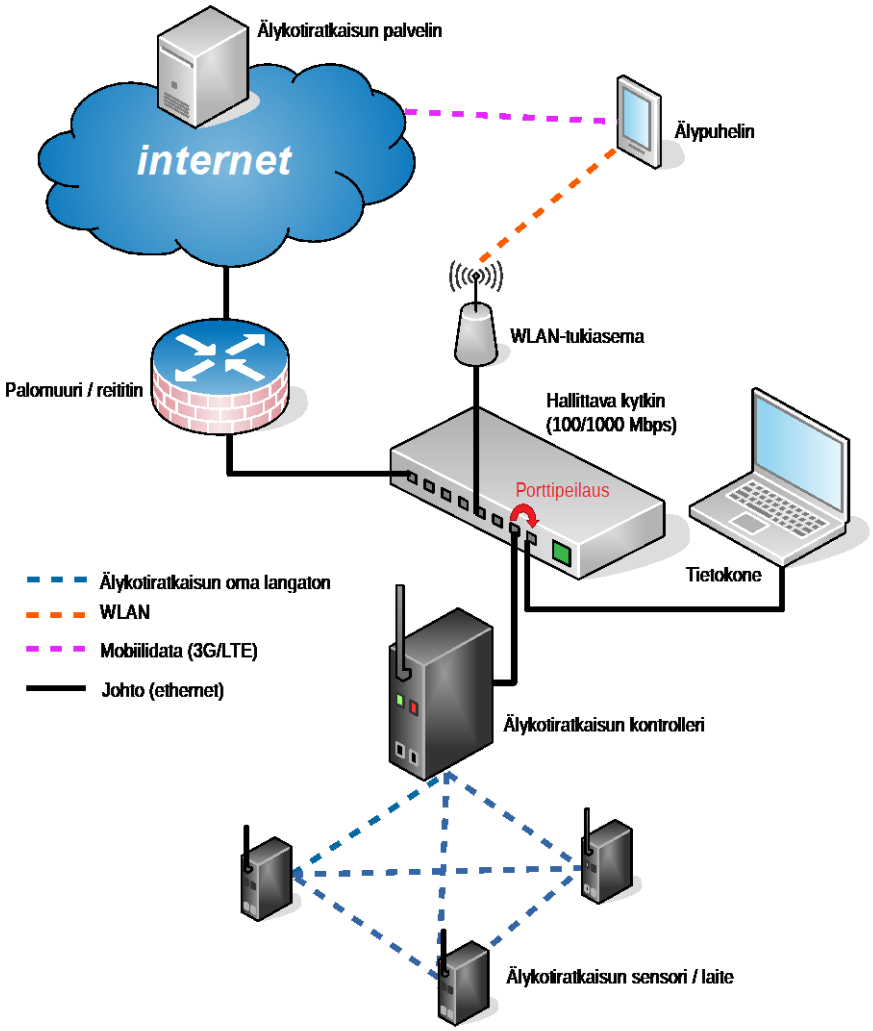
3 Älykotijärjestelmien testaus

3.1 Testiympäristö

Insinöörityön osana testattiin älykotilaitteiden tietoliikennettä. Testien tarkoituksena oli tutkia, miten laitteet kommunikoivat valmistajan palvelimien kanssa. Tärkein osa testistä oli liikennekaappaus, jolla saatiin tallennettua kaikki laitteiden ja palvelimen välillä liikkuva tieto. Liikennekaappauksesta selvisi suoraan, onko liikenne salattua, kuinka paljon tietoa vaihdettiin ja millä protokollalla tietoa lähetettiin. Liikennekaappausten lisäksi testattiin laitteiden tietoturvaa tutkimalla, mitkä portit ovat laitteissa auki, sillä jokainen ylimääräinen avoin portti on tietoturvan kannalta ongelma. Esimerkiksi loppuvuodesta 2016 tuhansia suomalaisia modeemeita kaapannut Mirai-haittaohjelma käytti hyväkseen avoimia portteja [38].

Pyrin suunnittelemaan laitteiden testiympäristön niin, että siinä olisi mahdollisimman vähän liikennettä muista kuin älykotiratkaisun omista laitteista. Ympäristön ytimessä on hallittava kytkin, johon tehtiin oma virtuaalinen lähiverkko (VLAN) testiä varten. Samainen VLAN jatkettiin myös WLAN-tukiasemalle, jossa VLAN sidottiin omaan SSID-tunnukseensa. Myös testiympäristön palomuuri tukee VLAN-verkkoja, jolloin testiverkko saatiin erotettua palomuurissa muusta verkosta ohjelmallisesti ja liikennettä voidaan analysoida tarkemmin.

Testattava älykotikontrolleri tulee suoraan kiinni kytkimeen, ja älykodin laitteet ottavat langattomasti yhteyden kontrolleriin. Yhteen kytkimen porttiin liitettiin tietokone, jolla tehtiin liikennekaappaukset Wireshark-ohjelmalla. Liikennekaappauksen onnistumiseksi kytkimeen tehtiin porttipeilaus. Peilaus tehtiin siitä portista, jossa kontrolleri oli kiinni, siihen porttiin, jossa tietokone oli kiinni. Peilattavasta ja peilauksen kohteena olevasta portista poistettiin käytöstä kaikki muut VLAN:t, ettei liikennekaappauksiin tullut turhaa liikennettä muista käytössä olevista verkoista. Jokaiselle kokoonpanolle suoritettiin kolme liikennekaappausta: kaappaus, kun laitteet käynnistetään ensimmäisen kerran, kaappaus tilanteessa jossa verkossa ei tapahdu muutoksia, ja kaappaus älypuhelimen sovelluksen liikenteestä. Viimeistä mainittua kaappausta varten porttipeilausta muutettiin niin, että peilattava portti oli kiinni lähiverkon WLAN-tukiasemassa ja kaappauksesta suodatettiin pois muut kuin testiverkon VLAN:n liikenne. Kuva 3 havainnollistaa testiverkon topologiaa.



Kuva 3. Testiympäristön topologia.

Osaa testatuista älykotiratkaisuista voi ohjata sekä älypuhelimella että tietokoneella, mutta tavoitteeni oli ohjata laitteita ensisijaisesti älypuhelimella, niin pitkälle kuin mahdollista. Testiympäristössä älypuhelin voidaan liittää suoraan testiverkon langattomaan tukiasemaan tai ottaa yhteys julkisen verkon puolelta käyttämällä 3G/LTE-yhteyttä.

3.2 Testi 1: Sen.sen Mother-kontrolleri ja Cookies-sensorit

Sen.se on ranskalainen älykotiratkaisuja valmistava yritys. Sen.sen ratkaisu perustuu pienten paristokäyttöisten sensorien käyttämiseen. Ne kommunikoivat kontrollerin eli ”Motherin” kanssa. Testissä oli Sen.sen myynnistä poistumassa olevat Cookie-sensorit, jotka pystyvät mittaamaan lämpötilaa ja liikettä (kuvassa 4). Sensorit ovat monikäyttöisiä, ja käyttämällä Sen.sen hallintaliittymän eri sovelluksia, voidaan muodostaa erilaisia hälytyksiä pohjautuen sensorien lähettämään tietoon:

- Oveen kiinnitetty sensori tunnistaa liikkeen perusteella, että ovi avataan.

- Käyttäjän mukana kulkevalla sensorilla voidaan seurata, onko käyttäjä kotona.

- Lääkeannostelijaan, hammasharjaan tai vaikka kastelukannuun liitettyä sensoria voidaan käyttää seuraamaan esineen käyttöä. Tässä tapauksessa järjestelmä hälyttää, kun esinettä ei ole liikutettu määrättynä aikana.

Kuva 4. Sen.sen Mother-kontrolleri ja pari Cookie-sensoria.

Sen.sen ratkaisu poikkeaa muista testatuista ratkaisuista sillä, että siinä ei ole mitään muita laitteita ohjaavia komponentteja, kuten kauko-ohjattavia pistorasioita, vaan se ainoastaan tarkkailee ympäristöään. Sen.sen laitteen saa liitettyä IFTTT-palveluun, joka on internetissä toimiva automatisointipalvelu eri ohjelmien ja laitteiden välille, mutta natiivia tukea laitteiden ohjaamiseen ei Sen.sellä ole.

Langaton yhteys kontrollerin ja sensorien välillä tapahtuu 868 MHz:n taajuudella. Tämä tieto selvisi vain laitteen paketista, sillä Sen.se ei itse kerro kotisivuillaan käyttämistään tekniikoista juuri mitään. Sen.sen tuotteita ei löydy sen enempää Z-Waven kuin Zigbeen sertifioitujen laitteiden listoilta [27; 28], joten Sen.se käyttänee jotain standardien ulkopuolista tekniikkaa tai ei ole hakenut sertifiointia.

Laitteiden käyttöönotto on helppoa. Kontrolleri liitetään sähköverkkoon ja lähiverkkojohdolla kotiverkkoon. Sensoreihin laitetaan vain mukana tulevat paristot sisään, minkä jälkeen ne ovat käyttövalmiit. Laitteiden liittäminen toisiinsa ja niiden ohjaaminen vaatii

maksutonta rekisteröitymistä Sen.sen kotisivuille. Rekisteröitymisen jälkeen kontrolleri liitetään omaan tiliin kirjoittamalla kotisivuille kontrollerin taakse kirjoitettu yksilöllinen nimi ja koskettamalla kontrolleria fyysisesti. Sensorit löytyvät automaattisesti kontrollerin alueelta, mutta omistajuus pitää niissäkin vahvistaa fyysisellä kosketuksella. Yksilöllisten nimien ja fyysisen kosketuksen vaatimus ovat hyviä menetelmiä varmistamaan, että liitetyt laitteet ovat oikeasti omassa hallussa, ja se on kuluttajalle varsin yksinkertainen prosessi. Kun laitteet on asennettu, voidaan verkkoa ohjata Sen.sen kotisivujen hallintapaneelin kautta tai älypuhelimeen asennettavan ohjelman avulla, joka näyttää sekin saman hallintapaneelin. Hallintapaneelista voi lisätä sensoreille haluamansa toiminnot valitsemalla haluamansa sovellukset ja liittämällä ne sensoreihin. Jokainen sensori voi olla osa useampaa sovellusta, esimerkiksi oven liikkeitä tunnistava sensori voi samalla mitata lämpötilaa. Vaikka käyttöönotto ja käyttö on tehty selkeäksi, suomalaisen kuluttajan kannalta on ikävää, että laitetta ei voi hallita suomeksi.

Tietoliikenteen kannalta Sen.sen ratkaisu vastaa pääpiirteiltään muita testattuja kokonaisuuksia. Sensorit lähettävät mittaustuloksensa kontrolleriin langattomasti, ja kontrolleri puolestaan lähettää tiedot eteenpäin Sens.sen palvelimille, jotka Sen.sen rekisteriselosteen mukaan sijaitsevat Saksassa [29]. Koko älykodin hallinta on siis saksalaisella palvelimella. Tehtyjen liikennekaappausten perusteella kontrolleri lähettää sensorien tietoja jatkuvasti palvelimelle. Vastaavasti älypuhelimen ohjaussovellus kommunikoi suoraan Saksan palvelimen kanssa, joka puolestaan ohjaa kontrolleria. Vaikka kännykkä olisi samassa lähiverkossa kuin kontrolleri, tapahtuu kaikki liikenne palvelimen kautta kierrättäen. Tämä liikenteen kierrättäminen palvelimen kautta aiheuttaa vääjäämättä viiveitä palveluiden käyttöön hitaissa verkoissa. Sen.sen ratkaisussa tosin ei ole mitään muita laitteita ohjaavia komponentteja, vaan ainoastaan tietoa kerääviä, joten viiveet eivät ole käytön kannalta niin merkityksellisiä.

Tietoliikenne kontrollerin ja palvelimen välillä tapahtuu TCP-paketeilla. Kontrolleri lähettää palvelimelle paketin aina, kun verkossa muuttuu jotain. Muutos voi olla vaikka niin pieni, että yhden sensorin signaalin voimakkuus muuttuu. Jos verkossa ei ole luonnostaan mitään lähetettävää 10 sekunnin aikana, lähettää kontrolleri palvelimelle ”TCP Keep-Alive” -paketin yhteyden ylläpitämiseksi. Vaikka paketteja lähetetään usein, liikenteen kuorma ei ole kovin suuri. Verkon ollessa vakaana keskimääräinen tiedonsiirtokuormitus oli 287 bittiä sekunnissa. [Liite 1.]

Tietoturvan kannalta Sen.sen ratkaisu on suorastaan surullinen: kontrollerin ja palvelimen välinen liikenne on täysin salaamatonta. Koska Sen.sen langaton verkko ei ole standardoitua tekniikkaa, voi senkin olettaa olevan salaamaton. Kun nämä seikat yhdistetään siihen, että kaikki liikenne kiertää aina julkisen verkon kautta, vaikka siihen ei olisikaan tarvetta, voidaan Sen.sen ratkaisun toteutusta pitää hyvin riskialttiina.

Seuraavassa on tuloste tietoliikennepaketista, jolla palvelin määrittää kontrollerin asetuksia: vastaavan paketin väärentämällä voisi esimerkiksi muuttaa, mihin osoitteeseen kontrolleri lähettää tietojaan, tai tehdä vain kiusaa käyttäjälle vaihtamalla merkkivalojen värejä, tai laitteen äänenvoimakkuutta. Sen.sen mobiilisovellus toimii sentään hieman paremmin kuin palvelimen ja kontrollerin välinen liikenne, mobiilisovelluksesta lähtevä liikenne on TLS-salattu. Tämä on kuitenkin pieni lohtu, sillä liikenne on salattu vain palvelimelle asti, kun taas palvelimelta kontrollerille liikenne on edelleen salaamatonta.

```
No.   Time       Source          Destination     Protocol     Length
160   374.272050 144.76.166.244  172.21.42.101   WebSocket    340

Frame 160: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits)
on interface 0

Ethernet II, Src: ZyxelCom_70:c3:be (b0:b2:dc:70:c3:be), Dst: Micro-
chi_e7:52:c7 (00:1e:c0:e7:52:c7)

Internet Protocol Version 4, Src: 144.76.166.244, Dst: 172.21.42.101
Transmission Control Protocol, Src Port: 80, Dst Port: 1251, Seq: 828,
Ack: 2232, Len: 286

WebSocket
Line-based text data
[truncated]{"body": {"stateFrequency": 180,"smileLed": "255,0,0","serv-
erUrl": "in.sen.se","rightLed": "160,0,240","rfPower": 100,"leftLed":
"160,0,240","serverPort": 80,"maxConn": 24,"soundLevel": 50}, "type":
"gateway", "resource
```

Sen.sen kontrollerista ei löytynyt porttiskannauksella yhtään avointa porttia, mutta tämäkään ei toiminut ongelmitta, sillä UDP-porttiskannaus yhdistettynä mahdollisen avoimen palvelun version tarkastamiseen sai kontrollerin uudelleenkäynnistyssilmukkaan, eikä silmukka päättynyt, ennen kuin skannauksen lopetti. Tämä tarkoittaa, että ilman verkossa olevaa erillistä palomuuria kontrolleri olisi altis julkisesta verkosta tuleville palvelunestohyökkäyksille.

Edellä mainittujen teknisen toteutuksen ongelmien lisäksi en saanut Sen.seltä pyynnöistä huolimatta minkäänlaista tietoa siitä, miten sen omat palvelimet on suojattu, miten käyttäjiltä kerättyä tietoa säilytetään tai kuka siihen pääsee käsiksi. Luonnollisesti

ranskalaisen yhtiön pitää noudattaa eurooppalaisia tietosuojalakeja, mutta oikeudellinen vastuu ei takaa sitä, että palvelimen suojaus olisi tehty asianmukaisesti.

3.3 Testi 2: Telldusin Z-Wave -aloituspaketti

Telldus on yksi ruotsalaisen automaatioratkaisutoimittaja Proove Ab:n tuotemerkeistä. Testatussa paketissa oli Tellstick ZNet Lite v1 -kontrolleri, oveen tai ikkunaan liitettävä magneettisensori ja kaksi kauko-ohjattavaa pistorasiaa (kuva 5). Kaikki paketissa mukana olevat laitteet ovat Z-Wave Plus -standardin mukaisia ja tukevat salausta. Z-Waven lisäksi kontrolleri tukee myös 433 MHz:n taajuutta, mutta osaa vain lähettää kyseisellä taajuudella, ei vastaanottaa. Tämä tarkoittaa, että kontrolleri voi esimerkiksi käskeä 433 MHz:n taajuutta käyttävän kauko-ohjattavan pistorasian päälle tai pois, mutta ei osaa lukea 433 MHz:a käyttävän lämpömittarin tietoja. 433 MHz:n vastaanotto olisi saatavilla laitteen uudemmassa versiossa (Tellstick ZNet Lite v2) [31].

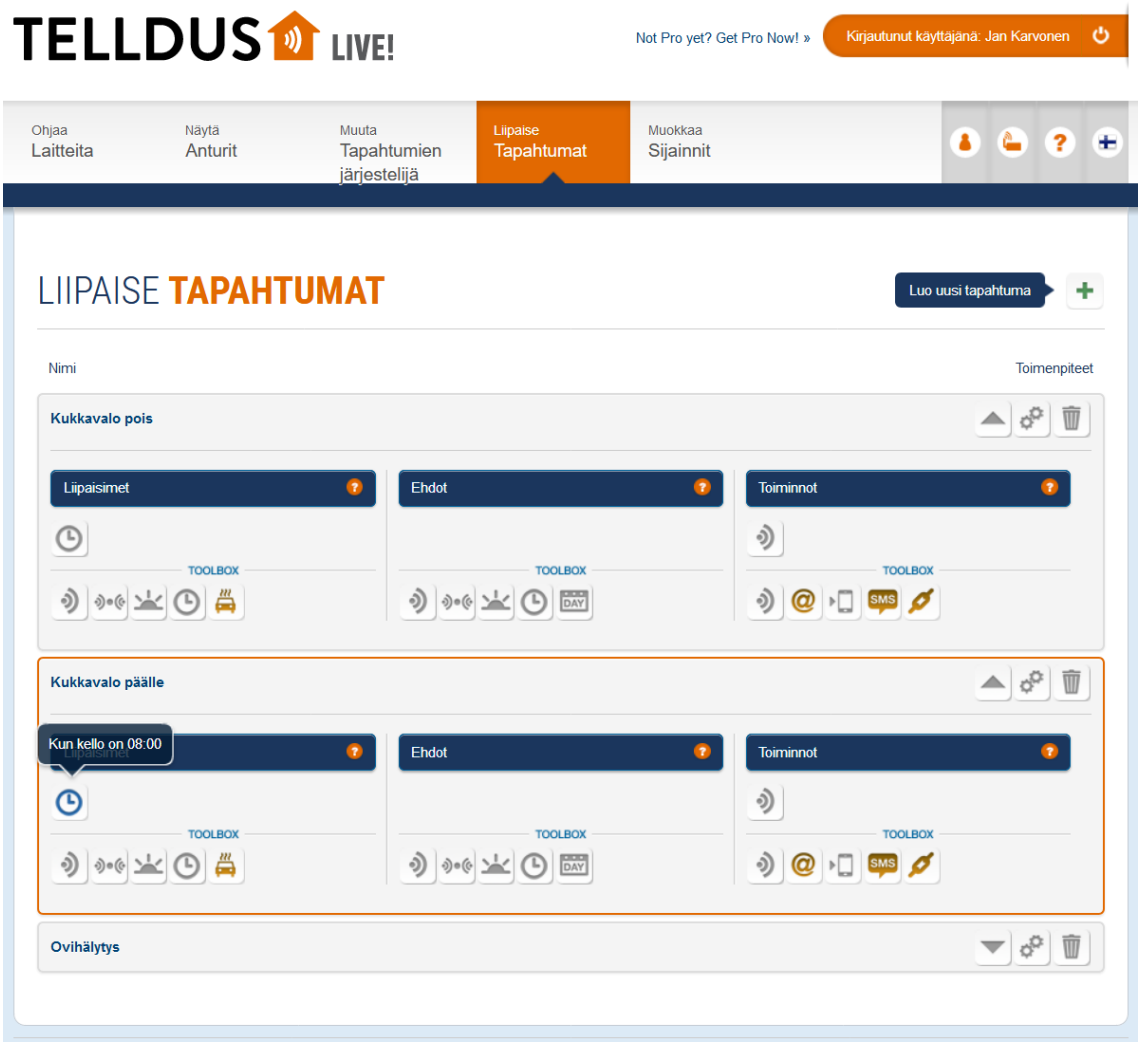
Kuva 5: Telldus Znet Lite, oven tai ikkunan magneettisensori ja kauko-ohjattava pistorasia.

Järjestelmän käyttöönotto on Telldusillakin helppoa. Kontrolleri liitetään sähköverkkoon ja lähiverkkojohdolla kotiverkkoon. Kontrolleri ottaa heti yhteyden palvelimelle ja päivittää itsensä, jos uudempi ohjelmistoversio on saatavilla. Telldusin palvelun käyttö vaati maksuttoman rekisteröinnin live.telldus.com-sivustolle. Kun rekisteröinti on tehty, pitää kontrolleri liittää tiliin, joko syöttämällä kontrollerin pohjassa lukevat tunnistetiedot tai automaattisella tunnistuksella, joka pohjautuu kontrollerin ja selaimen julkisten IP-osoitteiden vastaavuuteen [30]. Testissä automaattinen tunnistus toimi moitteetta, mutta se voi olla

ongelmallinen yhteyksissä, missä useammalla käyttäjällä on sama julkinen IP-osoite, kuten mobiilidatayhteyksissä usein on.

Sensoreiden ja muiden laitteiden liittämisprosessi riippuu laitteen käyttämästä tekniikasta. Z-Wave-laitteet liitettiin käynnistämällä liittämistoiminto hallintasivulta ja painamalla liitettävässä laitteessa olevaa painiketta kolme kertaa. Liittämistä hankaloitti se, että hallintasivu antoi valita joko salaamattoman Z-Waven yhdistämisen tai salatun yhdistämisen. Salatun yhdistämisen toiminto kehotti etsimään tuotepaketeista Z-Wave Secure -logoa, mutta tuotepaketeissa oli vain Z-Wave Plus -logot. Salattu yhdistäminen onnistui, mutta logojen eroavaisuus tuotepakettien ja käyttöliittymän välillä on harhaanjohtavaa. Keskusteltuani Telldusin tuen kanssa selvisi, että järjestelmän salatun yhdistämisen toiminto toimii myös salaamattomille laitteill;, toiminto kertoo vain, jälkeenpäin saatiinko yhteys salattua [30]. Tästä herääkin kysymys, miksi käyttöliittymässä on erikseen toiminto salaamattomalle yhdistämiselle, jos salatun yhdistämisen toimintokin osaa yhdistää myös salaamattomasti? Telldusilta kerrottiin, että salaamattoman yhdistämisen toiminto haluttiin kuitenkin pitää vaihtoehtona, muun muassa siksi, että salattu yhdistäminen kuluttaa laitteiden paristoja enemmän, jolloin käyttäjä voi valita sähköä säästävän vaihtoehdon vähemmän kriittisille laitteille [30].

Itse laitteiden hallinta tapahtuu Telldusin web-sivujen ”Telldus Live!” -palvelun kautta (kuvassa 6) tai älypuhelimeen saatavalla sovelluksella. Suomalaisen kuluttajan kannalta on positiivista, että Telldusin web-hallinta on saatavilla suomeksi, joskin rekisteröintisivu ja mobiilisovellus ovat toistaiseksi vain englanniksi. Laitteiden ehtojen ohjelmoinnin, eli ”liipaisimet”, saa asetettua vain web-hallinnan kautta, mutta ohjelmointi on helppoa ja vaihtoehtoja on paljon. Ihan perustasolla ohjelmointi voi perustua aikaan, esimerkiksi niin, että jokin lamppu palaa asetetulla aikavälillä. Ohjelmoinnin voi myös viedä pidemmälle niin, että toiminnot riippuvat järjestelmän omien sensorien syötteistä tai laitteiden tilasta. Esimerkkinä voisivat olla vaikka sälekaihtimet, jotka laskeutuvat alaspäin, kun valoisuusanturi havaitsee, että huoneen valoisuus ylittää annetun raja-arvon. Mobiilisovellus on huomattavasti rajoitetumpi, mutta selkeä käyttää, ja se mahdollistaa hälytyksien vastaanottamisen suoraan puhelimeen.



Kuva 6: Telldusin web-hallinta ja sen ehtojen ohjelmointi [39].

Tietoliikenne kontrollerilta palvelimelle tapahtuu käyttäen yksittäistä TCP-vuota, jota kumpikin pää ylläpitää. Yhteyttä ylläpidetään varsin verkkaisesti, ja Telldusin tuki tiesi kertoa, että jos kummallakaan päällä ei ole mitään lähetettävää toiselleen luonnollisesta syystä, kumpikin pää lähettää paketin yhteyden ylläpitämiseksi kahden minuutin kuluttua. Sitten jos yhteyttä ei saada kuuteen minuuttiin, tulkitsee palvelin kontrollerin sammuneeksi. [30.]

Telldusin ratkaisussa kaikki liikenne kiertää yrityksen pilvipalvelimien kautta. Telldus suunnittelee lisäävänsä myös mahdollisuuden kontrollerin suoraan hallintaan sisäverkon kautta, mutta toistaiseksi ominaisuutta ei vielä tueta [32]. Yrityksen ratkaisussa on onnistuttu minimoimaan turha tietoliikenne, ja kun järjestelmä oli muutoksettomassa tilassa, sain mitattua liikennemääräksi vain 76 bittiä sekunnissa, joka on merkityksettömän pieni liikennemäärä [liite 2].

Tietoturvan taso vaihtelee Telldusissa osioittain. Liikenne kontrollerin ja palvelimen välillä, kuten myös mobiilisovelluksen ja palvelimen välillä, on TLS-salattua. Liikenne kontrollerin ja ohjattavien laitteiden välillä voi olla salattu, jos ohjattava laite salausta tukee. Telldusin palvelimilla ei ole tällä hetkellä tietoturvasertifiointeja, mutta yrityksen tuki kertoi niiden hankkimisen olevan prioriteettilistalla [30].

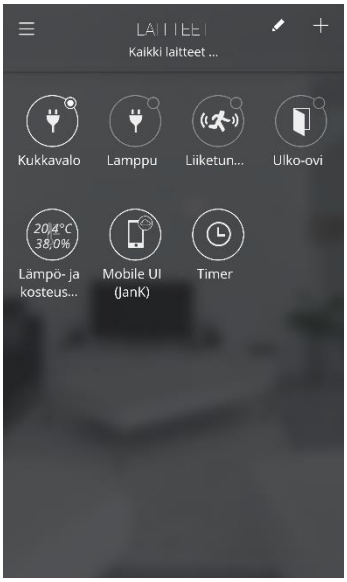
Telldusin kontrollerista löytyi kolme avointa porttia: TCP-portit 22 ja 80 sekä UDP-portti 30303. TCP-porttia 22 käyttää SSH-protokolla, ja TCP-porttia 80 käyttää HTTP-protokolla. Telldus ei paljasta SSH:n käyttöön tarvittavia tunnuksia, ja nopeasti testattuna ilman tunnuksia yhteyttä ei saa avattua, mutta itse palvelun olemassaolo viittaa siihen, että Telldusilla on juuritason tunnukset laitteen hallintaa varten. HTTP:n käyttäjätunnukset puolestaan tarkistetaan Telldusin palvelimelta, eli samalla käyttäjätunnuksella, jolla kirjaudutaan pilvipalvelimelle, pääsee myös laitteen paikalliseen HTTP-palvelimeen kiinni. Paikallisen liittymän kautta ei voi tehdä muuta kuin suorittaa laitteella skriptejä, mikä on itse asiassa hyödyllisempi työkalu hyökkääjälle, kuin laitteen tavalliselle käyttäjälle. Telldusin tuen mukaan nämä palvelut ovat auki valmistautumisena paikallisen hallintatoiminnon lisäämiseen [30]. Samoin viimeinen avoin portti, UDP 30303, on auki paikallista hallintaa varten. Tämän portin avulla Telldusin laitteet löytävät toisensa lähiverkosta [32]. On erittäin huolestuttavaa, että laitteisiin on jätetty tällainen hyökkäysrajapinta toiminnallisuuden takia, jota ei vielä ole toteutettu.

3.4 Testi 3: Cozify Hub 1.1 ja Telldusin 433 MHz:n sensorit

Cozify on suomalaisen Cozify Oy:n tuote [33]. Toisin kuin muilla testatuilla älykotijärjestelmillä, Cozifylla ei ole lainkaan omia sensoreita tai ohjattavia laitteita, vaan sen toiminta perustuu muiden valmistajien älykotikomponenttien hyödyntämiseen. Esimerkiksi nyt testattu aloituspaketti myytiin Telldusin, eli Proove AB:n, 433 MHz:n sensorien ja Nexan 433 MHz:n kauko-ohjattavien pistorasioiden kanssa (kuvassa 7). Cozify tukee 433 MHz:n verkkoa, Zigbeetä, 2,4 GHz:n WLANia ja Bluetoothia. Cozify tukee myös Z-wavea laitteiston osalta, mutta ohjelmiston puolelta tuki puuttuu, joten toistaiseksi Z-Wave ei Cozifylla vielä toimi. [34.]

Kuva 7. Cozify Hub, kauko-ohjattava pistorasia ja Telldus-lämpö- ja kosteusmittari.

Kuten muutkin testatut ratkaisut, Cozify liitettiin vain lähiverkkoon, ja sähkön kytkemisen jälkeen ei tarvinnut kuin asentaa sopiva mobiilisovellus. Muista testatuista järjestelmistä poiketen Cozifylla ei ole lainkaan web-sivuilla tai tietokoneella toimivaa ohjausta, vaan kaikki toiminnot tehdään mobiilisovelluksen kautta (kuvassa 8). Sovelluksen kielivalikoima on varsin suppea: Valittavana on suomi ja englanti. Toki suomenkielisen kuluttajan kannalta on hienoa, että käyttöliittymä on saatavilla suomeksi, mutta edes Suomen markkinoita ajatellen, olisi ruotsi, venäjä ja viro hyviä lisiä kielivalikoimaan.



Kuva 8. Cozifyn mobiilisovelluksen käyttöliittymä.

Cozifyn tuettujen laitteiden lista on varsin laaja, ja siihen saa liitettyä esimerkiksi Ikean älylamppuja ja ONVIF-rajapintaa tukevia IP-kameroita. Ensisijaisesti Cozify on rakennettu Zigbeen, ympärille ja uusia laitteita lisättäessä se etsii ensin nimenomaan Zigbee-laitteita ympäristöstään. 433 MHz:n tuki on myös kaksisuuntainen, toisin kuin testatussa Telldusin laitteessa, mutta Z-Wave-tuen puute rajaa tuettujen laitteiden määrää merkittävästi. Cozify on foorumeillaan lupaillut käyttäjille Z-Wave-tukea jo usean vuoden ajan [35], mutta tätä kirjoitettaessa tuki vielä puuttuu. Cozify osaa tosin hyödyntää olemassa olevaa WLAN-verkkoa kilpailijoitaan paremmin, esimerkiksi niin, että älypuhelimen läsnäolosta verkon alueella voidaan päätellä, onko käyttäjä kotona. Näin älypuhelin toimii itse sensorina, eikä erillistä mukana kannettavaa sensoria tarvita. Käytännön testit kuitenkin osoittivat, että tunnistus toimii melko heikosti.

Kuten muutkin testatut laitteet, Cozify kierrättää kaiken liikenteen palvelimen kautta, mutta tietoliikennekuormitusta Cozify aiheuttaa muita testattuja laitteita enemmän. Ollessaan käyttämättömänä, liikennekaappausten perusteella, Cozifyn kontrolleri ottaa lyhyen (alle sekunnin mittaisen) yhteyden palvelimeen puolen minuutin välein. Tästä ei aiheudu vielä suurta kuormitusta, mutta jostain syystä Cozify skannaa koko lähiverkon noin 90 sekunnin välein lähettämällä ARP-kyselyn jokaista aliverkon IP-osoitetta kohti. ARP-kyselyt ovat yleislähetyksinä koko aliverkkoon lähetettäviä viestejä, joilla laitteet selvittävät, millä fyysisellä laitteella on jokin tietty IP-osoite. ARP-kyselyt ovat osa normaalia IP-verkon toimintaa, mutta ei ole normaalia tutkia koko verkon laitekantaa jatkuvasti. Tällaisia koko verkon kartoituksia voisi kuvitella näkevänsä, jos käyttäjä on lisäämässä uutta laitetta kontrolleriin, mutta kaappaus tehtiin tilanteessa, jossa verkko oli stabiili eikä mitään laitteita edes käytetty.

Kun otetaan huomioon mainitut ARP-kyselyt, aiheuttaa Cozify verkkoon kuormitusta 4 647 bittiä sekunnissa [liite 3]. Tämä ei kuitenkaan ole koko totuus, koska ARP-kyselyt ovat yleislähetyksiä ja aiheuttavat kuormaa koko aliverkolle, minkä lisäksi laitteiden vastaukset kyselyihin aiheuttavat lisäkuormitusta. Testiverkossa oli kontrollerin lisäksi vain kaksi laitetta, joilla oli IP-osoite, joten vastauksia ei kaappauksessa näy juuri lainkaan. Liikennekaappausten mukaan kontrolleri lähettää noin 50 ARP-kyselyä sekunnissa. Tämä on vielä niin pieni määrä paketteja, ettei sen itsenäisesti pitäisi saada verkkoa jumiin, mutta se on kuitenkin turhaa liikennettä, jonka kaikki verkon laitteet joutuvat käsittelemään. Cozify ei ole vastannut kysymyksiini ARP-kyselyjen tarkoituksesta.

Tietosuoja on Cozifylla kohtuullisen hyvällä mallilla. Liikenne mobiilisovelluksesta palvelimeen ja palvelimelta kontrolleriin on TLS-salattu. Langattomien laitteiden salaus riippuu täysin käytetyistä laitteista. Cozifyn tapauksessa salaus on saatavilla vain Zigbee-laitteille, kun Z-Wavea ei tueta lainkaan ja 433 MHz on luonnostaan salaamaton. Porttiskannauksessa Cozifysta löytyi vain kaksi avointa porttia: UDP-portit 123 ja 5353. UDP-porttia 123 käyttää NTP-palvelin ja porttia 5353 käyttää Multicast DNS -palvelu. Multicast DNS -palveluun pohjautuu muun muassa Bonjour-protokolla, jolla Applen valmistamat laitteet löytävät toisensa ja tämä portti onkin todennäköisesti auki Applen tuotteiden tukemiseksi. Minulle ei selvinnyt miksi kontrollerissa on NTP-palvelinportti auki, eikä Cozify ole vastannut asiaa koskeviin kysymyksiini.

Cozify kertoo kotisivuillaan käyttävänsä Amazonin pilvipalvelimia, joissa tietoja säilytetään salattuna, ja että Amazonin palvelimet sekä yrityksen omat toiminnot ovat kolmannen osapuolen auditoimia [36]. Tietoturvasta mainittakoon lisäksi, että Cozify oli ainoa testatuista ratkaisuista, joka ei rekisteröitäessä kysynyt käyttäjän nimeä tai osoitetietoja. Tämä onkin pian voimaan astuvan GDPR-direktiivin mukaista, sillä käyttäjänimi tai osoite ovat turhaan kerättyjä tietoja suhteessa tarjottuun palveluun [37].

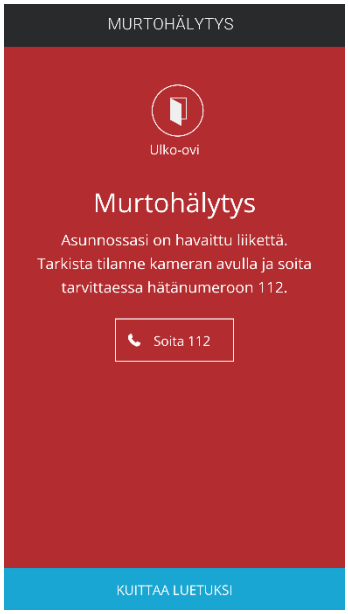
4 Testattujen ratkaisujen vertailu

4.1 Käyttökokemus

Kaikki testatut älykotijärjestelmät olivat helppokäyttöisiä, ja kaikkien järjestelmien käyttöönottaminen oli intuitiivista. Kaikkia tuotteita pystyi käyttämään englanniksi, mutta kokonaan suomen kielellä pystyi käyttämään ainoastaan Cozifya. Uusien laitteiden lisääminen oli kaikissa järjestelmissä helppoa, kuten myös ehtopohjaisten logiikoiden tekeminen. Kaikilla järjestelmillä onnistuivat aikapohjaiset säännöt, auringon nousu- ja laskuaikoihin pohjautuvat säännöt ja muiden laitteiden tilaan pohjautuvat säännöt. Siinä, miten järjestelmät lähettävät hälytyksiä käyttäjälle, on kuitenkin eroja. Kaikki järjestelmät osasivat lähettää hälytyksen omaan mobiilisovellukseensa ja lähettää sähköpostia. Telldus ja Cozify osasivat tämän lisäksi lähettää hälytyksen tekstiviestillä, joskin Telldusissa tämä oli maksullisen tilauksen vaativa ominaisuus. Lisäksi Cozify tarjoaa maksullisena palveluna mahdollisuutta tallentaa IP-kameran kuvaa palvelimelle, kun taas muut valmistajat eivät tätä toimintoa tarjonneet missään muodossa.

Kaikissa asioissa, joita järjestelmien käski tehdä, oli selkeä viive, arviolta aina sekunnin tai kaksi. Viive syntyy siitä, että tietoliikenne kiertää pilvipalvelimen kautta eikä mene suoraan kontrollerille. Älykotiratkaisujen hyödyllisyyden arviointi on subjektiivista. Itse pidin varsin hyödyllisenä esimerkiksi mahdollisuutta kukkalampun ajastamiseen kellonajan mukaan tai valon sytyttämistä liiketunnistimen perusteella. Kumpaankin käyttöön on saatavilla lukuisia muita ratkaisuja, jotka ovat huomattavasti yksinkertaisempia. Valoja on helpompi sytyttää tavallisesta katkaisijasta, eikä siinä ole viivettä kuten älykotiratkaisun kautta sytyttäessä. Vahvimmillaan älykotiratkaisut ovatkin kulunvalvonnassa ja kiinteistöautomaation ohjaamisessa.

Kaikilla testatuilla paketeilla sai hälytykset ulko-oven avauksesta, kun asukkaat eivät ole kotona, mutta yksikään ei toiminut ongelmitta. Kuvankaappaus Cozifyn mobiilisovellukseen saapuvasta hälytyksestä on alla. Sen:se ja Telldus eivät lähettäneet hälytystä joka avauksesta, kun taas Cozifylla oli vaikeuksia tunnistaa, milloin asukas on kotona eli milloin hälytyksen pitäisi olla päällä. Telldusin ongelmien epäilen johtuvan käytetystä Z-Wave-ovisensorista, jolla on lyhyempi kantama kuin Cozifyssa käytetyllä 433 MHz:n sensorilla, mutta koska testissä ollut Telldusin kontrolleri ei tukenut 433 MHz:n vastaanottoa, en voinut testata teoriaani tarkemmin.



Kuva 9. Cozifyn hälytys ulko-oven avauksesta.

Järjestelmien tukemien laitteiden määrä oli erittäin laaja, lukuun ottamatta Sen.seä, joka ei tue kuin omia laitteitaan. Positiivisia yllätyksiä olivat Telldusin tuki Clas Ohlsonin

halvoille kauko-ohjattaville pistorasioille ja Cozifyn tuki ONVIF-kameroille sekä Ikean älyvaloille. Yksikään ratkaisu ei kuitenkaan tukenut kaikkia tekniikoita samanaikaisesti.

4.2 Tietoliikenne ja tietoturva

Puhtaasti tietoliikenteen tehokkuuden kannalta Telldusin järjestelmä oli järkevimmin toteutettu ja aiheutti vähiten liikennettä. Minkään testatun järjestelmän tietoliikennemäärät eivät olleet erityisen suuria nykymittapuulla, mutta erot olivat isoja: Cozifyn liikennemäärät olivat jopa 60-kertaiset Telldusin ratkaisuun nähden [liite 2 ja liite 3].

Kaikki testatut järjestelmät kierrättävät kaiken liikenteen palvelimen kautta. Tämä on käyttäjälle helppoa, kun laitteita voi sen ansiosta myös ohjata mistä päin maailmaa tahansa. Kääntöpuolena mikään testatuista järjestelmistä ei toimi ilman internetyhteyttä, ei edes paikallisesti. Internetyhteydestä riippuvaisuus on järjestelmien pahin kompastuskivi, ja jos jonkin testatuista järjestelmistä ottaisi käyttöön kulunvalvontaan, tulisi internetyhteys kahdentaa. Samalla voidaan kyseenalaistaa, kannattaako vantaalaisen kerrostalokaksion valojen sytytystä kierrättää Frankfurtissa olevan palvelinsalin kautta.

Tietoturvallisen älykotiratkaisun rakentaminen on hyvin haasteellista. Pelkästään varmistuakseen siitä, että laitteiden ja kontrollerin välinen ilmatie on salattu, täytyy kuluttajan ensin selvittää, mitkä tekniikat ovat tietoturvallisia ja mitä tekniikoita ratkaisu tukee, ja sen jälkeen tulee vielä varmistaa, että käytetyt komponentit myös tukevat salausta. Jos haluaa varmistaa, että älykodin ilmatie on salattu eikä siinä ole merkittäviä haavoittuvaisuuksia, tulisi käyttää vain Z-Wave Secure tai Zigbee 3.0 -sertifioituja tuotteita. Käyttötesteissä sensoreista luotettavimmiksi osoittautuivat kuitenkin 433 MHz:n taajuudella toimivat laitteet, joissa ei siis ole salausta lainkaan. Tässä, kuten niin monessa muussakin tapauksessa, joudutaan tekemään kompromisseja käytettävyyden ja tietoturvan välillä.

Salatun ilmatien lisäksi tulisi varmistaa, että yhteys kontrollerista palvelimeen on suojattu ja että laitteissa ei ole avoimia portteja. Näihin seikkoihin ei ole mitään yhteistä toteutustapaa, ja toisin kuin ilmatien suojaamisen suhteen, kuluttaja joutuu luottamaan älykotiratkaisun valmistajan omaan suunnitteluun. Nyt testatuista ratkaisuista palvelimen ja kontrollerin välinen salaus oli kunnossa Telldusin ja Cozifyn ratkaisuissa, Sen:se oli täysin salaamaton. Vaikka salaus olikin kunnossa Telldusilla ja Cozifylla, kummastakin laitteesta löytyi turhaan avoimena olevia portteja.

Teknisen toteutuksen tietoturvan lisäksi on hyvä miettiä, mitä tietoa järjestelmät keräävät ja miksi. Kaikki järjestelmät vaativat käyttäjää rekisteröitymään, ja sekä Sen.sen että Telldusin palveluihin rekisteröityessä piti antaa täysi nimi, vaikkei siihen ollut mitään käytännön tarvetta. Cozifylle riitti henkilökohtaisiksi tiedoiksi pelkkä sähköpostiosoite. Valmistajat eivät anna myöskään tietoa siitä, mitä tietoa käyttäjästä tallennetaan, kuinka yksityiskohtaisesti ja kuinka pitkältä ajalta. Valmistajahan tietäisi esimerkiksi, milloin asukkaat tulevat ja menevät, milloin laitteita käytetään ja mitkä ovat järjestelmään liitettyjen laitteiden (esimerkiksi IP-kameroiden) salasanat. Valitettavasti näistä älykotiratkaisuista puhuttaessa pitääkin unohtaa odotukset yksityisyydestä.

4.3 Älykotiratkaisun hankkiminen

Kun miettii, minkä älykotiratkaisun hankkii, on tietoturva-asioiden lisäksi huomioitava ratkaisun laajennettavuus, ratkaisun helppokäyttöisyys (johon liittyy kielituki), sen miten paljon ratkaisu rasittaa muuta verkkoa ja mitä se maksaa. Taulukossa 1 on eriteltynä eri ratkaisujen tärkeimmät ominaisuudet ja niiden hinnat.

Taulukko 1: Älykotipakettien vertailu.

	Sen.se Mother	**Telldus** ZNet Lite v1	**Cozify** Cozify Hub 1.1
Tuetut tekniikat laitteiden ja sensorien yhdistämiseen	868 MHz	Z-Wave Plus ja 433 MHz (vain lähetys)	Zigbee, 433 MHz, Bluetooth ja WLAN
Kontrollerin ja laitteiden/sensorien välisen liikenteen salaus	Salaamaton	Osittainen[1]	Osittainen[1]
Palvelimen ja kontrollerin välisen liikenteen salaus	Salaamaton	TLS	TLS
Mobiilisovelluksen ja palvelimen välisen liikenteen salaus	TLS	TLS	TLS
Kontrollerin aiheuttama tietoliikennekuorma, kun verkko on muutokseton	287 b/s	76 b/s	4 647 b/s
Tuettujen laitteiden valikoima	Suppea (Sen.sen omat)	Laaja	Laaja
Kielituki	Englanti, ranska, saksa ja kiina.	Suomi, ruotsi, englanti, ranska, puola, tsekki, tanska, turkki, norja ja saksa.[2]	Suomi ja englanti.
Aloituspaketin hinta (kontrolleri ja 3–4 laitetta/sensoria)	99 € [3]	145 € [3]	276 € [4]

1) AES128-salaus on saatavilla vain salausta tukevissa laitteissa ja sensoreissa.
2) Monet käännökset ovat puutteellisia.
3) Hintatiedot valmistajan omilta sivuilta.
4) Verkkokauppa.comin oma paketti Telldusin sensoreilla. Verkkokauppa.comin hinta.

Taulukkomuodossa tietoja tarkastellessa näyttäisi Telldus tarjoavan rahalle eniten vastinetta. Tämä vastaa myös henkilökohtaista käyttökokemustani, jonka mukaan Telldus tuntui kaikkein tasapainoisimmalta ratkaisulta. Jos huomaa Telldusilta hankkia uudemman version kontrollerista (ZNet Lite v2), saa 433 MHz:lle myös vastaanoton tuen. Cozifyn paketti oli myös monipuolinen, mutta sen hinta on mielestäni liian korkea laitteen ominaisuuksiin nähden tällä hetkellä (Z-Wave-tuen vielä puuttuessa).

Älykodin hankkija saa olla varovainen laitteita ostaessaan, ja onkin suositeltavaa tarkistaa tarkat tuotetiedot valmistajan sivuilta ennen hankintaa. Kaikissa testatuissa tuotteissa oli harhaanjohtavia tai puutteellisia tietoja, eivätkä alan standarditkaan aina takaa haluttua toimintoa. Havaitsin testien aikana seuraavia ongelmia ja virheitä:

- Telldus väitti laitteensa tukevan 433 MHz:n taajuutta, vaikka tuki olikin tässä mallissa vain yksisuuntainen.

- Cozify mainostaa ”rautansa” tukevan Z-Wavea, vaikka ohjelmistotuki puuttui ja tukea ei siis käytännössä ole.

- Sen.se ei kerro tuotteistaan juuri mitään teknisiä tietoja.

- Z-Wave Plus -standardiin kuuluu tuki AES128-salaukselle, mutta salaus on valinnainen ominaisuus. Z-Wave Plus -logo paketissa ei takaa, että laitteen saa salattua. Z-Wave Secure -logo kertoisi salauksen saatavuudesta, mutta testissä olleista tuotepaketeista logo puuttui, vaikka salaus olikin saatavilla.

- Joistain tuotteista standardien logot puuttuvat, vaikka ne standardeja tukevatkin. Esimerkiksi Ikean älyvalotuotteet käyttävät Zigbee-standardia, mutta niissä ei ole lainkaan Zigbee-logoa.

Näiden seikkojen vuoksi, on kuluttajan itse selvitettävä laitteiden ominaisuudet ennen hankintaa. Nykytilanteessa kuluttaja ei voi olla varma, mitä saa, vaikka tuntisikin alan standardit ja logot. Tilannetta pahentaa se, että esimerkiksi näiden ratkaisujen valmistajien kotisivuilla keskitytään lähinnä mainostamaan, mitä laitteilla voi tehdä, mutta tekniset tiedot ovat vaikeasti saatavilla, jos ollenkaan, ja mahdollisesti kielellä, jota kuluttaja ei ymmärrä.

5 Yhteenveto

Insinöörityön tavoitteena oli selvittää, sopivatko älykotiratkaisut kuluttajakäyttöön ja mitä tietoturvaongelmia laitteissa esiintyy. Työssä testattiin kolmen eri valmistajan ratkaisuja. Testeissä kontrollereiden tietoliikenne kaapattiin ja analysoitiin, minkä lisäksi kontrollerista etsittiin avoimia portteja. Testien tarkoitus oli tutkia laitteiden tietoliikenteestä kuluttajalle näkymätöntä osaa, joka ei ole alan yleisten standardien alainen. Testeissä paljastui suuria eroja eri valmistajien toteutusten väliltä, mikä korostaa valmistajan roolia tietoturvallisen älykodin luomisessa.

Työssä kävi selväksi, että vaikka laitteet ovat kuluttajakaupassa saatavilla, on kuluttajilla edessään epämääräisten standardien viidakko ja valmistajien omat laitetoteutukset, joissa osa toteutuksista on melko kyseenalaisia. Vaikka älykotiratkaisut ovat helppokäyttöisiä tekniikkaan orientoitumattomallekin kuluttajalle, on tietoturvallisen älykotiratkaisun rakentaminen erittäin haasteellista, ellei lähes mahdotonta. Kaikissa testatuissa ratkaisuissa oli joitain ongelmia tietoturvan kanssa, eikä yksikään toiminut ilman jatkuvaa internetyhteyttä.

Standardit, kuten Z-Wave ja Zigbee, määrittelevät, miten ilmatietä käytetään, mutta siitä eteenpäin kuluttaja on valmistajan toteutuksen varassa. Standarditkaan eivät takaa sitä, että tietoturva olisi kunnossa, koska salaus ei välttämättä ole käytössä kaikissa standardia käyttävissä laitteissa. Älykodin perustajan täytyy myös hyväksyä se, että perustoiminnot, kuten valojen sytyttäminen ja sammuttaminen, muuttuvat hitaammaksi ja tältä osin älykoti hankaloittaa elämää eikä helpota sitä. Kuluttajan kannattaakin miettiä ennen järjestelmän hankkimista, mitä kaikkea haluaa automatisoida. Nämä älykotiratkaisut toimivat sitä paremmin, mitä monimutkaisempia kokonaisuuksia niistä rakennetaan; parin lampun takia ei kannata älykotia rakentaa.

Lähteet

1 Frequently asked questions. 2015. Verkkoaineisto. International Telecommunication Union. <www.itu.int/net/ITU-R/terrestrial/faq/index.html>. Luettu 7.3.2018.

2 Määräys luvasta vapaiden radiolähettimien yhteistaajuuksista ja käytöstä. 2018. Verkkoaineisto. Viestintävirasto. <www.viestintavirasto.fi/attachments/maarayk-set/Maarays_15AM.pdf>. Luettu 12.3.2018.

3 Tuetut laitteet ja radiot. 2018. Verkkoaineisto. Cozify Oy. <tuki.cozify.fi/sup-port/solutions/articles/8000033969-tuetut-laitteet-ja-radiot#supportedDevices>. Luettu 12.3.2018.

4 Sigma Designs Buying Smart Network Chipmaker Zensys. 2008. Verkkoaineisto. Gigaom. <gigaom.com/2008/12/18/sigma-designs-buying-smart-network-chip-maker-zensys>. Luettu 7.3.2018.

5 Safer, Smarter Homes Start with Z-Wave. 2018. Verkkoaineisto. Sigma Designs, Inc. <z-wave.com/about>. Luettu 7.3.2018.

6 Z-Wave Frequency Coverage. 2018. Verkkoaineisto. Sigma Designs, Inc. <z-wave.sigmadesigns.com/wp-content/uploads/Z-Wave_Frequency_Cover-age_180221.pdf>. Luettu 7.3.2018.

7 Z-Wave Smart Home Products FAQ. 2018. Verkkoaineisto. Sigma Designs, Inc. <www.z-wave.com/faq>. Luettu 7.3.2018.

8 Z-Wave Public Specification. 2018. Verkkoaineisto. Sigma Designs, Inc. <z-wave.sigmadesigns.com/design-z-wave/z-wave-public-specification/>. Luettu 12.3.2018.

9 T-REC-G.9959. 2015. Verkkoaineisto. International Telecommunication Union. <www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.9959-201501-I!!PDF-E&type=items>. Luettu 12.3.2018.

10 Sigma Designs Releases Z-Wave Interoperability Layer Into the Public Domain. 2016. Verkkoaineisto. Sigma Designs, Inc. <www.sigmade-signs.com/news/sigma-designs-releases-z-wave-interoperability-layer-into-the-public-domain/>. Luettu 12.3.2018.

11 Understanding Z-Wave Networks, Nodes & Devices. 2012. Verkkoaineisto. Ves-ternet Ltd. <www.vesternet.com/resources/technology-indepth/understanding-z-wave-networks>. Luettu 12.3.2018.

12 Z-Wave networking basics. 2016. Verkkoaineisto. Sigma Designs, Inc. <zwave-public.com/sites/default/files/APL13031-2%20-%20Z-Wave%20Network-ing%20Basics.pdf>. Luettu 12.3.2018.

13 Z-Wave Plus Role Type Specification. 2018. Verkkoaineisto. Sigma Designs, Inc. <zwavepublic.com/sites/default/files/command_class_specs_2017A/SDS11846-20%20Z-Wave%20Plus%20Role%20Type%20Specification.pdf>. Luettu 12.3.2018.

14 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. 2016. Verkkoaineisto. The Institute of Electrical and Electronics Engineers, Inc. <ieeexplore.ieee.org/document/7786995/>. Luettu 12.3.2018.

15 Shmoocon 2016: Z-Wave Protocol Hacked with SDR. 2016. Verkkoaineisto. <hackaday.com/2016/01/16/shmoocon-2016-z-wave-protocol-hacked-with-sdr/>. Luettu 12.3.2018.

16 Join the Zigbee Alliance and shape the future of the Internet of Things. 2018. Verkkoaineisto. Zigbee Alliance. <www.zigbee.org>. Luettu 12.3.2018.

17 IEEE 802.15.4-2015 - IEEE Standard for Low-Rate Wireless Networks. 2016. Verkkoaineisto. The Institute of Electrical and Electronics Engineers, Inc. <ieeexplore.ieee.org/document/7460875/>. Luettu 12.3.2018.

18 Zigbee 3.0. 2018. Verkkoaineisto. Zigbee Alliance.<www.zigbee.org/zigbee-for-developers/zigbee-3-0/>. Luettu: 12.3.2018.

19 What Is zigbee 3.0. 2017. Verkkoaineisto. Silicon Laboratories. <www.silabs.com/community/wireless/zigbee-and-thread/knowledge-base.entry.html/2017/06/15/what_is_zigbee_30-tCs4>. Luettu 12.3.2018.

20 802.15.4v-2017 - IEEE Standard for Low-Rate Wireless Networks - Amendment 5: Enabling/Updating the Use of Regional Sub-GHz Bands. 2017. Verkkoaineisto. The Institute of Electrical and Electronics Engineers, Inc. <eeexplore.ieee.org/document/7964803/>. Luettu 12.3.2018.

21 ECC Decision (04)06. 2004-2011. Verkkoaineisto. Electronic Communications Comitee. <erodocdb.dk/Docs/doc98/official/pdf/ECCDEC0406.PDF>. Luettu 12.3.2018.

22 Z-Wave and LightwaveRF Range Test. 2013. Verkkoaineisto. Vesternet Ltd. <www.vesternet.com/blog/testing-device-ranges/>. Luettu 14.3.2018.

23 Range test with Zigbee in indoor environments. 2006. Verkkoaineisto. IFAC Programmable Devices and Embedded Systems. <www.sciencedirect.com/science/article/pii/S1474667017302288/pdf?md5=84911597d56ea0ced7dad89e8b5ed228&pid=1-s2.0-S1474667017302288-main.pdf>. Luettu 14.3.2018.

24 Researchers find major security flaw with ZigBee smart home devices. 2015. Verkkoaineisto. Oath Tech Network Aol Tech. <www.engadget.com/2015/08/07/zigbee-security-flaw/>. Luettu 14.3.2018.

25 Zillner, Tobias. 2015. Zigbee exploited - The good, the bad and the ugly. Verkkoaineisto. <www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly.pdf>. Luettu 14.3.2018.

26 zigbee: Securing the Wireless IoT. 2017. Verkkoaineisto. Zigbee Alliance. <www.zigbee.org/zigbeealliance/white-papers/>. Luettu: 14.3.2018.

27 Z-Wave Products. 2018. Verkkoaineisto. Z-Wave Alliance. <products.z-wavealliance.org>. Luettu 22.3.2018.

28 ZigBee Certified Products. 2018. Verkkoaineisto. Zigbee Alliance. <www.zigbee.org/zigbee-products-2/#zigbeecertifiedproducts/>. Luettu 22.3.2018.

29 Terms and conditions. 2018. Verkkoaineisto. Sen.se. <sen.se/store/conditions/>. Luettu 22.3.2018.

30 Gullberg, Fredrik. 2018. Telldusin tukipalvelut. Sähköpostikirjeenvaihto 28.3.2018.

31 e-shop Telldus Smart Homes. 2018. Verkkoaineisto. Proove Ab. <telldus.com/webshop/>. Luettu 29.3.2018.

32 TellStick Net protocol. 2018. Verkkoaineisto. Proove Ab. <developer.telldus.com/doxygen/html/TellStickNet.html>. Luettu 5.4.2018.

33 Cozify. 2018. Verkkoaineisto. Cozify Oy. <www.cozify.fi>. Luettu 5.4.2018.

34 Tuetut laitteet ja radiot. 2018. Verkkoaineisto. Cozify Oy. <tuki.cozify.fi/support/solutions/articles/8000033969-tuetut-laitteet-ja-radiot#includedRadios>. Luettu 5.4.2018.

35 Cozifyn kehityksen eteneminen. 2017. Verkkoaineisto. Cozify Oy – Käyttäjäfoorumi. <forum.cozify.fi/discussion/471/cozifyn-kehityksen-eteneminen>. Luettu 5.4.2018.

36 Kuinka tietoturva on otettu huomioon? 2018. Verkkoaineisto. Cozify Oy. <tuki.cozify.fi/support/solutions/articles/8000033970-usein-kysytyt-kysymykset#faq-security>. Luettu 5.4.2018.

37 EU:n tietosuojauudistus. 2018. Verkkoaineisto. Tietosuojavaltuutetun toimisto. <www.tietosuoja.fi/fi/index/euntietosuojauudistus.html>. Luettu 8.4.2018.

38 Viestintäviraston varoitus 04/2016. 2016. Verkkoaineisto. Viestintävirasto. <www.viestintavirasto.fi/kyberturvallisuus/varoitukset/2016/varoitus-2016-04.html>. Luettu 20.4.2018.

39 Telldus Live. 2018. Verkkoaineisto. Proove Ab. <live.telldus.com>. Luettu 14.3.2018.

Sen.sen liikennekaappaus

Taulukossa on Wireshark-ohjelmalla tehty liikennekaappaus Sen.sen kontrollerin ja palvelimen välisestä liikenteestä 3 minuutin ajalta, kun järjestelmässä ja ympäristössä ei tapahdu muutoksia.

172.21.42.101 on kontrolleri. TCP Keep Alive -paketit korostettuina.

Taulukossa käytetty Wireshark-suodatin:
frame.time_relative <= 180 and (arp.src.proto_ipv4 == 172.21.42.101 or ip.addr == 172.21.42.101)

Time	Source	Destination	Protocol	Length	Info
0.000000	172.21.42.101	144.76.166.244	TCP	60	1251 > 80 [ACK] Seq=1 Ack=1 Win=4000 Len=1
0.049188	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [ACK] Seq=1 Ack=2 Win=65535 Len=0
2.143400	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [PSH, ACK] Seq=1 Ack=2 Win=65535 Len=3
2.145037	172.21.42.101	144.76.166.244	TCP	60	1251 > 80 [ACK] Seq=2 Ack=4 Win=4000 Len=0
4.037108	172.21.42.101	144.76.166.244	TCP	188	1251 > 80 [PSH, ACK] Seq=2 Ack=4 Win=4000 Len=134
4.087367	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [ACK] Seq=4 Ack=136 Win=65535 Len=0
14.087575	172.21.42.101	144.76.166.244	TCP	60	[TCP Keep-Alive] 1251 > 80 [ACK] Seq=135 Ack=4 Win=4000 Len=1
14.136645	144.76.166.244	172.21.42.101	TCP	60	[TCP Keep-Alive ACK] 80 > 1251 [ACK] Seq=4 Ack=136 Win=65535 Len=0
22.144019	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [PSH, ACK] Seq=4 Ack=136 Win=65535 Len=3
22.145704	172.21.42.101	144.76.166.244	TCP	60	1251 > 80 [ACK] Seq=136 Ack=7 Win=4000 Len=0
32.144102	172.21.42.101	144.76.166.244	TCP	60	[TCP Keep-Alive] 1251 > 80 [ACK] Seq=135 Ack=7 Win=4000 Len=1
32.192975	144.76.166.244	172.21.42.101	TCP	60	[TCP Keep-Alive ACK] 80 > 1251 [ACK] Seq=7 Ack=136 Win=65535 Len=0
35.953866	172.21.42.101	144.76.166.244	TCP	227	1251 > 80 [PSH, ACK] Seq=136 Ack=7 Win=4000 Len=173
36.003434	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [ACK] Seq=7 Ack=309 Win=65535 Len=0
41.958702	172.21.42.101	144.76.166.244	TCP	227	1251 > 80 [PSH, ACK] Seq=309 Ack=7 Win=4000 Len=173
41.975219	172.21.42.101	144.76.166.244	TCP	227	1251 > 80 [PSH, ACK] Seq=482 Ack=7 Win=4000 Len=173
42.007782	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [ACK] Seq=7 Ack=482 Win=65535 Len=0
42.024981	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [ACK] Seq=7 Ack=655 Win=65535 Len=0
42.143375	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [PSH, ACK] Seq=7 Ack=655 Win=65535 Len=3
42.145050	172.21.42.101	144.76.166.244	TCP	60	1251 > 80 [ACK] Seq=655 Ack=10 Win=4000 Len=0
51.961281	172.21.42.101	144.76.166.244	TCP	227	1251 > 80 [PSH, ACK] Seq=655 Ack=10 Win=4000 Len=173
52.011109	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [ACK] Seq=10 Ack=828 Win=65535 Len=0
62.011320	172.21.42.101	144.76.166.244	TCP	60	[TCP Keep-Alive] 1251 > 80 [ACK] Seq=827 Ack=10 Win=4000 Len=1
62.060450	144.76.166.244	172.21.42.101	TCP	60	[TCP Keep-Alive ACK] 80 > 1251 [ACK] Seq=10 Ack=828 Win=65535 Len=0
62.144029	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [PSH, ACK] Seq=10 Ack=828 Win=65535 Len=3
62.145706	172.21.42.101	144.76.166.244	TCP	60	1251 > 80 [ACK] Seq=828 Ack=13 Win=4000 Len=0
64.037830	172.21.42.101	144.76.166.244	TCP	188	1251 > 80 [PSH, ACK] Seq=828 Ack=13 Win=4000 Len=134
64.087489	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [ACK] Seq=13 Ack=962 Win=65535 Len=0
74.087857	172.21.42.101	144.76.166.244	TCP	60	[TCP Keep-Alive] 1251 > 80 [ACK] Seq=961 Ack=13 Win=4000 Len=1
74.136563	144.76.166.244	172.21.42.101	TCP	60	[TCP Keep-Alive ACK] 80 > 1251 [ACK] Seq=13 Ack=962 Win=65535 Len=0
82.143394	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [PSH, ACK] Seq=13 Ack=962 Win=65535 Len=3
82.145091	172.21.42.101	144.76.166.244	TCP	60	1251 > 80 [ACK] Seq=962 Ack=16 Win=4000 Len=0
92.143621	172.21.42.101	144.76.166.244	TCP	60	[TCP Keep-Alive] 1251 > 80 [ACK] Seq=961 Ack=16 Win=4000 Len=1

92.192665	144.76.166.244	172.21.42.101	TCP	60	[TCP Keep-Alive ACK] 80 > 1251 [ACK] Seq=16 Ack=962 Win=65535 Len=0
94.041881	172.21.42.101	144.76.166.244	TCP	201	1251 > 80 [PSH, ACK] Seq=962 Ack=16 Win=4000 Len=147
94.091202	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [ACK] Seq=16 Ack=1109 Win=65535 Len=0
97.965128	172.21.42.101	144.76.166.244	TCP	227	1251 > 80 [PSH, ACK] Seq=1109 Ack=16 Win=4000 Len=173
98.014341	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [ACK] Seq=16 Ack=1282 Win=65535 Len=0
102.143639	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [PSH, ACK] Seq=16 Ack=1282 Win=65535 Len=3
102.145300	172.21.42.101	144.76.166.244	TCP	60	1251 > 80 [ACK] Seq=1282 Ack=19 Win=4000 Len=0
103.969948	172.21.42.101	144.76.166.244	TCP	227	1251 > 80 [PSH, ACK] Seq=1282 Ack=19 Win=4000 Len=173
103.986470	172.21.42.101	144.76.166.244	TCP	227	1251 > 80 [PSH, ACK] Seq=1455 Ack=19 Win=4000 Len=173
104.019895	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [ACK] Seq=19 Ack=1455 Win=65535 Len=0
104.036658	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [ACK] Seq=19 Ack=1628 Win=65535 Len=0
113.972533	172.21.42.101	144.76.166.244	TCP	227	1251 > 80 [PSH, ACK] Seq=1628 Ack=19 Win=4000 Len=173
114.022410	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [ACK] Seq=19 Ack=1801 Win=65535 Len=0
122.144146	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [PSH, ACK] Seq=19 Ack=1801 Win=65535 Len=3
122.145859	172.21.42.101	144.76.166.244	TCP	60	1251 > 80 [ACK] Seq=1801 Ack=22 Win=4000 Len=0
124.038797	172.21.42.101	144.76.166.244	TCP	188	1251 > 80 [PSH, ACK] Seq=1801 Ack=22 Win=4000 Len=134
124.088499	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [ACK] Seq=22 Ack=1935 Win=65535 Len=0
134.088740	172.21.42.101	144.76.166.244	TCP	60	[TCP Keep-Alive] 1251 > 80 [ACK] Seq=1934 Ack=22 Win=4000 Len=1
134.137840	144.76.166.244	172.21.42.101	TCP	60	[TCP Keep-Alive ACK] 80 > 1251 [ACK] Seq=22 Ack=1935 Win=65535 Len=0
142.143618	144.76.166.244	172.21.42.101	TCP	60	80 > 1251 [PSH, ACK] Seq=22 Ack=1935 Win=65535 Len=3
142.145278	172.21.42.101	144.76.166.244	TCP	60	1251 > 80 [ACK] Seq=1935 Ack=25 Win=4000 Len=0
152.143813	172.21.42.101	144.76.166.244	TCP	60	[TCP Keep-Alive] 1251 > 80 [ACK] Seq=1934 Ack=25 Win=4000 Len=1
152.193088	144.76.166.244	172.21.42.101	TCP	60	[TCP Keep-Alive ACK] 80 > 1251 [ACK] Seq=25 Ack=1935 Win=65535 Len=0

Kaappauksen aikana TCP-keskustelussa siirretty tieto

Koska Sen.se ei käytä liikenteen salausta, voidaan TCP-keskustelu lukea liikennekaappauksesta.

...-...~....{"resource" : "events", "method" : "post", "body" : [{"timestamp" : "2018-03-22 08:54:29", "feed_type" : "1", "value" : "1"}]}..-........{"resource" : "events", "method" : "post", "body" : [{"node" : "02C7231E", "timestamp" : "2018-03-22 08:55:01", "feed_type" : "1", "signal" : "-76", "value" : "2"}]}........{"resource" : "events", "method" : "post", "body" : [{"node" : "02C6082C", "timestamp" : "2018-03-22 08:55:07", "feed_type" : "1", "signal" : "-31", "value" : "2"}]}........{"resource" : "events", "method" : "post", "body" : [{"node" : "02CD1A24", "timestamp" : "2018-03-22 08:55:07", "feed_type" : "1", "signal" : "-67", "value" : "2"}]}..-........{"resource" : "events", "method" : "post", "body" : [{"node" : "02CB2311", "timestamp" : "2018-03-22 08:55:17", "feed_type" : "1", "signal" : "-67", "value" : "2"}]}..-...~....{"resource" : "events", "method" : "post", "body" : [{"timestamp" : "2018-03-22 08:55:29", "feed_type" : "1", "value" : "1"}]}..-........{"resource" : "events", "method" : "post", "body" : [{"timestamp" : "2018-03-22 08:55:59", "feed_type" : "99", "value" : "Nb Cookie : 4"}]}........{"resource" : "events", "method" : "post", "body" : [{"node" : "02C7231E", "timestamp" : "2018-03-22 08:56:03", "feed_type" : "1", "signal" : "-76", "value" : "2"}]}..-........{"resource" : "events", "method" : "post", "body" : [{"node" : "02C6082C",

"timestamp" : "2018-03-22 08:56:09", "feed_type" : "1", "signal" : "-31", "value" : "2"}]}........{"resource" : "events", "method" : "post", "body" : [{"node" : "02CD1A24", "timestamp" : "2018-03-22 08:56:09", "feed_type" : "1", "signal" : "-67", "value" : "2"}]}........{"resource" : "events", "method" : "post", "body" : [{"node" : "02CB2311", "timestamp" : "2018-03-22 08:56:19", "feed_type" : "1", "signal" : "-69", "value" : "2"}]}..-...~....{"resource" : "events", "method" : "post", "body" : [{"timestamp" : "2018-03-22 08:56:29", "feed_type" : "1", "value" : "1"}]}..-

Sen.sen kaappauksen tilastot

Paketteja (kpl)	60
Pakettien aikaväli (s)	152,193
Paketteja sekunnissa, keskiarvo	0,4
Paketin koko, keskiarvo (B)	91,5
Tavuja	5461
Tavuja sekunnissa, keskiarvo	35
Bittejä sekunnissa, keskiarvo	287

Telldusin liikennekaappaus

Taulukossa on Wireshark-ohjelmalla tehty liikennekaappaus Telldusin kontrollerin ja palvelimen välisestä liikenteestä 3 minuutin ajalta, kun järjestelmässä ja ympäristössä ei tapahdu muutoksia.

172.21.42.101 on kontrolleri. ARP-paketit korostettuina. Ensimmäiseen 13,8 sekuntiin verkossa ei ole liikennettä, jonka lähde tai kohde Telldus olisi.

Taulukossa käytetty Wireshark-suodatin:
frame.time_relative <= 180 and (arp.src.proto_ipv4 == 172.21.42.101 or ip.addr == 172.21.42.101)

Time	Source	Destination	Protocol	Length	Info
13.846825	109.74.4.32	172.21.42.101	TCP	188	45000 > 43150 [PSH, ACK] Seq=1 Ack=1 Win=501 Len=122 TSval=2329533235 TSecr=426504
13.847056	172.21.42.101	109.74.4.32	TCP	66	43150 > 45000 [ACK] Seq=1 Ack=123 Win=7632 Len=0 TSval=438929 TSecr=2329533235
18.850049	TelldusT_01:53:e2	ZyxelCom_70:c3:be	ARP	60	172.21.42.101 is at ac:ca:54:01:53:e2
18.857361	172.21.42.101	109.74.4.32	TCP	188	43150 > 45000 [PSH, ACK] Seq=1 Ack=123 Win=7632 Len=122 TSval=439430 TSecr=2329533235
18.876445	109.74.4.32	172.21.42.101	TCP	66	45000 > 43150 [ACK] Seq=123 Ack=123 Win=501 Len=0 TSval=2329538265 TSecr=439430
23.864594	TelldusT_01:53:e2	ZyxelCom_70:c3:be	ARP	60	Who has 172.21.42.1? Tell 172.21.42.101
134.325234	109.74.4.32	172.21.42.101	TCP	188	45000 > 43150 [PSH, ACK] Seq=123 Ack=123 Win=501 Len=122 TSval=2329653713 TSecr=439430
134.325368	172.21.42.101	109.74.4.32	TCP	66	43150 > 45000 [ACK] Seq=123 Ack=245 Win=7632 Len=0 TSval=450977 TSecr=2329653713
139.330248	TelldusT_01:53:e2	ZyxelCom_70:c3:be	ARP	60	172.21.42.101 is at ac:ca:54:01:53:e2
139.337725	172.21.42.101	109.74.4.32	TCP	188	43150 > 45000 [PSH, ACK] Seq=123 Ack=245 Win=7632 Len=122 TSval=451478 TSecr=2329653713
139.357208	109.74.4.32	172.21.42.101	TCP	66	45000 > 43150 [ACK] Seq=245 Ack=245 Win=501 Len=0 TSval=2329658745 TSecr=451478
144.345052	TelldusT_01:53:e2	ZyxelCom_70:c3:be	ARP	60	Who has 172.21.42.1? Tell 172.21.42.101

Telldusin liikennekaappauksen tilastot

Paketteja (kpl)	12
Pakettien aikaväli (s)	130,498
Paketteja sekunnissa, keskiarvo	0,1
Paketin koko, keskiarvo (B)	104,5
Tavuja	1 256
Tavuja sekunnissa, keskiarvo	9
Bittejä sekunnissa, keskiarvo	76

Cozifyn liikennekaappaus

Taulukossa on Wireshark-ohjelmalla tehty liikennekaappaus Cozifyn kontrollerin ja palvelimen välisestä liikenteestä 3 minuutin ajalta, kun järjestelmässä ja ympäristössä ei tapahdu muutoksia.

172.21.42.103 on kontrolleri. ARP-paketit korostettuina. Kummankin punaisen viivan kohdalta on poistettu 500 ARP-pakettia.

Taulukossa käytetty Wireshark-suodatin:
frame.time_relative <= 180 and (arp.src.proto_ipv4 == 172.21.42.103 or ip.addr == 172.21.42.103)

Time	Source	Destination	Protocol	Length	Info
0.000000	172.21.42.103	54.77.86.190	TLSv1.2	280	Application Data
0.070594	54.77.86.190	172.21.42.103	TLSv1.2	178	Application Data
0.070921	172.21.42.103	54.77.86.190	TCP	66	52471 > 443 [ACK] Seq=215 Ack=113 Win=1288 Len=0 TSval=1030001 TSecr=887736370
1.455286	172.21.42.103	172.21.42.1	TCP	74	38020 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1030140 TSecr=0 WS=64
2.402585	172.21.42.103	239.255.255.250	UDP	69	57800 > 10000 Len=27
5.074413	TexasIns_e3:6c:31	ZyxelCom_70:c3:be	ARP	60	172.21.42.103 is at 90:70:65:e3:6c:31
28.552214	172.21.42.103	195.197.54.100	DNS	76	Standard query 0xa389 A cloud4.cozify.fi
28.552426	172.21.42.103	212.54.0.3	DNS	76	Standard query 0xa389 A cloud4.cozify.fi
28.552567	172.21.42.103	8.8.8.8	DNS	76	Standard query 0xa389 A cloud4.cozify.fi
28.566132	212.54.0.3	172.21.42.103	DNS	108	Standard query response 0xa389 A cloud4.cozify.fi A 52.51.145.109 A 34.243.221.45
28.566218	195.197.54.100	172.21.42.103	DNS	108	Standard query response 0xa389 A cloud4.cozify.fi A 34.243.221.45 A 52.51.145.109
28.582083	8.8.8.8	172.21.42.103	DNS	108	Standard query response 0xa389 A cloud4.cozify.fi A 52.51.145.109 A 34.243.221.45
28.582445	172.21.42.103	8.8.8.8	ICMP	136	Destination unreachable (Port unreachable)
28.589590	172.21.42.103	52.51.145.109	TCP	74	44412 > 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1032853 TSecr=0 WS=64
28.647733	52.51.145.109	172.21.42.103	TCP	74	443 > 44412 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=4126787643 TSecr=1032853 WS=256
28.648099	172.21.42.103	52.51.145.109	TCP	66	44412 > 443 [ACK] Seq=1 Ack=1 Win=29248 Len=0 TSval=1032859 TSecr=4126787643
28.773211	172.21.42.103	52.51.145.109	TLSv1.2	583	Client Hello
28.831273	52.51.145.109	172.21.42.103	TCP	66	443 > 44412 [ACK] Seq=1 Ack=518 Win=28160 Len=0 TSval=4126787689 TSecr=1032871
28.832625	52.51.145.109	172.21.42.103	TLSv1.2	1514	Server Hello
28.832694	52.51.145.109	172.21.42.103	TLSv1.2	1448	Certificate, Server Key Exchange, Server Hello Done
28.832907	172.21.42.103	52.51.145.109	TCP	66	44412 > 443 [ACK] Seq=518 Ack=1449 Win=32128 Len=0 TSval=1032877 TSecr=4126787689
28.833084	172.21.42.103	52.51.145.109	TCP	66	44412 > 443 [ACK] Seq=518 Ack=2831 Win=35008 Len=0 TSval=1032877 TSecr=4126787689
28.858242	172.21.42.103	52.51.145.109	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
28.916519	52.51.145.109	172.21.42.103	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
28.947030	172.21.42.103	52.51.145.109	TLSv1.2	592	Application Data
29.015383	52.51.145.109	172.21.42.103	TCP	66	[TCP Previous segment not captured] 443 > 44412 [FIN, ACK] Seq=3960 Ack=1170 Win=29184 Len=0 TSval=4126787735 TSecr=1032889
29.015427	52.51.145.109	172.21.42.103	TCP	922	[TCP Out-Of-Order] 443 > 44412 [PSH, ACK] Seq=3073 Ack=1170 Win=29184 Len=856 TSval=4126787735 TSecr=1032889
29.015436	52.51.145.109	172.21.42.103	TCP	97	[TCP Out-Of-Order] 443 > 44412 [PSH, ACK] Seq=3929 Ack=1170 Win=29184 Len=31 TSval=4126787735 TSecr=1032889
29.015643	172.21.42.103	52.51.145.109	TCP	78	[TCP Dup ACK 27#1] 44412 > 443 [ACK] Seq=1170 Ack=3073 Win=37888 Len=0 TSval=1032896 TSecr=4126787710 SLE=3960 SRE=3961

29.015809	172.21.42.103	52.51.145.109	TCP	78	44412 > 443 [ACK] Seq=1170 Ack=3929 Win=40832 Len=0 TSval=1032896 TSecr=4126787735 SLE=3960 SRE=3961
29.015932	172.21.42.103	52.51.145.109	TCP	66	44412 > 443 [ACK] Seq=1170 Ack=3961 Win=40832 Len=0 TSval=1032896 TSecr=4126787735
29.024766	172.21.42.103	52.51.145.109	TCP	66	44412 > 443 [RST, ACK] Seq=1170 Ack=3961 Win=40832 Len=0 TSval=1032896 TSecr=4126787735
30.381885	172.21.42.103	239.255.255.250	SSDP	159	M-SEARCH * HTTP/1.1
30.382447	172.21.42.103	239.255.255.250	SSDP	168	M-SEARCH * HTTP/1.1
30.382862	172.21.42.103	239.255.255.250	SSDP	143	M-SEARCH * HTTP/1.1
30.399705	172.21.42.103	172.21.42.1	TCP	74	38029 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1033034 TSecr=0 WS=64
31.395312	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38029 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1033134 TSecr=0 WS=64
33.395352	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38029 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1033334 TSecr=0 WS=64
33.495356	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38020 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1033344 TSecr=0 WS=64
33.584409	TexasIns_e3:6c:31	ZyxelCom_70:c3:be	ARP	60	172.21.42.103 is at 90:70:65:e3:6c:31
37.405325	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38029 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1033735 TSecr=0 WS=64
45.415381	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38029 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1034536 TSecr=0 WS=64
48.379196	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.2? Tell 172.21.42.103
48.388179	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.5? Tell 172.21.42.103
48.407956	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.8? Tell 172.21.42.103
48.427992	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.11? Tell 172.21.42.103
58.427265	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.128? Tell 172.21.42.103
58.507462	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.22? Tell 172.21.42.103
58.527517	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.128? Tell 172.21.42.103
59.999469	172.21.42.103	54.77.86.190	TLSv1.2	280	Application Data
60.072826	54.77.86.190	172.21.42.103	TLSv1.2	178	Application Data
60.073131	172.21.42.103	54.77.86.190	TCP	66	52471 > 443 [ACK] Seq=429 Ack=225 Win=1288 Len=0 TSval=1036001 TSecr=887751371
61.455451	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38029 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1036140 TSecr=0 WS=64
62.402996	172.21.42.103	239.255.255.250	UDP	69	42175 > 10000 Len=27
65.074573	TexasIns_e3:6c:31	ZyxelCom_70:c3:be	ARP	60	172.21.42.103 is at 90:70:65:e3:6c:31
88.553675	172.21.42.103	195.197.54.100	DNS	76	Standard query 0xbb4d A cloud4.cozify.fi
88.553878	172.21.42.103	212.54.0.3	DNS	76	Standard query 0xbb4d A cloud4.cozify.fi
88.554042	172.21.42.103	8.8.8.8	DNS	76	Standard query 0xbb4d A cloud4.cozify.fi
88.567650	195.197.54.100	172.21.42.103	DNS	108	Standard query response 0xbb4d A cloud4.cozify.fi A 34.243.221.45 A 52.51.145.109
88.567726	212.54.0.3	172.21.42.103	DNS	108	Standard query response 0xbb4d A cloud4.cozify.fi A 52.51.145.109 A 34.243.221.45
88.568496	172.21.42.103	212.54.0.3	DNS	76	Standard query 0x7182 A cloud4.cozify.fi
88.575397	172.21.42.103	34.243.221.45	TCP	74	52475 > 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1038851 TSecr=0 WS=64
88.582000	212.54.0.3	172.21.42.103	DNS	108	Standard query response 0x7182 A cloud4.cozify.fi A 52.51.145.109 A 34.243.221.45
88.583173	8.8.8.8	172.21.42.103	DNS	108	Standard query response 0xbb4d A cloud4.cozify.fi A 34.243.221.45 A 52.51.145.109
88.583423	172.21.42.103	8.8.8.8	ICMP	136	Destination unreachable (Port unreachable)
88.588155	172.21.42.103	52.51.145.109	TCP	74	44422 > 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1038853 TSecr=0 WS=64
88.630837	34.243.221.45	172.21.42.103	TCP	74	443 > 52475 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=1145457058 TSecr=1038851 WS=256
88.631178	172.21.42.103	34.243.221.45	TCP	66	52475 > 443 [ACK] Seq=1 Ack=1 Win=29248 Len=0 TSval=1038857 TSecr=1145457058
88.645989	52.51.145.109	172.21.42.103	TCP	74	443 > 44422 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=4126802642 TSecr=1038853 WS=256
88.646390	172.21.42.103	52.51.145.109	TCP	66	44422 > 443 [ACK] Seq=1 Ack=1 Win=29248 Len=0 TSval=1038859 TSecr=4126802642
88.761735	172.21.42.103	34.243.221.45	TLSv1.2	583	Client Hello

88.817227	34.243.221.45	172.21.42.103	TCP	66	443 > 52475 [ACK] Seq=1 Ack=518 Win=28160 Len=0 TSval=1145457105 TSecr=1038870
88.818126	34.243.221.45	172.21.42.103	TLSv1.2	1514	Server Hello
88.818483	34.243.221.45	172.21.42.103	TLSv1.2	1448	Certificate, Server Key Exchange, Server Hello Done
88.818484	172.21.42.103	34.243.221.45	TCP	66	52475 > 443 [ACK] Seq=518 Ack=1449 Win=32128 Len=0 TSval=1038876 TSecr=1145457105
88.818728	172.21.42.103	34.243.221.45	TCP	66	52475 > 443 [ACK] Seq=518 Ack=2831 Win=35008 Len=0 TSval=1038876 TSecr=1145457105
88.888047	172.21.42.103	52.51.145.109	TLSv1.2	583	Client Hello
88.913054	172.21.42.103	34.243.221.45	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
88.946374	52.51.145.109	172.21.42.103	TCP	66	443 > 44422 [ACK] Seq=1 Ack=518 Win=28160 Len=0 TSval=4126802717 TSecr=1038883
88.947698	52.51.145.109	172.21.42.103	TLSv1.2	1514	Server Hello
88.947989	172.21.42.103	52.51.145.109	TCP	66	44422 > 443 [ACK] Seq=518 Ack=1449 Win=32128 Len=0 TSval=1038889 TSecr=4126802718
88.948070	52.51.145.109	172.21.42.103	TLSv1.2	1448	Certificate, Server Key Exchange, Server Hello Done
88.948383	172.21.42.103	52.51.145.109	TCP	66	44422 > 443 [ACK] Seq=518 Ack=2831 Win=35008 Len=0 TSval=1038889 TSecr=4126802718
88.968401	34.243.221.45	172.21.42.103	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
88.968724	172.21.42.103	34.243.221.45	TCP	66	52475 > 443 [ACK] Seq=644 Ack=3073 Win=37888 Len=0 TSval=1038891 TSecr=1145457143
88.974187	172.21.42.103	52.51.145.109	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
88.982762	172.21.42.103	34.243.221.45	TLSv1.2	592	Application Data
89.032383	52.51.145.109	172.21.42.103	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
89.040835	172.21.42.103	52.51.145.109	TLSv1.2	592	Application Data
89.056466	34.243.221.45	172.21.42.103	TLSv1.2	922	Application Data
89.056509	34.243.221.45	172.21.42.103	TLSv1.2	97	Encrypted Alert
89.056710	34.243.221.45	172.21.42.103	TCP	66	443 > 52475 [FIN, ACK] Seq=3960 Ack=1170 Win=29184 Len=0 TSval=1145457165 TSecr=1038892
89.065601	172.21.42.103	34.243.221.45	TCP	66	52475 > 443 [RST, ACK] Seq=1170 Ack=3961 Win=40832 Len=0 TSval=1038900 TSecr=1145457165
89.104463	52.51.145.109	172.21.42.103	TLSv1.2	685	Application Data
89.104510	52.51.145.109	172.21.42.103	TLSv1.2	97	Encrypted Alert
89.104751	52.51.145.109	172.21.42.103	TCP	66	443 > 44422 [FIN, ACK] Seq=3723 Ack=1170 Win=29184 Len=0 TSval=4126802757 TSecr=1038898
89.113493	172.21.42.103	52.51.145.109	TCP	66	44422 > 443 [RST, ACK] Seq=1170 Ack=3724 Win=40832 Len=0 TSval=1038905 TSecr=4126802757
89.157218	172.21.42.103	34.243.221.45	TCP	74	52477 > 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1038910 TSecr=0 WS=64
89.214106	34.243.221.45	172.21.42.103	TCP	74	443 > 52477 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=1145457204 TSecr=1038910 WS=256
89.214377	172.21.42.103	34.243.221.45	TCP	66	52477 > 443 [ACK] Seq=1 Ack=1 Win=29248 Len=0 TSval=1038915 TSecr=1145457204
89.332749	172.21.42.103	34.243.221.45	TLSv1.2	583	Client Hello
89.389988	34.243.221.45	172.21.42.103	TCP	66	443 > 52477 [ACK] Seq=1 Ack=518 Win=28160 Len=0 TSval=1145457248 TSecr=1038927
89.390928	34.243.221.45	172.21.42.103	TLSv1.2	1514	Server Hello
89.391218	172.21.42.103	34.243.221.45	TCP	66	52477 > 443 [ACK] Seq=518 Ack=1449 Win=32128 Len=0 TSval=1038933 TSecr=1145457248
89.391294	34.243.221.45	172.21.42.103	TLSv1.2	1448	Certificate, Server Key Exchange, Server Hello Done
89.391527	172.21.42.103	34.243.221.45	TCP	66	52477 > 443 [ACK] Seq=518 Ack=2831 Win=35008 Len=0 TSval=1038933 TSecr=1145457248
89.417122	172.21.42.103	34.243.221.45	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
89.473636	34.243.221.45	172.21.42.103	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
89.482164	172.21.42.103	34.243.221.45	TLSv1.2	584	Application Data
89.551758	34.243.221.45	172.21.42.103	TLSv1.2	810	Application Data
89.551789	34.243.221.45	172.21.42.103	TLSv1.2	97	Encrypted Alert
89.551950	34.243.221.45	172.21.42.103	TCP	66	443 > 52477 [FIN, ACK] Seq=3848 Ack=1162 Win=29184 Len=0 TSval=1145457288 TSecr=1038942
89.560488	172.21.42.103	34.243.221.45	TCP	66	52477 > 443 [RST, ACK] Seq=1162 Ack=3849 Win=40832 Len=0 TSval=1038950 TSecr=1145457288
90.389147	172.21.42.103	239.255.255.250	SSDP	159	M-SEARCH * HTTP/1.1

90.389747	172.21.42.103	239.255.255.250	SSDP	168	M-SEARCH * HTTP/1.1
90.390209	172.21.42.103	239.255.255.250	SSDP	143	M-SEARCH * HTTP/1.1
90.407223	172.21.42.103	172.21.42.1	TCP	74	38040 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1039035 TSecr=0 WS=64
91.405517	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38040 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1039135 TSecr=0 WS=64
93.405484	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38040 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1039335 TSecr=0 WS=64
93.495479	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38029 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1039344 TSecr=0 WS=64
93.584591	TexasIns_e3:6c:31	ZyxelCom_70:c3:be	ARP	60	172.21.42.103 is at 90:70:65:e3:6c:31
97.415523	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38040 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1039736 TSecr=0 WS=64
105.435586	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38040 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1040538 TSecr=0 WS=64
111.866315	172.21.42.103	239.255.255.250	UDP	704	45770 > 3702 Len=662
120.000082	172.21.42.103	54.77.86.190	TLSv1.2	280	Application Data
120.073004	54.77.86.190	172.21.42.103	TLSv1.2	178	Application Data
120.073317	172.21.42.103	54.77.86.190	TCP	66	52471 > 443 [ACK] Seq=643 Ack=337 Win=1288 Len=0 TSval=1042001 TSecr=887766371
121.495627	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38040 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1042144 TSecr=0 WS=64
122.402729	172.21.42.103	239.255.255.250	UDP	69	37725 > 10000 Len=27
138.379808	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.2? Tell 172.21.42.103
138.388801	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.5? Tell 172.21.42.103
138.408365	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.8? Tell 172.21.42.103
138.428460	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.11? Tell 172.21.42.103
148.447598	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.59? Tell 172.21.42.103
148.467602	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.169? Tell 172.21.42.103
148.487572	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.204? Tell 172.21.42.103
148.507671	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.101? Tell 172.21.42.103
148.557219	172.21.42.103	195.197.54.100	DNS	76	Standard query 0x359e A cloud4.cozify.fi
148.557443	172.21.42.103	212.54.0.3	DNS	76	Standard query 0x359e A cloud4.cozify.fi
148.557725	172.21.42.103	8.8.8.8	DNS	76	Standard query 0x359e A cloud4.cozify.fi
148.571110	195.197.54.100	172.21.42.103	DNS	108	Standard query response 0x359e A cloud4.cozify.fi A 34.243.221.45 A 52.51.145.109
148.571427	212.54.0.3	172.21.42.103	DNS	108	Standard query response 0x359e A cloud4.cozify.fi A 34.243.221.45 A 52.51.145.109
148.577475	8.8.8.8	172.21.42.103	DNS	108	Standard query response 0x359e A cloud4.cozify.fi A 52.51.145.109 A 34.243.221.45
148.577846	172.21.42.103	8.8.8.8	ICMP	136	Destination unreachable (Port unreachable)
148.578199	172.21.42.103	34.243.221.45	TCP	74	52486 > 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1044852 TSecr=0 WS=64
148.608002	TexasIns_e3:6c:31	Broadcast	ARP	60	Who has 172.21.42.101? Tell 172.21.42.103
148.634236	34.243.221.45	172.21.42.103	TCP	74	443 > 52486 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 MSS=1460 SACK_PERM=1 TSval=1145472059 TSecr=1044852 WS=256
148.634600	172.21.42.103	34.243.221.45	TCP	66	52486 > 443 [ACK] Seq=1 Ack=1 Win=29248 Len=0 TSval=1044857 TSecr=1145472059
148.812767	172.21.42.103	34.243.221.45	TLSv1.2	583	Client Hello
148.869013	34.243.221.45	172.21.42.103	TCP	66	443 > 52486 [ACK] Seq=1 Ack=518 Win=28160 Len=0 TSval=1145472118 TSecr=1044875
148.870344	34.243.221.45	172.21.42.103	TLSv1.2	1514	Server Hello
148.870409	34.243.221.45	172.21.42.103	TLSv1.2	1448	Certificate, Server Key Exchange, Server Hello Done
148.870672	172.21.42.103	34.243.221.45	TCP	66	52486 > 443 [ACK] Seq=518 Ack=1449 Win=32128 Len=0 TSval=1044881 TSecr=1145472118
148.870790	172.21.42.103	34.243.221.45	TCP	66	52486 > 443 [ACK] Seq=518 Ack=2831 Win=35008 Len=0 TSval=1044881 TSecr=1145472118
148.920674	172.21.42.103	34.243.221.45	TLSv1.2	192	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
148.977106	34.243.221.45	172.21.42.103	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
148.977500	172.21.42.103	34.243.221.45	TCP	66	52486 > 443 [ACK] Seq=644 Ack=3073 Win=37888 Len=0 TSval=1044892 TSecr=1145472144

148.998861	172.21.42.103	34.243.221.45	TLSv1.2	592	Application Data
149.065520	34.243.221.45	172.21.42.103	TCP	66	[TCP Previous segment not captured] 443 > 52486 [FIN, ACK] Seq=3960 Ack=1170 Win=29184 Len=0 TSval=1145472167 TSecr=1044894
149.065580	34.243.221.45	172.21.42.103	TCP	922	[TCP Out-Of-Order] 443 > 52486 [PSH, ACK] Seq=3073 Ack=1170 Win=29184 Len=856 TSval=1145472167 TSecr=1044894
149.065639	34.243.221.45	172.21.42.103	TCP	97	[TCP Out-Of-Order] 443 > 52486 [PSH, ACK] Seq=3929 Ack=1170 Win=29184 Len=31 TSval=1145472167 TSecr=1044894
149.065664	172.21.42.103	34.243.221.45	TCP	78	[TCP Dup ACK 1231#1] 52486 > 443 [ACK] Seq=1170 Ack=3073 Win=37888 Len=0 TSval=1044900 TSecr=1145472144 SLE=3960 SRE=3961
149.065971	172.21.42.103	34.243.221.45	TCP	78	52486 > 443 [ACK] Seq=1170 Ack=3929 Win=40832 Len=0 TSval=1044900 TSecr=1145472167 SLE=3960 SRE=3961
149.066024	172.21.42.103	34.243.221.45	TCP	66	52486 > 443 [ACK] Seq=1170 Ack=3961 Win=40832 Len=0 TSval=1044900 TSecr=1145472167
149.075068	172.21.42.103	34.243.221.45	TCP	66	52486 > 443 [RST, ACK] Seq=1170 Ack=3961 Win=40832 Len=0 TSval=1044901 TSecr=1145472167
150.397071	172.21.42.103	239.255.255.250	SSDP	159	M-SEARCH * HTTP/1.1
150.397622	172.21.42.103	239.255.255.250	SSDP	168	M-SEARCH * HTTP/1.1
150.398064	172.21.42.103	239.255.255.250	SSDP	143	M-SEARCH * HTTP/1.1
150.414456	172.21.42.103	172.21.42.1	TCP	74	38049 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1045035 TSecr=0 WS=64
151.405832	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38049 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1045135 TSecr=0 WS=64
153.405825	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38049 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1045335 TSecr=0 WS=64
153.575825	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38040 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1045352 TSecr=0 WS=64
153.634866	TexasIns_e3:6c:31	ZyxelCom_70:c3:be	ARP	60	172.21.42.103 is at 90:70:65:e3:6c:31
154.663301	172.21.42.103	62.237.86.238	NTP	90	NTP Version 4, client
154.687716	62.237.86.238	172.21.42.103	NTP	90	NTP Version 4, server
155.663446	172.21.42.103	89.163.128.33	NTP	90	NTP Version 4, client
155.702214	89.163.128.33	172.21.42.103	NTP	90	NTP Version 4, server
157.415860	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38049 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1045736 TSecr=0 WS=64
165.435899	172.21.42.103	172.21.42.1	TCP	74	[TCP Retransmission] 38049 > 54171 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1046538 TSecr=0 WS=64
171.866144	172.21.42.103	239.255.255.250	UDP	704	35310 > 3702 Len=662
175.663557	172.21.42.103	185.31.136.34	NTP	90	NTP Version 4, client
175.678261	185.31.136.34	172.21.42.103	NTP	90	NTP Version 4, server

Cozifyn liikennekaappauksen tilastot

Tiedot sisältävät taulukosta poistetut ARP-paketit.

Paketteja (kpl)	1 182
Pakettien aikaväli (s)	175,678
Paketteja sekunnissa, keskiarvo	6,7
Paketin koko, keskiarvo (B)	86,5
Tavuja	102 062
Tavuja sekunnissa, keskiarvo	580
Bittejä sekunnissa, keskiarvo	4 647