TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Albert Derevski 185879 IACB

KNX SECURE RAKENDAMINE ELAMUS

Bakalaurusetöö

Juhendaja: Andres Rähni, tehnikateaduste magister

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Albert Derevski

10.03.2023

Annotatsioon

KNX Secure on KNX-standardil põhinev turvalisuslahendus, mis on mõeldud hoonete automaatika- ja juhtimissüsteemidele. Selle eesmärk on tagada KNX-võrgu turvalisus, võimaldades autentimist ja autoriseerimist seadmete vahel ning andmeedastuse krüpteerimist.

Töös teostatakse lühike võrdlus KNX, Zigbee ja Z-Wave hooneautomaatika süsteemide vahel tuues välja nende plussid ja miinused. Esitatakse KNX projekti turvalisuse tõstmise näidis ETS6 tarkvaras. Hinnatakse olemasoleva KNX projekti riske, kui KNX Secure't mitte kasutada. Töös tehakse kokkuvõtvad üldistused, millal on KNX Secure kasutamine elamutes vajalik ja millal soovituslik.

Abstract

KNX Secure is a security solution based on the KNX standard intended for building automation and control systems. Its purpose is to ensure the security of the KNX network by enabling authentication and authorization between devices and encryption of data transmission.

The thesis makes a short comparison between KNX, Zigbee and Z-Wave building automation systems, highlighting their pros and cons. An example of improving the security of the KNX project in the ETS6 software is presented. The risks of an existing KNX project if KNX Secure is not used are assessed. In the paper, summary generalizations are made, when the use of KNX Secure in residential buildings is necessary and when it is recommended.

Sisukord

Lühendite ja tähiste loetelu

AES (Advanced Encryption Standard) - Täiustatud krüpteerimisstandard

CA (Certificate Authority) – Sertifikaadi väljastaja

DDOS (Distributed denial-of-service) – Teenusetõkestusrünne, mis tähendab seadme või võrgu ülekoormamine suure hulga päringute saatmise teel.

End device – (KNX) Liini seade

EN (Europäische Norm) – Euroopa standard

ETS – Engineering Tool Software

Fiber optics - Fiiberoptika

IP – Internet protokoll

IP backbone – IP magistraalvõrk

IP coupler – IP liinile ühendaja

IP device – IP võrgu seade

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) - Rahvusvaheline Standardiorganisatsioon/Rahvusvaheline Elektrotehnikakomisjon

KNX.PL – Toitepingevõrgupõhise andmesidega KNX võrk (Power Line)

KNX.RF (KNX.Radio Frequency) – Raadisageduslik KNX ühendus

KNX.TP (KNX.Twisted-Pair) –

KNXnet/IP – Internet protokolliga KNX ühendus

Line coupler (TP1/TP1) – Seade elektrienergia ülekandmiseks ühest ahelast teise, mille esmane ja sekundaarne külg omab keerdpaar meediumit.

PKI (Public Key Infrastructure) - Avaliku võtme infrastruktuur

QR (Quick Response) kood - Kahemõõtmeline maatrikskood

TP area – Keerdpaarliiniga ala

TP line – Keerdpaarliin

Sissejuhatus

Hooneautomaatika süsteemid mängivad tänapäeva hoonetes olulist rolli, võimaldades integreerida erinevaid seadmeid ja süsteeme ning tagades nende tõhusa juhtimise ja halduse. KNX-standard on üks laialdaselt kasutatavatest standarditest selles valdkonnas, mis võimaldab erinevatel seadmetel omavahel suhelda ühtse KNX-võrgu kaudu.

KNX Secure on turvalisuslahendus, mis on välja töötatud hooneautomaatika süsteemide jaoks. Selle rakendamine on muutunud üha olulisemaks elamutes, kuna rohkem inimesi integreerib oma kodudes nutikaid seadmeid ja süsteeme, nagu valgustus, kütte- ja jahutussüsteemid, turvasüsteemid ja palju muud. KNX Secure pakub täiendavat turvalisuskihti, mis aitab kaitsta elamu KNX hooneautomaatika osasid, andmete kuritarvitamise või ründe eest.

Elamute automatiseerimine ja juhtimissüsteemide kasutamine võimaldab inimestel täielikku kontrolli oma kodude üle, parandades mugavust, energiatõhusust ja turvalisust. Nutikad seadmed ja süsteemid suhtlevad omavahel, võimaldades kasutajatel juhtida erinevaid funktsioone ja saada reaalajas teavet. Sellised süsteemid, kus on mitmeid seadmeid ja nende omavaheline suhtlus, tekitavad aga ka turvariske. Volitamata juurdepääs võib panna ohtu nii isikliku privaatsuse kui ka füüsilise turvalisuse. Seetõttu on ülioluline tagada selliste süsteemide turvalisus.

Töö esimeses kahe peatükis kirjeldatakse KNX ja KNX Secure tehnoloogia põhimõtteid, töö eesmärkideks on näidata kuidas tõsta projekti turvalisust ETS6 tarkvaras kasutades KNX Secure lahendust. Samuti kolmandas peatükis on olemasoleva hooneautomaatika projekti lahenduse riskide hindamine kui mitte kasutada KNX Secure’i. Neljandas peatükkis esitatakse suurimad poolt ja vastu argumendid miks kasutada või miks mitte kasutada KNX Secure lahendust elamuhoones.

1 KNX tehnoloogia

Konnex (KNX), varem tuntud kui European Installation Bus (EIB), on hoone juhtimis sidesüsteem, mis kasutab infotehnoloogiat ühenduse loomiseks selliste seadmete vahel nagu andurid, täiturmehhanismid, kontrollerid ja inimliides. Andmeid vahendatakse sellises süsteemis kasutades andmeraamistiku, mis on standardiseeritud viis, kuidas vahetada ja struktureerida andmeid KNX süsteemides (vt Joonis 1.1). KNX tehnoloogia on loodud automatiseeritud funktsioonide ja protsesside rakendamiseks hoonete elektripaigaldistes.

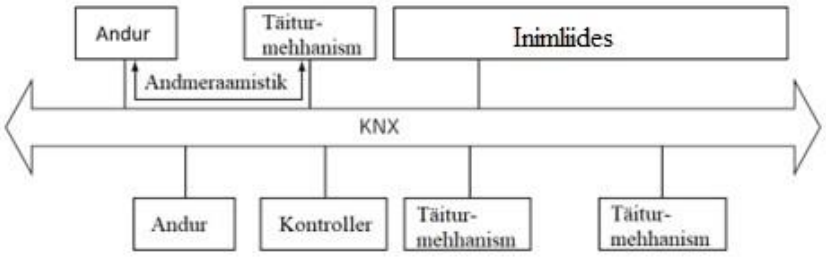
„European Installation Bus (EIB) ajalugu algas aastal 1990, kui oli loodud ühing *European Installation Bus Association*. Ühingu eesmärgiks oli EIB standardi edasi viimine ning arengu soodustamine. Hiljem kujunes sellest ühingust välja *Konnex Association*, ning European Installation Bus standard muutus Konnex standardiks.“ [1]

Andmete saatmisel ühest seadmest teise, manustatakse esmalt saadetav informatsioon andmeraamistikku ning seejärel edastatakse digitaalsel teel mööda väljasiini. Ülekande jaoks kasutatakse erinevaid andmekande meediaid : keerdpaarkaabel (KNX.TP), vahelduvpinge toitepingevõrku (KNX.PL), raadiosagedus (KNX.RF) ja fiiberoptiline kaabel. Seadmed, mis on funktsiooni täitmisega seotud, vahetavad omavahel teavet otse.

Konnex’it on võimalik kasutada valgustite, kütte, ventilatsiooni või aknavarjete juhtimiseks. Genereerides käsku anduriga, näiteks surunupuga edastaks see käsk andmeside kaudu täiturmehhanismi. Niipea kui täiturmehhanism võtab andmeid vastu, vastab ta saates tagasi kinnituse ning seejärel täidab käsku. Võimalik on ka näiteks seadistada küttesüsteem nii, et see alustaks oma tööd tund aega enne hoone avamist. Sellega saavutatakse hoones vajaliku temperatuur enne selle kasutust.

KNX, kasutades peamiselt KNX.TP ehk keerdpaarkaablit, paigaldatakse uutesse elamu- ja ärihoonetesse, kuid on võimalik integreerida ka vanematesse hoonetesse kasutades lisaks toitepingevõrgupõhist või raadiosageduslikku andmesidet.

Kogu KNX süsteemide projekteerimine ning seadistamine käib läbi *Konnex Association*’i poolt loodud ETS6 tarkvara millest räägitakse täpsemalt peatükkis kolm.



Joonis 1.1 Hoone juhtimissüsteemi seadmed ühendatud KNX kaudu

KNX on loodud avatud standardina. Antud kontekstis tähendab, et seadmed, mis on toodetud erinevate tootjate poolt saavad omavahel suhelda läbi KNX. Hooneoperaator ei pea kasutama ühte konkreetset tootjat, vaid võib valida erinevaid seadmeid vastavalt vajadusele.

Süsteem on detsentraliseeritud, mis tähendab et iga seade omab mikrokontrollerit, läbi mille toimub suhtus teiste seadmetega. Tänu sellisele lahendusele pole vajadust juhtiva keskseadme järele. KNX andmeside ja andmesituse põhimõtted on standardiseeritud järgnevates ISO, EN ja IEC standardites: EN50090-#, ISO/IEC 14543-3-#, EN 13321-#, ISO EN 22510. [1]

1.1 Topoloogia

Erinevalt tava elektripaigaldistest omavad KNX süsteemi seadmed lisaks andmesidevõrku nn KNX andmesideliini. Vajaminev liin installeeritakse hoones andmesidevõrku. KNX lihtsamad väiksetarbega seadmed saavad toite sama keerupaari juhtmete e liini kaudu, mille kaudu toimib ka andmeside. Siiski vahelduvoolu toitevõrku tarbijasse kommuteerivad täiturseadmed vajavad lisaks andmesideliinile ka toitevõrgu ühendust.

Joonise 1.1 ja 1.2 topoloogia selgitab süsteemi struktuuri, kuidas on seadmed omavahel ühendatud. Topoloogia baseerub tavapärasel võrgustruktuuril, mida tuntakse kui puutopoloogia.

Puutopoloogia omab järgmist hierarhilist struktuuri:

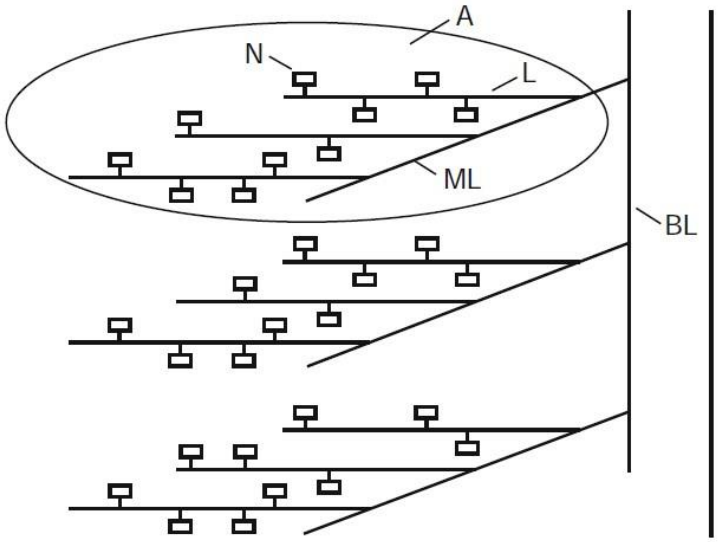
- Seadmed, mida nimetatakse ka sõlmedeks (nodes), kinnituvad liinile
- Põhiliini kaudu ühenduvad mitu liini ning moodustavad ala
- Magistraalliini kaudu ühenduvad mitu ala

Liin koosneb tavaliselt ühest liinisegmendist ja võib sisaldada kuni 64 seadet. Keerukamad süsteemid, mida katavad suuremat pindala ning omavad suuremat hulka seadmeid jaotatakse

aladeks mis sisaldavad kuni 16 liini. Iga liin saab sisaldada kuni neli liinisegmenti ja seetõttu omab kuni 256 seadet. Liinisegment on iseseisev võrguosa, kus saab hallata ja kontrollida KNX seadmeid ilma teiste liinisegmentide mõjutamiseta. Liinisegmendi eesmärk on parandada KNX süsteemi töökindlust ja vähendada sidehäirete riske. Uuemale KNX TP1 – 256 standardile vastavaid seadmeid saab ühele liinile ühendada 256 tükki ilma Line Repeater-eid (liinijärgureid) kasutamata. Uues starndardis saab Segmendis kokku panna ka TP ja RF seadmeid.[32] Liinisegmendid, liinid ja alad ühenduvad omavahel kasutades liinijärgureid, liiniühendajaid ja piirkonna ühendusi. Seadmeteks KNX süsteemis peetakse andureid, täiturmehhanisme ja liideseid, mis suhtlevad omavahel andmevahetuse teel. Iga seade omab grupiaadressi, mida kasutatakse suhtlemiseks ning füüsilise aadressi, mida kasutatakse seadme liinile seadistamisel.

Järgnevalt on toodud reeglid, mida peab jälgima liini või liinisegmendi projekteerimisel:

- Maksimaalne liini pikkus ei saa olla rohkem kui 1000 m.
- Maksimaalne kaugus kahe suhtleva seadme vahel ei saa ületada 700 m
- Toiteallika ja seadme vahemaa ei saa olla rohkem kui 350 m
- Kahe toiteallika vahemaa ühel liinisegmendil peab olema vähemalt 200 m



Joonis 1.2. KNX puutopoloogia, kus BL – Magistraalliini, A – Ala, ML – Põhiliin, L – Liin, N – Seade[1]

Iga liinisegment, põhiliin ja magistraalliin vajab oma vooluallikat. Eeliseks on see, kui liinil kaob toide, siis mõjutab see ainult seadmeid mis olid ühendatud antud liiniga. Muude liinide seadmeid ühe liini voolukatsestus ei mõjuta, kui juhuslikult ei tekki probleem põhi- või magistraalliinil siis kanduvad ka probleemid nendega ühendatud liinidele. [1]

1.2 Andmeedastus

KNX süsteem kasutab andmevahetuseks erinevaid meetodeid (andmeside meediaid). Nendeks meetoditeks on:

- Keerdpaarjuhe (ingl twisted pair või KNX.TP)
- Raadiosagedus (ingl radio frequency või KNX.RF)
- Ethernet (KNXnet/IP)
- Fiiberoptika (ingl fiber optics)
- Vahelduvpinge toitevõrk (KNX.PL)

Andmeedastus meetodit valitakse vastavalt hoone vajadustele, võimalustele ning minimeerides kulusid. Üheks meetodiks on keerdpaarjuhe. Selle eelis teiste edastusmeetodite üle on hind. Keerdpaar juhet on odav valmistada, paigaldada ja hooldada võrreldes teiste andmeside meediumitega nagu näiteks fiiberoptiline kaabel. Kuna kaabel on konstrueeritud elektromagnetilise segava mõju (EMI) ja raadiosagedusliku segava mõju (RFI) vähendamiseks teisest elektroonilistest seadmetest või kaablitest, siis mõjutab see andmeedastus kiirust ja kvaliteeti minimaalselt.

Vahelduvtoitepingevõrgu põhine andmeside on samuti üheks andmeedastus meetodiks. Selle eelduseks keerdpaar ühenduse üle on võimalus kasutada hoones juba olevat elektrivõrku. Vahelduvtoitepingevõrgul mööduv signaal pole kaitstud müra eest, mis omakorda langetab signaali kiirust ja kvaliteeti. [1]

Viimastel aastatel on populaarsust kogunud raadiosageduse meetod, mis kasutab andmete edastuseks raadiolaineid. Selle meetodi kasutust soodustab andmete võimet läbida seinu ja takistusi, tänu millele kaob vajadus KNX siinikaablis. Selline andmeedastuse omadus vähendab süsteemi paigalduse keerukust ning langetab ka selle hinna. [33]

2 KNX Secure

Koos asjade interneti (IoT) kasvuga maailmas on hoonete automatiseerimis süsteemid muutunud ühe ühendatumaks ja keerukamaks, võimaldades suuremat automatiseerimist, intelligentsust ja andmepõhist otsustamist. Kasvav sõltuvus hoonete automatiseerimis süsteemidest tähendab ka seda, et on suurem vajadus turvalise suhtluse järgi nende süsteemidega ühendatud seadmete vahel. Süsteemi turvalisuse ohud kujutavad endast olulist riski hoones viibijatele. Pahatahtlik edukas rünnak või autoriseerimata ühendus hoone

juhtsüsteemiga võib kaasa tuua erinevaid negatiivseid tagajärgi, sealhulgas privaatsuse kaotust, varalist kahju ja isegi ohtu elu jaoks. [7]

Selliste turvalisusprobleemide lahendamiseks on välja töötatud mitmesuguseid turvaprotokolle ja turvastandardeid. Need protokollid püüavad tagada turvalist suhtlust, autentimist ja andmekaitset seadmete vahel, tagades suhtluse konfidentsiaalsuse ja tervikluse. KNX ja teiste hoonete automatiseerimissüsteemide kasvav kasutamine on kaasa toonud suurema turvariski. KNX Secure on välja töötatud, et tagada KNX süsteemidele ja nendega ühendatud seadmetele turvaline suhtlus. [7]

KNX Secure võimaldab andmeid krüpteerida ja autentida säilitades suhtluse tervikluse. Antud protokoll tagab turvalise võrgusisese suhtluse ja volitamata seadmete juurdepääsu takistamise. KNX Secure kaudu saavad hoone omanikud ja administraatorid tagada oma hoonete automaatiseerimis süsteemide turvalisuse kaitstes elanike ning vara. [7]

KNX protokoll on loodud, et pakkuda turvalist ja töökindlat kommunikatsiooni hoonetele. KNX on juba iseenesest turvaline protokoll, kui süsteem ei oma ühendust välivõrguga näiteks internetiga või ründajal pole otsest ligipääsu süsteemi seadmetele või KNX liinile. KNX Secure laiendab KNX protokolli, lisades turvaelemente ja mehhanisme ohtude eest kaitsmiseks. [7]

2.1 KNX Secure arhitektuur

KNX Secure arhitektuur koosneb kahest põhikomponendist: KNX IP Secure ja KNX Data Secure. Iga komponent mängib olulist rolli võrgu turvalisuse tagamisel. Need komponendid tagavad turvalise kommunikatsiooni KNX-seadmete vahel juhtmega, juhtmeta ja IP-võrkude kaudu ning terviklu võrguturvalisuse.

KNX Secure arhitektuuri turvalisuse eelisteks on: [2], [4]

- Krüpteeritud andmeedastus – KNX Secure arhitektuur kasutab täiustatud krüpteerimisstandardit (AES), mis tagab andmete turvalise edastamise KNX-seadmete vahel.
- Volitatud juurdepääs – KNX Secure arhitektuur tagab, et võrgus on ainult volitatud seadmed ja kasutajad, vältides seeläbi volitamata juurdepääsu.
- Tsentraliseeritud autentimine ja autoriseerimine – KNX Secure Server pakub keskset autentimist ja autoriseerimist KNX-seadmetele, kontrollides võrgus olevate seadmete identiteedi ja volitusi.

2.1.1 KNX IP Secure

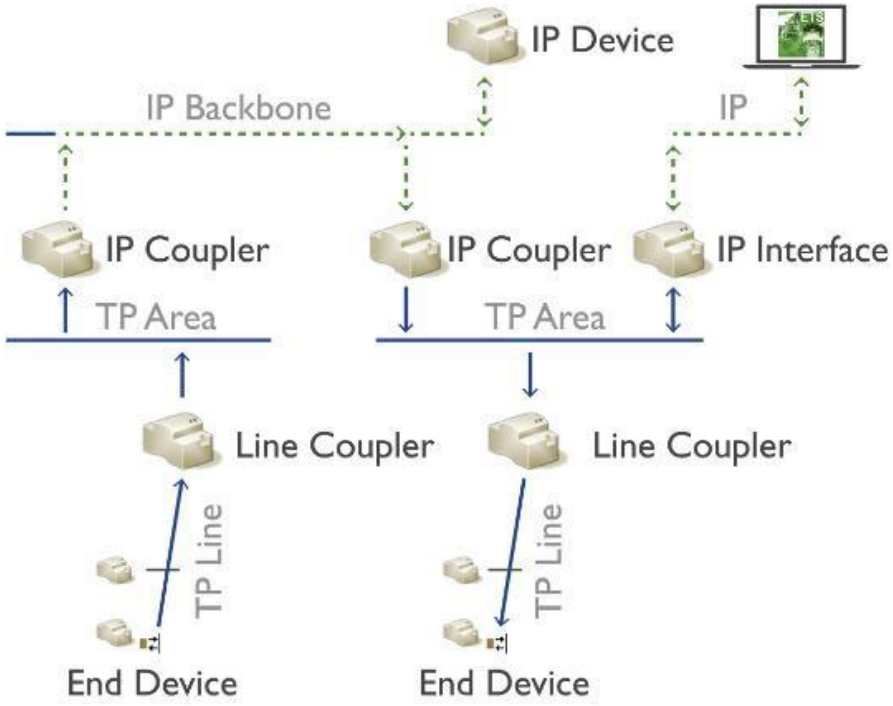
KNX IP Secure on KNX Secure arhitektuuri peamine tarkvarakomponent, mis tagab turvalise ühenduse KNX seadmete, võrgu kommutaator ja kesksete juhtimissüsteemide vahel (vt Joonis 2.1). See komponent kasutab ISO EN 22510 standardis kehtestatud, et krüpteerida ja autentida andmeedastust TCP/IP võrgus.

Üks olulisemaid aspekte turvalise ühenduse loomisel on võtmekehtestus, mille käigus genereeritakse ja vahetatakse turvalised võtmed, mida kasutatakse andmete krüpteerimiseks ja dekrüpteerimiseks.

KNX IP Secure võtmekehtestus toimub järgmiste sammude abil:

1. Võtmete genereerimine - Esimene samm võtmekehtestuses on võtmete genereerimine. Iga KNX IP Secure seade genereerib oma privaatse ja avaliku võtme, kusjuures privaatne võti hoitakse salajas ja avalik võti edastatakse teisele seadmele. Võtmete genereerimine toimub kohapeal ja on automatiseeritud.
2. Võtmevahetus - Järgmine samm on võtmekehtestus, kus kaks KNX IP Secure seadet vahetavad oma avalikke võtmeid. Seda võib teha automaatselt, ilma et kasutaja peaks midagi tegema. Võtmekehtestus käigus saavad mõlemad seadmed teada üksteise avalikud võtmed.
3. Ühise krüpteerimisvõtme genereerimine - Pärast avalike võtmete vahetamist genereerivad mõlemad KNX IP Secure seadmed ühise krüpteerimisvõtme, kasutades oma privaatset võtit ja vastuvõetud avalikku võtit. See ühine krüpteerimisvõti kasutatakse andmete krüpteerimiseks ja dekrüpteerimiseks, mis edastatakse turvalises ühenduses.
4. Turvalise ühenduse kinnitamine - Lõpuks tuleb turvaline ühendus kinnitada, et tagada, et volitamata seadmed ei saaks võrgule juurde pääseda. See saavutatakse kasutades autentimismeetodeid, näiteks sertifikaadipõhine autentimine.

Kuna seadmed saavad automaatselt luua turvalise ühenduse, ilma et administraatorid peaksid võtmeid haldama, siis lihtsustab see konfigureerimisprotsessi. [2], [3]

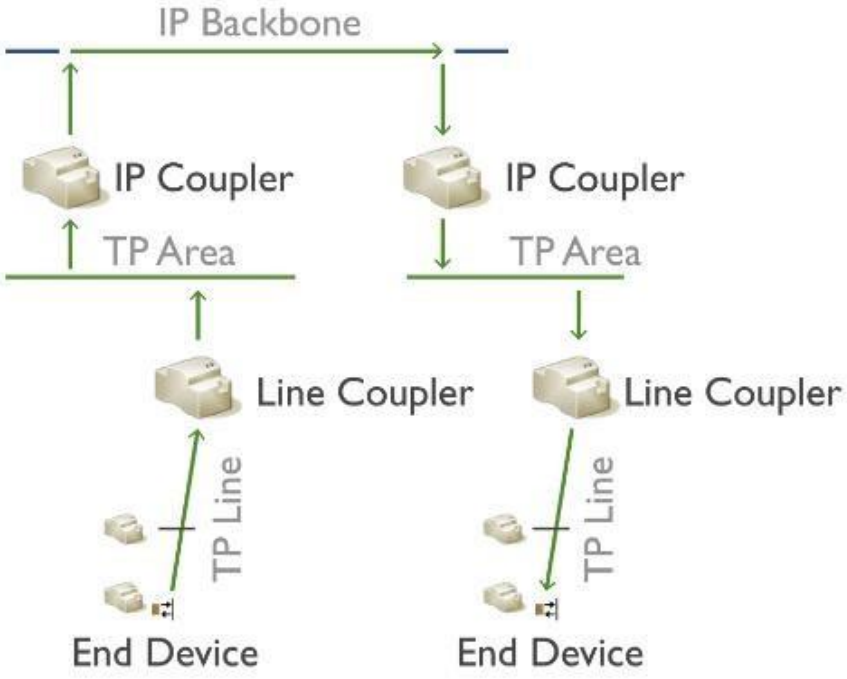


Joonis 2.1 KNX IP Secure ühendus hoonete vahel, kus rohelise joonega on märgitud turvaline ühendus KNX IP Secure poolt [14]

2.1.2 KNX Data Secure

KNX Data Secure on komponent, mis tagab KNX-seadmete turvalise kommunikatsiooni juhtmega ja juhtmeta võrkude kaudu. KNX Data Secure on kehtestatud ISO/IEC 14543-3-7 standardis kasutab AES-algoritmi kogu KNX-seadmete vahelise kommunikatsiooni krüpteerimiseks. See tagab, et kogu võrgu kaudu edastatud teave on turvaline ja seda ei saa kõrvalt kuulata ega muuta (vt Joonis 2.2). KNX Data Secure komponent on kohustuslik kõigile KNX Secure seadmetele ja tagab, et seadmed vastavad KNX Secure

spetsifikatsioonidele.[7],[19]



Joonis 2.2 KNX Data Secure ühendus hoones, kus rohelisena märgitud kaitstud ühendus[14]

2.2 KNX IP turva ja autentimismehhanismid

Autentimismehhanismid on KNX Secure arhitektuuri komponendid, mis võimaldavad seadmetel ennast identifitseerida ning tagavad volitatud juurdepääsu võrgus.

KNX Secure arhitektuuril on kaks autentimismehhanismi:

1. X.509 standard
2. TLS protokollid

Autentimismehhanismid töötavad süsteemis samal ajal. X.509 standard tegeleb seadmete autentimisega KNX-võrgus ning TLS protokollid pakub andmete krüpteerimist nende seadmete vahel. [2]

2.2.1 X.509 standard

X.509 on laialdaselt kasutatav avaliku võtme infrastruktuuri (PKI) ja digitaalsete sertifikaatide standard. X.509 sertifikaadid võimaldavad identiteedi autentimist, tervikluse tagamist ja krüpteerimist internetis ja muudes võrguühendustes.

KNX Secure kasutab X.509 sertifikaate autentimiseks ja krüpteerimiseks. Sertifikaadid sisaldavad avaliku võtme teavet, mis võimaldab teistel seadmetel autentida seadme identiteeti. Kui seade üritab KNX võrguga ühendust võtta, esitab ta oma sertifikaadi ja teised seadmed võivad kontrollida, kas sertifikaat on kehtiv ja autentne. [2] [21]

2.2.2 TLS protokoll

TLS protokollide kasutamine KNX Secure-s võimaldab kaitsta KNX võrku volitamata juurdepääsu, andmete kopeerimise ja muude rünnaku tüüpide eest. KNX Secure kasutab TLS protokolle andmete turvaliseks edastamiseks KNX võrgus. TLS protokollid võimaldavad krüpteerida andmeid, mis liiguvad KNX võrgus, nii et ainult volitatud seadmed saavad neid lugeda. Samuti võimaldavad TLS protokollid autentida KNX võrgus olevate seadmete identiteeti. TLS protokollid kasutavad avaliku võtme krüptograafiat.

TLS protokollid tagavad ka KNX võrgus olevate seadmete autentimise. Iga seade võtab enne võrguga ühenduse loomist ühendust sertifikaadi väljastanud asutusega, et kontrollida, kas sertifikaat on kehtiv ja autentne. Seejärel kasutatakse sertifikaate seadmete identiteedi kontrollimiseks KNX võrgus. [2],[15]

2.2.3 Sertifikaadid

Sertifikaadipõhine autentimine on KNX Secure'is põhiline autentimismehhanism. Selle mehhanismi korral autenditakse seadmed ja kasutajad digitaalsete sertifikaatide abil. Igal seadmel ja kasutajal on unikaalne digitaalne sertifikaat, mille väljastab usaldusväärne CA (Certificate Authority) ehk sertifikaadi väljastaja.

Sertifikaate väljastab ja haldab KNX Secure keskasutus. Keskasutus vastutab sertifikaatide väljastamise ja haldusega kõigi võrgul olevate seadmete ja kasutajate jaoks.

Kui uus seade või kasutaja lisatakse KNX-võrku, siis esitab selle omanik taotluse sertifikaadi saamiseks. Sertifikaadi taotlus peab sisaldama seadme või kasutaja identiteeti ja avalikku võtit, mis on seotud privaatvõtmega, mis on seadmel või kasutajal endal. KNX Secure keskasutus kontrollib sertifikaadi taotlust ja autendib seadme või kasutaja. Kui seade või kasutaja on autenditud, siis väljastatakse digitaalne sertifikaat. Sertifikaat sisaldab seadme või kasutaja identiteeti, avalikku võtit ja sertifikaadi kehtivusaega. Sertifikaatide haldamine toimub ETS6 tarkvara abiga.

KNX Secure keskasutus vastutab ka sertifikaatide haldamise eest. See hõlmab kehtivuse perioodide jälgimist, kehtivuse pikendamist ja tühistamist. Kui seade või kasutaja eemaldatakse võrgust, siis tühistatakse ka tema digitaalne sertifikaat.[2], [16], [21]

Üheks sertifikaatide haldus programmiks võib kasutada ettevõtte Jung poolt toodetud „Service app“, mida paigaldatakse ETS6 tarkvara laiendusena. Sertifikaatide lisamisel tarkvara laienduse abil peegelduvad nad ETS6 tarkvaras, kus on võimalik neid edasi hallata.[31]

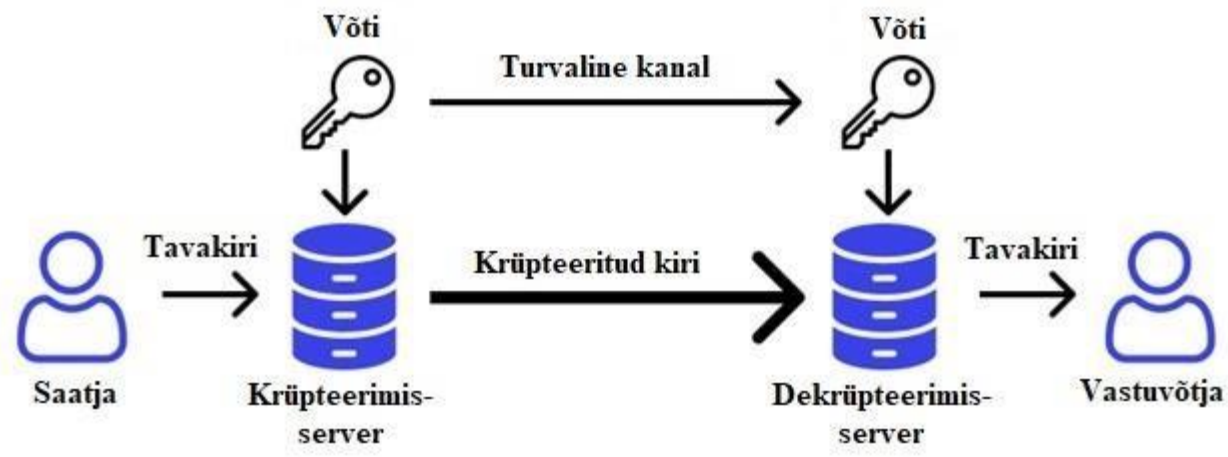
2.2.4 AES Protokoll

AES on krüptograafiline algoritm, mis on laialdaselt kasutusel andmete krüpteerimisel ja dekrüpteerimisel. KNX Secure, peamiselt KNX Data Secure kasutab AES-128 krüpteerimisalgoritmi andmete turvalisuse tagamiseks.

AES-128 on tugev krüpteerimisalgoritm, mis kasutab 128-bitist võtmepikkust. See tähendab, et erinevaid võtmekombinatsioone andmete dekrüpteerimiseks võib olla miljardeid. Antud tugevus muudab pahatahtliku murdmise äärmiselt raskeks, isegi kui ründaja kasutab tugevat arvutusvõimsust.

Krüpteerimisel kasutatakse kahte võtit, ühte saatmiseks ja teist vastuvõtmiseks. Andmeedastus on krüpteeritud enne saatmist ja dekrüpteeritud pärast vastuvõtmist, mis tähendab, et andmed on krüpteeritud kogu protsessi vältel. Seda tüüpi krüpteerimine lubab, et volitamata isikud ei saa KNX süsteemis andmeid lugeda ega muuta. AES-128 kasutamisega on võimalik kontrollida andmeedastuse autentsust (vt Joonis 2.3). Andmed saavad olla ainult siis dekrüpteeritud, kui vastuvõtja võti klapib saatja võtmega. See tagab seda, et andmeid poole muudetud volitamata isiku poolt.

AES protokoll tagab ka konfidentsiaalsuse. Selleks peab aga KNX süsteem olema seadistatud nii, et kõik süsteemi osad kasutaksid sama krüpteerimisalgoritmi ehk AES protokolli. [5], [17]



Joonis 2.3 AES algoritmi töö mudel, kus vasakul on saatja ja paremal on vastuvõtja [18]

2.3 KNX Secure autoriseerimismehhanismid

KNX Secure autoriseerimismehhanismid ehituvad rollipõhisel juurdepääsu kontrollil. See tähendab, et igale seadmele ja kasutajale on antud kindel roll, mis määrab tema võrgu juurdepääsuõigused ning funktsiooni selles võrgus.

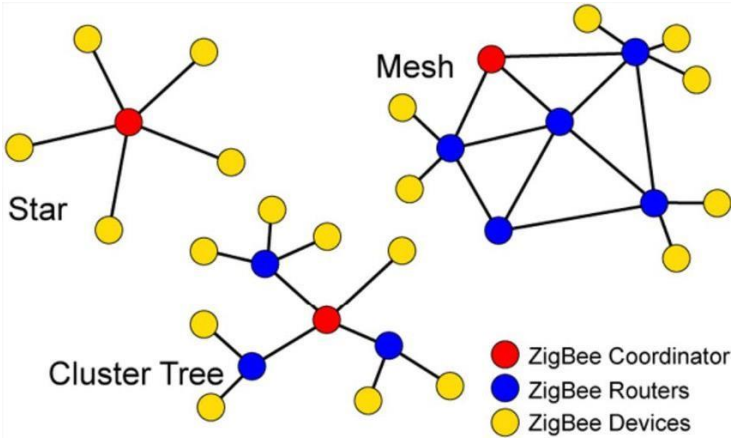
Iga KNX Secure seade võib kuuluda ühte või mitmesse rolligruppi, millel võivad olla erinevad õigused ja funktsioonid. Rollid võivad olla seotud konkreetsete alamsüsteemide või funktsioonidega. Näiteks võib üks rolligrupp olla seotud valgustuse juhtimisega, samas kui teine rolligrupp võib olla seotud hoone temperatuuri juhtimisega. [2]

2.4 KNX Secure võrdlus teiste turvalisust omavate protokollidega

KNX pole ainuke koduautomaatika standard mida kasutatakse laialdaselt üle maailma. Tema peamised juhtmevabad konkurendid on Z-Wave ja ZigBee. Z-Wave ja ZigBee on mõlemad juhtmevabad sideprotokollid, mida kasutatakse koduautomaatika ja IoT rakenduste jaoks. Mõlemad protokollid kasutavad madalat energiatarbimist ja võimaldavad seadmetel omavahel suhelda ilma kaabli ühenduseta.

Z-Wave on loodud 1999. aastal Taani ettevõtte Zensys poolt ja selle eripäraks on madal energiatarve, mis võimaldab seadmetel pikka aega töötada väikeste patareidega. Z-Wave põhineb silmusvõrk topoloogial. See tähendab, et iga võrku paigaldatud seade muutub signaali kordajaks, mis võimaldab seadmetel suhelda omavahel võrgus olevate teiste seadmete kaudu. Selle tulemusena muutub võrk tugevamaks, mida rohkem seadmeid hoones on.

ZigBee on loodud 2002. aastal ja see protokoll kasutab samuti madalat energiatarbimist. Zigbee omab kolme tüüpi võrgu topoloogiat. Tähe topoloogia, puu topoloogia ja silmusvõrk topoloogia. Igal topoloogial on erinev mõju sõnumite suunamisele ja sellele, millised seadmed milliste seadmetega ühendavad.



Joonis 2.4 paremalt vasakule: tähe topoloogia, puu topoloogia, silmusvõrk topoloogia [24]

Kui võrrelda KNX (vt Tabel 1), Z-Wave (vt Tabel 2) ja ZigBee (vt Tabel 3) siis on näha, et nende koduautomaatika standardite vahel pole kindlat võitjat. Iga lahendus omab plusse ja miinuseid. Seega valida mida kasutada tuleb vastavalt vajadustele ja olukorrale. [20], [23]

Tabel 1 KNX plussid ja miinused Z-Wave ja ZigBee suhtes:

KNX plussid	KNX miinused
Kõrge turvalisustase: KNX IP Secure pakub tugevat krüpteerimist, kaitstes andmeedastust seadmete vahel. Sellega tagatakse kõrge turvalisustaseme nutikate hoonete jaoks.	Hind: KNX seadmed on tavaliselt teiste protokollidega võrreldes kallimad, mis võib olla kasutajale piiravaks teguriks.
Koostöövõimelisus: KNX nagu ka Zigbee on avatud standardprotokollid, mis tähendab, et erinevate tootjate seadmed saavad omavahel suhelda probleemi vabalt, pakkudes maksimaalset paindlikkust nutikate kodu- ja hoonete integreerimiseks.	Keerukus: KNX seadmete paigaldus ja konfigureerimine nõuavad spetsiaalset väljaõpet ja teadmisi, mis võib olla väljakutseks hooneautomaatika tavakasutajatele.
Usaldus: KNX on turul olnud üle 30 aasta ja see on osutunud usaldusväärseks ja vastupidavaks protokolliks. Tänu sellele on turul ka väga suur valik seadmeid.	Signaalide leviku piirangud: KNX RF kasutab lühikese levialaga raadiolaineid, mis võivad olla tundlikud takistustele, näiteks seintele või muudele elektroonikaseadmetele, mis võivad signaali levikut piirata.

Tabel 2 Z-Wave plussid ja miinused KNX ja ZigBee suhtes:

Z-Wave plussid	Z-Wave miinused
Kõrge turvalisustase: Kõik kolm protokolli kasutavad AES128 standardi andmete krüpteerimiseks, kuid Z-Wave kasutab ka veel täiendavat turvakihti, Security 2, mis kaitseb sedameid DDOS rünnakute eest.	Piiratud ülekandekiirus: Z-Wave võrgud on madalama ülekandekiiruse, seega ei pruugi need olla optimaalsed suuremahuliste andmete edastamiseks. Andmeedastuse kiiruseks on keskmiselt 100Kbps
Skaleeritavus: Z-Wave seadmeid on võimalik võrgust lihtsasti lisada või eemaldada, muutes selle kõrgelt skaleeritavaks ja kohandatavaks erinevatele kodu- ja hoonete automatiseerimisstsenaariumitele.	Väiksem ühilduvus seadmetel: Z-Wave võrku on võimalik ühendada kõige väiksem arv seadmeid, milleks on 232. Selleks, et tõsta seadmete arvu peab kasutusse võtma sillatuid võrke.

Hind: Z-Wave seadmed on üldiselt odavamad kui KNX seadmed, mis teeb selle taskukohaseks valikuks nutikate kodude ja hoonete automatiseerimiseks.	Signaalide leviku piirangud: Nagu ka KNX RF kasutab Z-Wave protokoll lühikese levialaga raadiolaineid, mis võivad olla tundlikud takistustele.

Tabel 3 ZigBee plussid ja miinused KNX ja Z-Wave suhtes:

ZigBee plussid	ZigBee miinused
Kõrge skaleeritavus: ZigBee võrgud võivad toetada kuni 65000+ seadet, luues suurema katvuse ja paindlikkuse hooneautomaatika rakendustes.	Ühilduvus: Erinevate ZigBee seadmete vahel võib tekkida ühilduvusprobleeme, eriti juhul, kui need pärinevad erinevatelt tootjatelt või kasutavad erinevaid ZigBee profiile.
Hind: Zigbee nagu ka Z-Wave seadmed üldiselt odavamad kui KNX seadmed, mis teeb neid taskukohaseks valikuks nutikate kodude ja hoonete automatiseerimiseks.	Töösagedus: Kuna Zigbee töötab 2.4 GHz sagedusel, mis ühtib Wi-Fi töösagedusega, siis võib Zigbee töö häirida Wi-Fi võrgu tööd.
Kiirus: Zigbee on võimeline edastama andmeid kiiremini kasutades kõrgemat sagedust. Keskmiseks andmekiiruseks on 250 Kbps	Signaali ulatus: Zigbee signaali ulatus on väiksem kuna töötab kõrgemal sagedusel.

2.5 KNX Secure konfigureerimine ning optimeerimise tavad

KNX Secure on KNX-võrgu turvalisuse tagamiseks oluline lahendus. Kuid selle paigaldamine ja konfigureerimine nõuab hoolikat planeerimist ja tähelepanu detailidele. Seetõttu on eksisteerivad paigaldamise tavad, mida tuleb jälgida KNX Secure süsteemi püstitamisel.

2.5.1 KNX Secure arhitektuuri mõistmine

Süsteemi püstitamine algab tavaliselt arhitektuuri mõistmisega, mille alla kuulub arusaam kuidas eraldi komponendid töötavad. Näiteks on KNX IP Secure ja KNX Data Secure omavahel tihedalt seotud, kuna KNX IP Secure tagab turvalise IP-põhise ühenduse ja KNX Data Secure krüpteerib andmed, mida selle ühenduse kaudu edastatakse.

Lisaks on oluline mõista, kuidas KNX Secure arhitektuur sobitub üldise KNX-võrgu arhitektuuriga. KNX Secure võib töötada koos KNX-standardiga, mis tagab interoperatiivsuse ja ühilduvuse KNX-seadmetega. See tähendab, et KNX Secure võib olla integreeritud olemasolevasse KNX-võrku ilma selle ümberkujundamiseta. [4], [8], [9], [28]

2.5.2 KNX Secure paigaldamise eesmärgid ja eeltingimused

Esimeseks sammuks on leida eesmärke ning eeltingimusi enne KNX Secure paigaldamist, mis võivad enda alla võtta erinevaid aspekte, nagu näiteks tundlike andmete kaitse, turvalise sissepääsu ja häirete tuvastamine. Süsteemi eesmärkide määratlemisel tuleks arvestada ka konkreetse KNX-võrgu tüübiga ja selle kasutusviisiga. Näiteks võib eluruumide KNX-võrk vajada erinevaid turvameetmeid võrreldes tööstusliku KNX-võrguga. [4],

KNX Secure paigaldamise eeltingimused omavad mitmeid olulisi samme, mida tuleb täita, et tagada paigalduse tõhusus. Näiteks tuleb tagada, et kõik KNX-seadmed on ühilduvad KNX Secure-ga. Lisaks tuleb tagada, et kõik sertifikaadid ja võtmed on korrektselt väljastatud ja paigaldatud, et tagada andmete konfidentsiaalsus, terviklus ja autentsus. [8], [28]

2.5.3 KNX Secure komponentide õige konfigureerimine

Oluline samm on ka KNX Secure komponentide konfigureerimine. Siiski enne konfigureerimist tuleb kõigepealt tagada, et kõik KNX Secure komponendid on paigaldatud vastavalt tootja juhistele ning omavad õiget tarkvara koos püsivaraga. Järgmisena tuleb määratleda turvapoliitika, mis sisaldab turvameetmete kogumit. Rakendades neid tagatakse KNX-võrgu turvalisus. Poliitikas tuleb määratleda ka, millised seadmed on volitatud KNX-võrku sisenemiseks, millised funktsioonid on nendele seadmetele lubatud, millised mitte ning millised turvameetmed tuleks rakendada turvaliseks toimeks. [4]

Nagu ka paigaldamisel, tuleb konfigureerimisel jälgida vastavalt tootja juhistele, sealhulgas sertifikaatide ja võtmete installeerimine. Lisaks tuleks rakendada sobivaid turvameetmeid, nagu näiteks tulemüüri konfigureerimine, liikluse monitoorimine ja häirete tuvastus. Samuti tuleks jälgida, et KNX Secure konfiguratsioonid oleksid pidevalt ajakohased, et tagada nende vastavus turvalisuse standarditele ja minimeerides turvariske. [4], [28]

KNX Secure paigaldamise eesmärkide ja eeltingimuste ning komponentide õige konfigureerimine nõuab hoolikat planeerimist ja läbimõeldud strateegiat. Selleks tuleb kaasata spetsialiste ja eksperte, kes aitavad kindlaks teha sobivaimad turvameetmed ning kindlustada konfigureerimise efektiivsuse ja turvalisuse. Samuti on oluline

kindlustada, et paigaldamise ning konfigureerimise protsess oleks dokumenteeritud ja testitud enne selle kasutuselevõttu. [4], [9]

2.5.4 KNX-seadmete turvalisus k.a. KNX Secure seadmed

Järgmisena tuleb mõelda KNX-seadmete turvalisuse peale, kuna see tagab KNX-võrgu terviklikkuse, kaitstes volitamata juurdepääsude eest. KNX-seadmete turvalisus sisaldab mitmeid turvameetmeid, mis on rakendatud seadmete projekteerimisel, tootmisel ja paigaldamisel. Üks olulisemaid turvameetmeid on tarkvara uuenduste regulaarne paigaldamine, mis tagab, et KNXseadmed töötavad alati kõige ajakohasema turvakaitsega.

Kaaluda tuleb ka seadmetele füüsilise juurdepääsu piiramist, näiteks lukustamine füüsiliste või elektrooniliste lukkudega. Oluline on koolitada kasutajaid ja töötajaid, et tagada nende teadlikkus
KNX-seadmete turvalisusest ning vajalike turvameetmete
rakendamisest ja järgimisest.[4],[8],[28]

2.5.5 KNX Secure monitooring ja audit

KNX Secure monitooring ja audit võimaldab jälgida KNX-võrgu turvalisust ja kindlustab, et turvameetmed on efektiivsed ja vastavad standarditele. Monitooringu ja auditi kaudu tuvastatakse turvarikkeid ja turvalisuse nõrkuseid ning rakendatakse vajalikud meetmed nende kõrvaldamiseks ja vältimiseks tulevikus.

KNX Secure monitooring ja audit sisaldavad erinevaid tegevusi, nagu näiteks logifailide analüüs, võrgus toimuvate sündmuste jälgimine, võrgu turvalisuse nõrkuste skaneerimine ja testimine. Need tegevused võimaldavad tuvastada võimalikke rikkumisi ja turvariske, mis võivad olla seotud kasutaja käitumise, võrgu konfiguratsiooni või tarkvara nõrkusega. [4], [9],

Monitooring ja audit peab olema regulaarne protsess, mis toimub kindla ajakava järgi. See võib toimuda nädalaste või kuupõhiste tsüklitega, mille jooksul kogutakse andmeid võrguliikluse ja turvarikkumiste kohta. See võimaldab turvalisuseeskirjade jälgimist ja vastavust standarditele.

KNX Secure monitooring ja audit on tihedalt seotud infoturbe protsessidega, et kindlustada efektiivse turvameetmete kasutamise ja järgimise. Lisaks peab audit sisaldama selgeid meetmeid ja soovitusi, mida tuleks rakendada, et parandada võrgu turvalisust ja vältida edasisi rikkumisi. Samuti peab monitooring ja audit andma ülevaate võrgu turvalisuse seisundist ning võimaldama õigeaegset reageerimist võimalikele turvariskidele. [4], [8], [28]

2.5.6 Regulaarne KNX Secure tarkvara uuendamine

Regulaarne KNX Secure tarkvara uuendamine on oluline osa turvalisuse tagamisel ja võrgu kaitsevõime suurendamisel. Tarkvara uuendused sisaldavad enamasti uute turvapakettide ja paranduste väljalaskmist, mis võivad olla vajalikud võrgu turvalisuse tagamiseks. Seetõttu on oluline jälgida KNX Secure tarkvara tootjate välja antud värskenduste teadaandeid, et neid võimalikult kiiresti rakendada.

Regulaarsed KNX Secure tarkvara uuendused aitavad vähendada võimalusi rünnakuteks, kuna enamik rünnakuid on suunatud just leitud nõrkustele, mida tootjad pidevalt parandavad. Tarkvara uuendused võivad lisada uusi turvafunktsioone ja parandada olemasolevaid, suurendades võrgu kaitsevõimet. [4], [28]

Tarkvara uuendamine võib olla keeruline protsess, eriti kui see hõlmab võrgu ulatuslikke komponente. Seetõttu on soovitatav, et tarkvara uuendamist teostaksid spetsialistid, kes omavad asjakohaseid teadmisi ja kogemusi KNX Secure tarkvara haldamisel. Lisaks tuleb enne tarkvara uuendamisi teha varukoopiaid ja testida uuendusi eraldi keskkonnas, et vältida võimalikke süsteemi katkestusi ja vigu. [4], [9],

2.6 KNX Secure edasiarendus KNX assotsiatsioon poolt

KNX Secure on viimastel aastatel oluliselt arenenud. Paljud funktsioonid on lisatud, et tõsta süsteemi efektiivsust ja tagada KNX-võrgu kaitse võimalike rünnakute eest. KNX Secure arendajad töötavad jätkuvalt uute funktsioonide kallal, mis võivad tulevikus veelgi suurendada turvalisust ja tõsta võimalusi KNX Secure võrgus.

Tulevikusuund kuhu enamasti liigutakse on KNX Secure lihtsam kasutatavus ja süsteemi lihtsam integreerimine. KNX Secure võrgu haldamine muutub tänu sellele kergemaks ja kiiremaks. See omakorda tähendab, et uued tööriistad ja liidesed võimaldavad lihtsamat seadistamist ja juurdepääsu erinevatele funktsioonidele. KNX Secure integreerimine muude ehitusautomaatika lahendustega muutub ka tulevikus lihtsamaks.

KNX Secure tulevik on ka seotud turbe tehnoloogiate arengutega. Uued tehnoloogiad nagu näiteks kvantarvutid ja tehisintellekti areng võivad muuta KNX Secure turvalisust. See võib tähendada uute krüpteerimisalgoritmide ja autentimisviiside kasutuselevõttu. Seetõttu peavad KNX Secure arendajad olema pidevalt kursis uute tehnoloogiate arengutega ja otsida viise nende integreerimiseks KNX Secure turvalisusse. [10]-[13], [25]

2.6.1 KNX assotsiatsioon tuleviku väljakutsed KNX Secure suhtes

Kuigi KNX Secure on viimastel aastatel arenenud, on siiski mitmeid väljakutseid, mis seonduvad turvalisusega KNX-võrkudes ja KNX Secure'is.

Esimene väljakutse on turvalisuse teadlikkuse tõstmine kasutajate seas. Paljud KNX-võrkude omanikud ning kasutajad ei pruugi olla teadlikud selle turvalisusest või ei võta seda piisavalt tõsiselt. See võib põhjustada KNX-võrkude nõrkusi või isegi rünnakutele avatud olemist. Seetõttu oluline samm on suurendada teadlikkust KNX Secure'i turvalisusest ja selle tähtsusest. Seda võib saavutada kasutades hariduskampaaniaid, juhendeid ja tööriistu KNX-võrgu turvalisuse tagamiseks ning turvaauditeid.

Teine väljakutse on KNX-võrkude ulatuslik levik ja kasutus. KNX-võrkude kasutamine ja laienemine on aastatega ainult suurenenud. See tähendab, et KNX Secure peab vastama erinevatele nõudmistele ja võimaldama laialdast rakendamist erinevates ehitusautomaatika projektides. [11]-[13], [25]

2.6.2 KNX assotsiatsioon tuleviku plaanid ning võimalused KNX Secure suhtes

KNX Secure pakub tulevikus palju võimalusi ehitusautomaatika lahenduste ja turvalisuse jaoks. Üks peamisi võimalusi on seotud KNX Secure'i integreerimisega teiste ehitusautomaatika lahendustega. KNX Secure lubab ühendust teiste lahendustega, nagu näiteks IP-põhised lahendused, tagades KNX-võrgu ja kogu ehitusautomaatika süsteemi turvalisuse.

Teine võimalus on seotud KNX Secure'i kasutamisega suuremates projektides, näiteks tervishoiu- või haridusasutustes. Sellistes projektides on KNX-võrkude turvalisus eriti oluline ja KNX Secure võib olla ideaalne lahendus, mis tagab tervikliku turvalisuse. [10]-[11], [25]

3 KNX Secure rakendamine ETS6 tarkvaras

ETS6 (Engineering Tool Software 6) on tarkvara, mida kasutatakse KNX-süsteemi projekteerimiseks, programmeerimiseks ja hooldamiseks. Tarkvara võimaldab kasutajatel projekteerida erinevaid KNX-süsteeme vastavalt hoone nõuetele ning programmeerida neid vastavalt hoone omaniku vajadustele. Lisaks sellele pakub ETS6 ka diagnostikavõimalusi, et tagada süsteemi töökindlus ja võimaldada süsteemi hooldust.

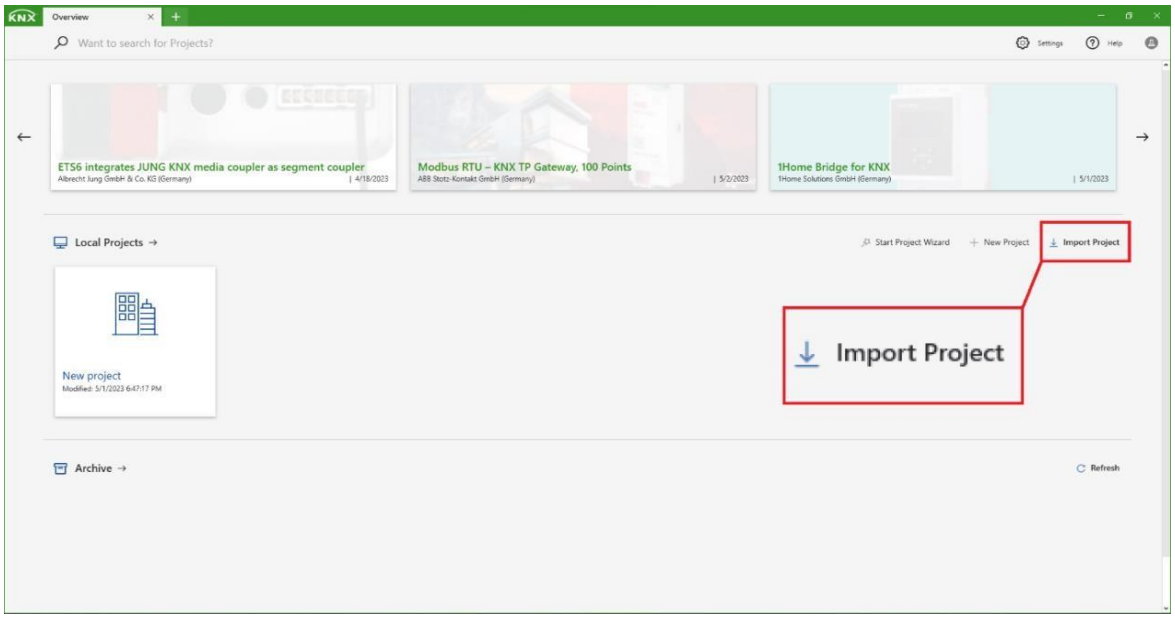
ETS6 tarkvara kasutamiseks on vaja litsentse, mis võimaldavad juurdepääsu erinevatele funktsioonidele ja võimalustele. Litsentse on kolme tüüpi:

1. ETS6 Demo litsents: ETS6 Demo litsents võimaldab kasutajal tutvuda ETS6 tarkvara põhifunktsioonidega. See on võimekuselt piiratud litsents, mis võimaldab kasutajal ühendada projektis mitte rohkem kui 5 seadet. Litsentsi kasutus on tasuta.
2. ETS6 Lite litsents: ETS6 Lite litsents on suurema funktsionaalsusega litsents, siiski on kasutavate seadme hulk piiratud 20 seadmega. Litsentsi hinnaks on 200€
3. ETS6 Professional litsents: See on täisfunktsionaalne litsents, mis võimaldab kasutajal juurdepääsu kõigile ETS6 tarkvara funktsioonidele. Litsentsi hinnaks on 1000€

Lõputöös tehtud näited baseeruvad ETS6 Demo litsentsil. [26]

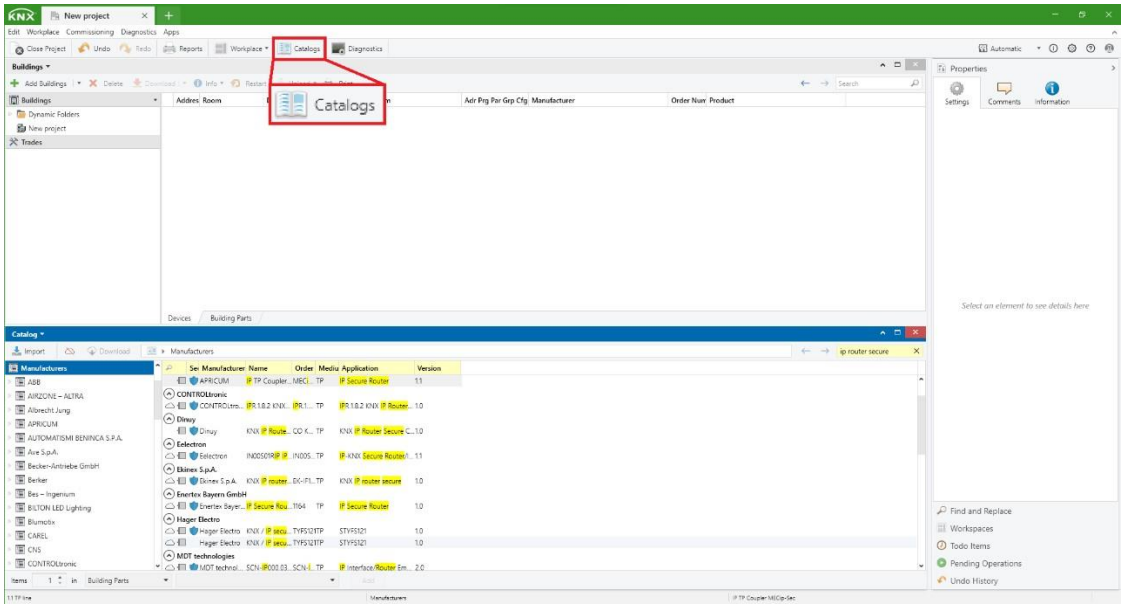
3.1 KNX Secure ETS6

KNX süsteemi kindlustamiseks KNX IP Secure lahendusega on vaja avada ETS6 rakenduses vajalik projekt. Selleks on võimalik kasutada nuppu „*Import Project*“ (vt Joonis 3.1) ning otsides ülesse projekt on võimalik seda avada ning alustada turvalahenduse seadistamisega.



Joonis 3.1 ETS6 käivitamise liides

Kui vajaminev projekt on avatud lisame projektile seadmete kataloogist meie poolt juba KNX süsteemi füüsiliselt paigaldatud IP Router’it, otsides üles selle mudeli nime või tellimisnumbri järgi (vt Joonis 3.2). ETS6 palub ruuteri lisamisel luua parool, mis kaitseks projekti ning ei võimalda seda avada teistel kasutajatel. Antud näites kasutame Controltroniku poolt toodetud IPR.1.8.2 KNX IP Router secure.

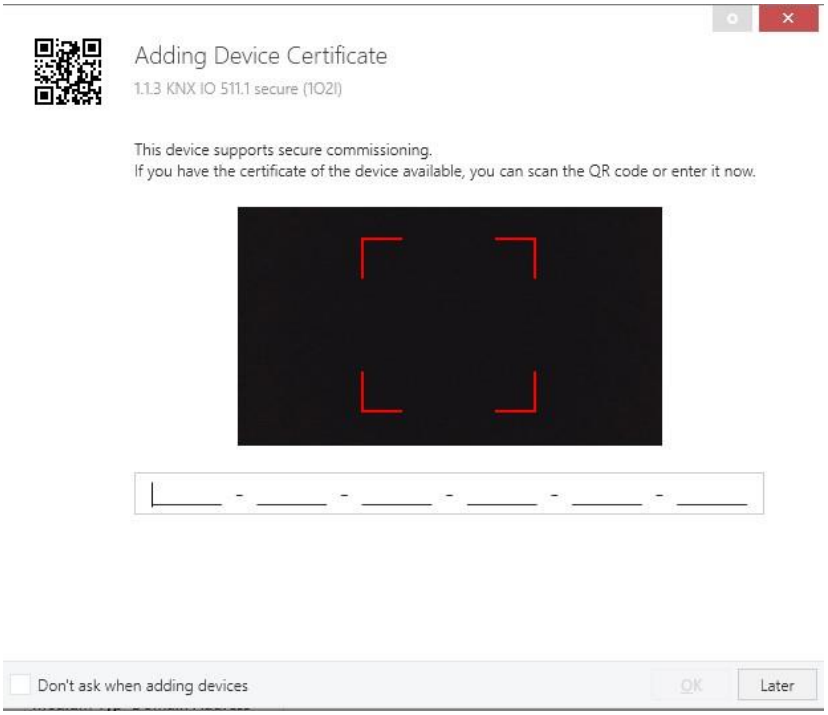


Joonis 3.2 seadmete valik kataloogist

Kui seade on lisatud, küsib ETS6 skaneerida või sisestada ruuteril olevat QR koodi seadme kinnitamiseks. Sellega on KNX IP Secure paigaldatud ETS6 tarkvaras. Ruuterit on võimalik seadistada vajutades selle peale topoloogia paneelil ning liikudes „Settings“ vahekaardile (vt Joonis 3.3), mis seadistab ruuterit või „IP“, kus on võimalik konfigureerida võrku.

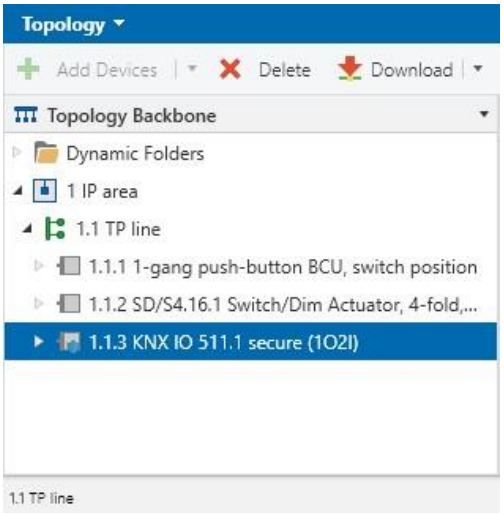
Joonis 3.3 seadmete seadistuse liides

KNX süsteemi kindlustamiseks KNX Data Secure lahendusega on projektile vaja lisada KNX Data Secure teenust toetavat täiturmooduli, milleks antud näite puhul oli valitud ettevõtte WEINZIERL ENGINEERING poolt toodetud „KNX IO 511.1 secure“. Seadme ühendamisel süsteemi, küsib tarkvara selle seadme aktiveerimiseks skaneerida või sisestada käsitsi QR kood (vt Joonis 3.4).



Joonis 3.4 Seadme QR koodi kaameraga skaneerimise aken

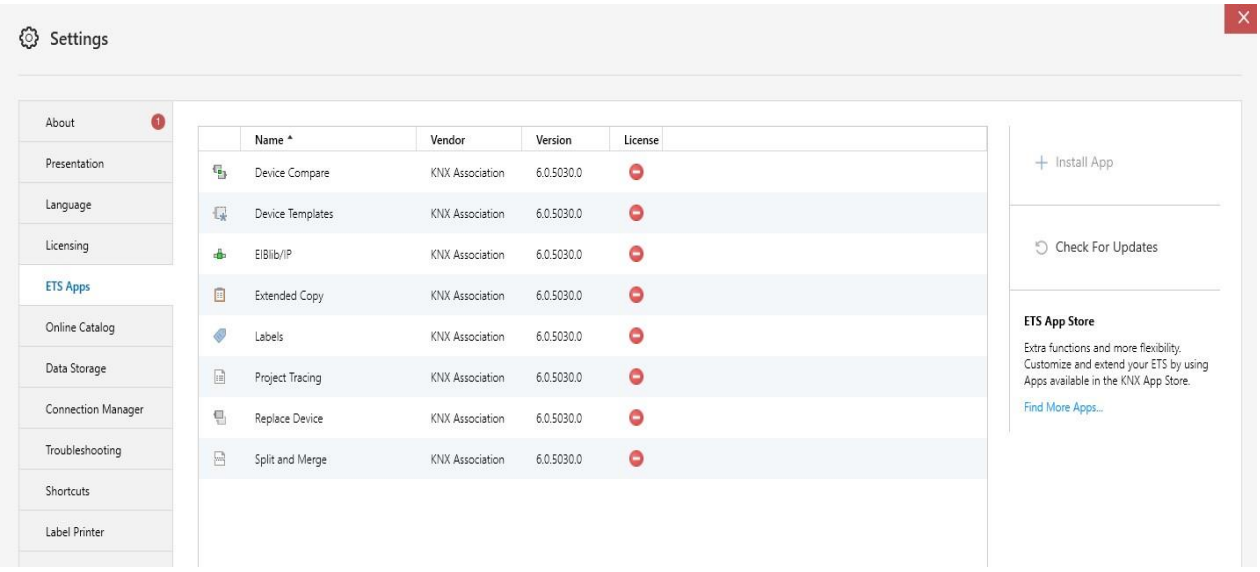
Seadme aktiveerimisel tuleb teda seadistada vastavalt tootja nõuetele. WEINZIERL ENGINEERING on seadistamise ja kasutamise manuaali paigaldanud oma koduleheküljele kasutamiseks. Manuaali täpsel jälgimisel ja KNX Data Secure seadistamisel on süsteemi turvalisus edukalt tõstetud.



Joonis 3.5 Näidisprojekti topoloogia

Edukal paigaldusel peab turvalise ühendusega seade olema nähtav vastaval liinil (vt Joonis 3.5). Selle peale vajutamisel ja seadetesse liikumisel on samuti nagu ka KNX IP Secure seadet võimalik seda konfigureerida vastavalt projekti nõuetele.

KNX Secure sertifikaatide haldustarkvara lisamiseks ja rakenduseks ETS6 tarkvaras on esiteks vaja vajaminev rakendus alla laadida. Rakendus „Service App“ toodetud ettevõtte Jung poolt tegeleb just nende ülesannetega ning on tasuta kättesaadav KNX Association koduleheküljel. Allalaadimisel on fail „ .etsapp“ formaadis, mis on loodud spetsiaalselt ETS6 tarkvara jaoks. Faili rakendamiseks ja kasutamiseks tuleb avada ETS6 rakendus ning leida seadetes koht nimega „ETS Apps“ (vt Joonis 3.6). [31]

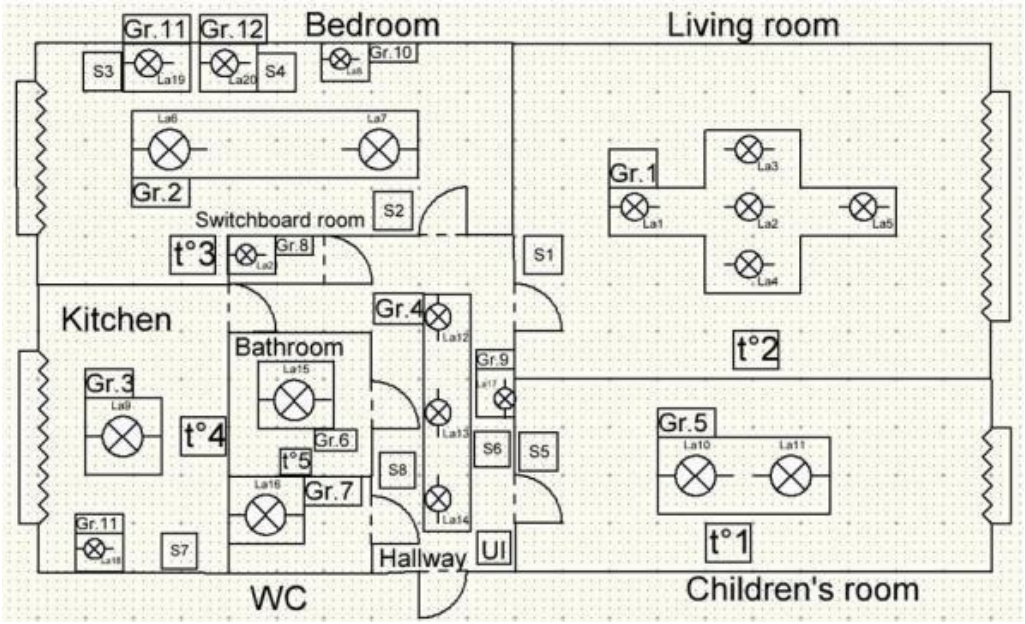


Joonis 3.6 ETS6 tarkvara laienduste liides

Siin on võimalik näha kõiki tarkvara laiendusi, mis on ETS6 põhivarale lisatud. „Service App“ installeerimiseks tuleb vajutada paremal nurgas olevat „Install App“ nuppu ning otsida juba varem allalaetud fail. Faili ülesleidmisel ning edukal installeerimisel lisandub ta olemasolevasse tarkvara laienduste nimekirja. Selle liidese kaudu on võimalik ka jälgida uuenduste tekkimist olemasolevate laienduste jaoks.

3.2 KNX Secure kasutamisest loobumise riskid

Olemasoleva lahenduse riskide hindamisel KNX Secure rakendamisest loobumise juhul, kasutame Tallinna Tehnikaülikooli üliõpilase poolt varem koostatud projekti [27] ning uurime KNX Secure vajadust. Koostatud projekt on kolmetoaline korter korrusmajas. Projektis kasutatud seadmed on toodetud erinevate tootjate poolt ja on standardi tõttu kokku sobivad üksteisega. Korter koosneb elutoast, magamistoast, lastetoast, köögist, WC, vannitoast, esikust ja kilbiruumist.



Joonis 3.7 korteri skeem [27]

Esimesena tuleb vaadata korteri turva nõudeid. KNX Secure on mõeldud tundlikute andmete kaitseks, mis liiguvad mööda KNX võrku. Antud juhul on tegemist väiksema korteriga, kus pahatahtlik ligipääs seadmetele ja andmetele poleks suurelt mõjutanud korteri elanike. Korteris reguleeritakse KNX võrgu kaudu toa temperatuure ning valgust. Seega pahatahtlikul juurdepääsul oleks ligipääs nendele seadmetele ning seadistustele. Juurdepääsu teostamiseks on vaja füüsilist juurdepääsu KNX võrgu liinile ja juba on võimalik andmeliikumist pealt

kuulata ning valesid signaale süsteemis ringi saata. Eluohtlikuks sellist olukorda nimetada ei saa. KNX secure kasutamine on siin pigem mitte vajalik. Vajalik oleks kasutada KNX Secure kui oleks tegemist kriitiliste andmetega, või kui ligipääs seadmetele riski seadnud suure hulga inimesi.

Järgmisena tuleb tähelepanu pöörata, kas korteril on turvalisuse nõrku kohti, mida on võimalik ära kasutada. Vaadates korteri plaani on näha, et kõik seadmed on paigaldatud korteri sisse ja KNX RF seadmeid ei kasutata. Lisaks sellele paikneb kilbiruum samuti korteris. Ükski seade või liides ei jää korterist välja. See tähendab, selleks et omada otsest ligipääsu seadmetele või kilbiruumile peab asuma korteri siseruumides. Korteri seadmed ja süsteemid pole ühenduses internetiga, seega ainuke viis kuidas neid mõjutada on otsese füüsilise juurdepääsuga. Antud juhtumil on korter välise pahatahtliku volitamata juurdepääsu eest kaitstud ning KNX Secure kasutus on mitte vajalik. Vajalik oleks kasutada KNX Secure't kui mõni seade või KNX moodulite elektrikilp, mis on KNX süsteemis turvalisuse poolest kõige nõrgem koht, paikneks korterist väljas. Kuna siis isegi omades ligipääsu kilbiruumile või seadmetele poleks võimalik mõjutada andmeid või neid pealt kuulata.

Korter omab ka väikse ründepindala kõigest 3 tuba, mida on võimalik lihtsasti jälgida ning kontrolli all hoida minimaalse valvesüsteemiga. Samuti mida väiksem on valvesüsteem seda vähem kohti omab ta potentsiaalseks rünnakuks. Kui oleks tegemist mitmekorruselise elamuga, kus kõik korrused oleksid ühendatud ühise KNX süsteemiga oleks ka ründepindala ka palju suurem ning füüsiliselt jälgida ning hoida ära rünnakuid oleks keerulisem. Lisaks muutuvad ka valvesüsteemid sellistes hoonetes palju keerulistemaks ja tähtsamateks osadeks. Mida suurem ja keerulisem on valvesüsteem, seda hoolikamalt tuleb seda kaitsta, kuna selline süsteem omab palju suuremat riski pahatahtlikuks rünnakuks. Sellistes hoonetes oleks KNX Secure kasutus vajalik.

Viimase sammuna tuleb vaadata süsteemi uuendamisega kaasnevaid kulusid. Siin tuleb arvestada olemasolevate seadmete värskendamise või ühildumatute seadmete asendamise rahalisi mõjusid. Tuleb hinnata aega ja ressursse, mis kuluvad süsteemi ümberprogrammeerimiseks ja uuesti konfigureerimiseks ning hiljem ka hooldamiseks. Vaadates seadmeid, mis on korteris välja toodud on neid võimalik integreerida KNX Secure süsteemi, lisaks oleks vaja paigalda uus täiturmooduli seade, mis toetab KNX Secure't.

Valitud sai ettevõtte WEINZIERL ENGINEERING poolt toodetud „KNX IO 511.1 secure". Tegemist on kompaktse lülitustoimelise väljundiga ja 2 binaarse sisendiga täiturmooduliga,

mis tähendab, et täiturmehhanism on universaalne ning on võimeline pakkuma väljundit näiteks küttesüsteemile või valgustusele. Mooduli sisendeid saab ühendada tavaliste lülititega 12V230V. Seade omab kahte nuppu ja kolme LED-i oleku näitamiseks. Mooduli paigalduse käigus on võimalik rakendada süsteemile KNX Secure.[30]

Seadme hinnaks on 110.80 €, mis tõstaks kogu süsteemi hinna 5% võrra. Kuna tegemist on väiksema korteriga siis süsteemi teisendamisprotsess ei nõuaks palju aega ja ressursse. Siiski kuna süsteemis on rohkem kui 5 seadet, aga vähem kui 20 siis pole võimalik see projekt teostada ETS6 demo litsentsiga. Kasutusse tuleb võtta kas ETS6 lite või ETS6 professional litsents. [27]

Seadme kirjeldus	Tootja	Mudel	Kogus	Tüki hind	Hind kokku
Toiteallikas	Phoenix Contact	2868635	1	27.64 €	27.64 €
Termostaat	MDT	SCN-RT1GS.01	5	168.00 €	840.00 €
Relee	EIBMARKET	SA.12.16	1	239.00 €	239.00 €
Drossel	Siemens	5WG1 120-1AB02	1	34.99 €	34.99 €
Dimmer	Inegenium	ING-KNX-RK3X500	2	129.00 €	258.00 €
Lüliti 2 nuppu	MDT	BE-TA5502.01	6	50.86 €	305.16 €
Lüliti 4 nuppu	MDT	BE-TA5504.01	2	57.47 €	114.94 €
Kasutajaliides	Ingenium	DS241X00	1	491.00 €	491.00 €
				Summa	2,310.73 €

Joonis 3.8 projekti seadmete kalkulatsioon [27]

4 KNX secure rakendamise vajadus elamus

KNX Secure'i kasutamine elamutes on tänapäeval üha olulisemaks muutunud, kuna turvalisus ja privaatsus on üha suurema tähtsusega. KNX Secure pakub täiendavat turvameedet KNX süsteemides, mis võimaldab kaitsta võrgus liikuvaid andmeid volitamata juurdepääsu ja manipuleerimise eest. Siiski ei ole KNX Secure alati vajalik ja selle kasutamine sõltub konkreetsest olukorrast. [4]

KNX Secure'i kasutamine on põhjendatud juhul, kui andmete kaitse ja privaatsus on elanike ja vara kaitse seisukohast kriitilise tähtsusega. See on eriti oluline elamutes, mis asuvad kõrgema turvariskiga piirkondades või kus on olemas potentsiaalsed välised ohud, nagu hooneautomaatika ühendus välise võrguga, näiteks Internetiga. KNX Secure'i kasutamine võimaldab kaitsta süsteeme, milleks on näiteks turvasüsteemid ja valveseadmed tagades nende konfidentsiaalsuse. [4], [8].

Peatükkis 4.1 tuuakse täpsemaid näiteid KNX Secure kasutamise põhjendustest seletades paremini lahti ülaltoodud näiteid.

Siiski on KNX Secure'i kasutamine mittevajalik, kui turvariskid on madalad või kui elamu KNX võrk on isoleeritud ilma välise võrguühenduseta. Kui tundlike andmete töötlemine puudub ja turvalisus ei ole prioriteet, võib standardne KNX-protokoll olla piisav andmeedastuseks ja juhtimiseks. Lisaks tuleb arvestada ka kuludega, mis võivad kaasneda KNX Secure'i rakendamisega seotud seadmete, litsentside ja turvameetmete soetamisel. [4], [10]-[13].

Peatükkis 4.2 seletatakse lahti punkte millele tuleb tähelepanu pöörata et paremini mõista, miks KNX Secure kasutus pole alati vajalik.

4.1 KNX Secure kasutamise põhjendus

Elanike turvalisus on üks olulisemaid aspekte, mida tuleb kaaluda KNX Secure'i kasutamisel elamute hoonetes. KNX Secure'i kasutamine on vajalik, kui elanike andmete kaitse ja privaatsus on kriitilise tähtsusega. See kehtib eriti elamute puhul, mis võivad asuda kõrgema turvariskiga piirkondades või milles on palju kallist vara, mida tuleb kaitsta, nagu näiteks luksuslikud kodud, villad või häärberid. Turvasüsteemide, valvesüsteemide ja juurdepääsukontrolli andmete krüpteerimine võimaldab vältida volitamata juurdepääsu ja manipuleerimist, tagades elanike ohutuse.

KNX Secure'i kasutamine on oluline juhul, kui elamus on kasutusel kõrgema turvariskiga sisenemiskontrollisüsteem. Sellised süsteemid võivad hõlmata näiteks elektroonilisi lukke, kaardilugejaid või sõrmejäljelugejaid, mis kontrollivad juurdepääsu hoonetele, korteritele või teatud piirkondadele. KNX Secure tagab, et hooneautomaatika süsteemi andmed omavahelisel suhtlusel on krüpteeritud ja kaitstud volitamata juurdepääsu eest.

KNX Secure'i kasutamine on vajalik ka siis, kui elamus on paigaldatud valvesüsteemid. Valvesüsteemid hõlmavad tavaliselt andurite, signaalide ja teavitustegevuste kompleksi, mis annavad märku võimalikest hädaolukordadest, nagu tulekahju, sisse tungimine või gaasileke. KNX Secure tagab, et alarmsüsteemi andmeedastus on turvaline ja kaitstud volitamata juurdepääsu eest, tagades elanikele täiendava turvatunde.

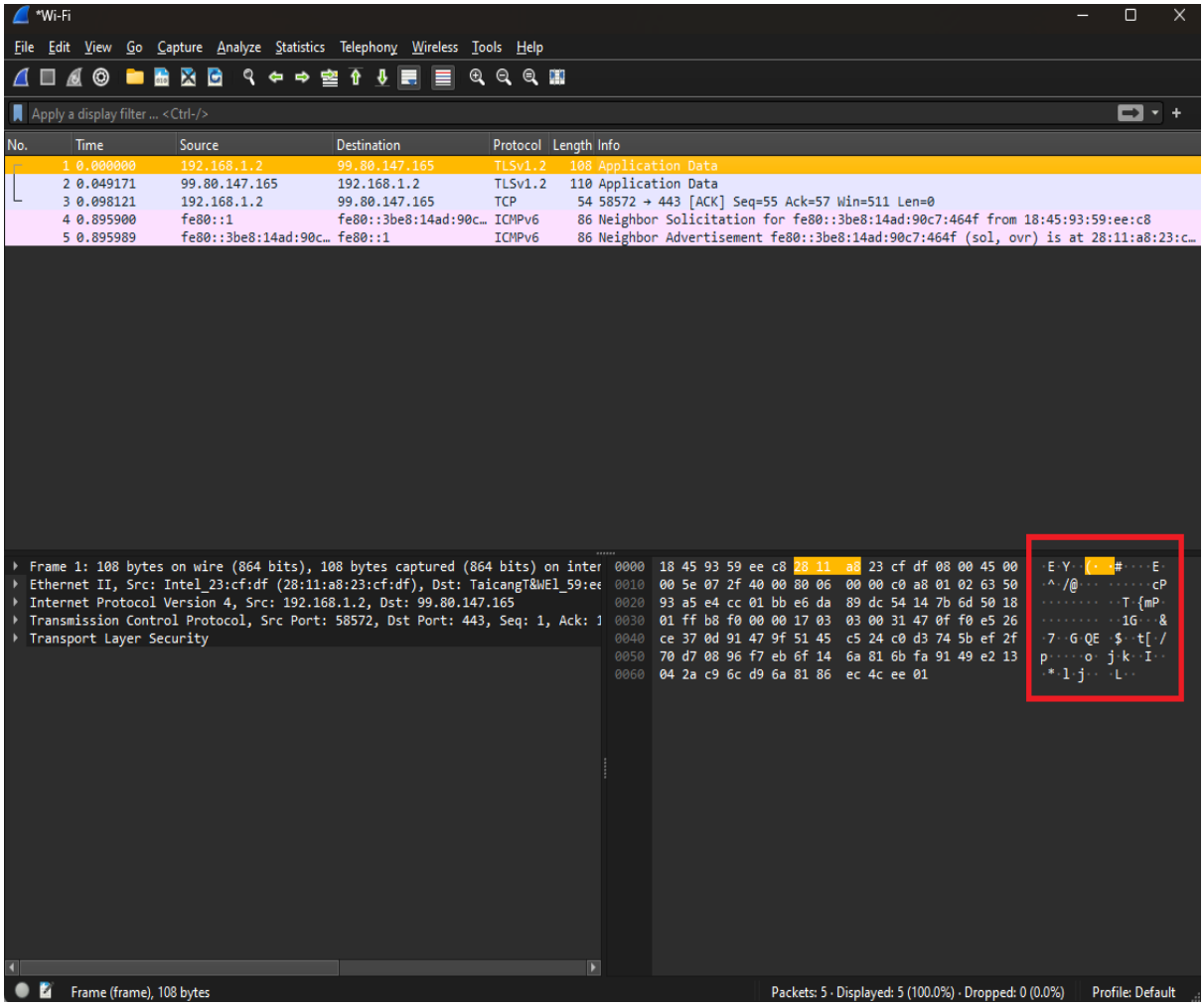
Hoonesüsteemide admeside ühendused väljaspoole hoonet on veel üks oluline tegur, mida tuleb arvestada KNX Secure'i kasutamisel elamute hoonetes.

Kui elamus on KNX võrk ühendatud pilveteenustega või kasutatakse pilvepõhiseid lahendusi, on KNX Secure vajalik samadel põhjustel. Pilveühendus võib avada ukse volitamata isikutele, kes püüavad saada juurdepääsu võrgule või seadmetele. KNX Secure tagab, et andmeedastus pilve kaudu on turvaline, krüpteeritud ja kaitstud volitamata juurdepääsu eest. Turul eksisteerib isegi sellele teenusele spetsialiseerunud ettevõtteid, näiteks CannX, kes tegeleb KNX ruuterite paigaldusega ja pilvevõrgu kaitsega. [29]

KNX Secure on vajalik elamuse suhtlemisel teiste süsteemidega, näiteks turvasüsteemide, videovalve süsteemide või automatiseeritud kodu lahendustega. Sellised integratsioonid loovad potentsiaalseid turvariske, kuna volitamata isikud võivad püüda saada juurdepääsu või manipuleerida erinevaid süsteeme. KNX Secure tagab turvalise andmeedastuse ja autentimise, hoides volitamata juurdepääsu kontrolli all. [28]

Tavalist KNX süsteemi on võimalik peat kuulata omades seadet, milleks on arvuti vajaliku tarkvaraga ning omada ühendust KNX võrguga. KNX võrgu pakettide vaatamise tarkvaraks võib kasutada näteks „Wireshark“[32] tarkvara, mis on tasuta kättesaadav ning tegeleb andmepakettide analüüsiga. Esimeseks sammuks ühenduse seadistamine seadme ja KNX võrgu vahel. Ühenduse saamisel tuleb käivitada pealtkuulamis tarkvara ning alustada võrguliikluse jälgimist. Liikluse kuulamine on edukalt sooritatud ning nüüd on võimalik jälgida andmepakette mida saadetakse süsteemis ringi. Kui võrgul on rakendatud Secure lahendus siis võrguliikluse pealtkuulamisel on pakette võimalik lugeda, kuid kuna nad on krüpteeritud siis

mis on nende andmepakettides kirjas pole võimalik arusaada. Ainult määratud vastuvõtjal on privaat võti, mille abil on võimalik andmeedastus paketi sisu loetavaks muuta. Sellise krüpteerimise tagajärjel muutub andmete ülekuulamine kasutuks isegi otsese ühenduse omamisel. [5], [17]



Joonis 4.1 Wireshark tarkvara kasutajaliidese aken

Joonisel 4.1 on toodud ette näide „Wireshark“ tarkvara kasutajaliidesest. Antud näites on toodud seadme milleks on arvuti ühendus välismaailmaga kasutades Wi-Fi. Selline ühendus kasutab samuti turvalisuseks TLS protokolli nagu ka KNX Secure seepärast sobib. Nagu on kasutajaliidesest näha, ühenduse loomisel on võimalik täpselt määrata aeg millal toimus andmeedastus, kust need andmed tulid ja kuhu läksid. Kuid tänu sellele, et andmed on krüpteeritud kõige tähtsam osa ehk andmepaketti sisust pole võimalik arusaada. Joonisel on andmepaketti sisu määratud punasega.

4.2 KNX Secure-ta lahendused

Kui elamu asub rahulikus piirkonnas, kus pahatahtlik füüsiline sekkumine andmeedastus kanalisse on vähema tõenäosusega, võib KNX Secure'i täiendava turvalisuse kasutamine olla vähem oluline. Siiski tuleks arvestada mõningate täiendavate aspektidega, et teha põhjendatud otsus.

Enne otsuse tegemist võib olla kasulik koguda statistikat või läbi viia turuanalüüs piirkonna turvalisuse kohta. See hõlmab kuritegevuse määra, varguste arvu, vandalismi juhtumeid ja muid turvalisust puudutavaid tegureid. Kui piirkond on tuntud oma turvalisuse poolest ja turvariskid on väga madalad, võib standardse KNX-protokolli kasutamine olla piisav. Samuti kui piirkond on tuntud naabrivalve algatuste või turvateenuste olemasolu poolest, võib see mõjutada KNX Secure'i vajadust. Sellised meetmed võivad juba pakkuda piisavat turvalisust ja jälgimist, vähendades seeläbi täiendava krüpteerimise vajadust KNX süsteemis. Siiski võib ründeohu suurus sõltuda ka isiku taustast. Kui on küberkurjategijatel persooni vastu huvi tõstab see eluasemes KNX Secure kasutamis vajadust. [4], [10]-[13]

Kui elamus puuduvad süsteemid, mis reageerivad erinevatele tingimustele või teguritele, milleks võivad olla, näiteks turvasüsteemid, keskkonnajuhtimissüsteemid või andmed, mis vajavad täiendavat turvalisust, võib KNX Secure'i kasutamine olla valikuline, mis tähendab, et kuna KNX Secure koosneb mitmetest osadest siis kasutusse võib võtta ka ainult vajalik kindel osa sellest süsteemist, näiteks IP võrgu kaitsmise soovi korral võib kasutusse võtta KNX IP Secure, mis täidaks selle rolli. Kui elamus ei ole paigaldatud spetsiifilisi turvasüsteeme, näiteks sissepääsu kontrollsüsteemid, valvekaamerad või häirete haldus süsteemid, võib KNX Secure'i kasutamine olla vähem oluline. Selliste süsteemide puudumisel on tõenäosus volitamata juurdepääsuks ja andmete manipuleerimiseks väiksem.

KNX Secure'i rakendamine on vähem oluline kui elamus on juurdepääsu ja seadme kasutamise osas range kontroll ning ainult usaldusväärsed isikud saavad võrku ja süsteeme juhtida. Näiteks kui ainult elanikud ise või usaldusväärsed teenusepakkujad omavad juurdepääsuõigusi ja volitusi KNX võrgule. [4], [10]-[13], [28]

KNX Secure'i rakendamine toob kaasa lisakulusid, mis hõlmavad seadmete, litsentside ja turvameetmete omandamist. KNX Secure'i kasutamiseks tuleb vajalikuks osutuda uuemate ja turvalisemate seadmete soetamine või olemasolevate seadmete tarkvarauuendused. Need seadmed peaksid vastama KNX Secure'i nõuetele ja

samuti ka spetsiifilistele turvafunktsioonidele, mis suurendavad nende hindu võrreldes standardsete KNX-seadmetega.

KNX Secure'i nagu ka muude turvatud andmesidega lahenduste, näiteks Zigbee ja Z-Wave kasutamine nõuab täiendavaid turvameetmeid, näiteks tulemüüre või VPN-lahendusi, mis tagavad võrgu ja seadmete kaitset kui seadmeid kasutatakse olulistes süsteemides või hoonetes, kus rünnaku oht on suurem ning võib ohustada inimelusid. [4]

KNX Secure'i rakendamine toob kaasa täiendavaid haldamiskulusid, sealhulgas turvakonfiguratsioonide seadistamist ning regulaarsed turvaauditi läbiviimist. Need kulud võivad tuleneda spetsialistide töötundidest, kes vastutavad turvalisuse tagamise eest, ning võivad olla pikaajalised kulud võrgu turvalise toimimise tagamiseks. [4], [10]-[13]

Kokkuvõte

Käesoleva töö raames on antudd põhjalik ülevaade KNX Secure autentimis- ja autoriseerimismehhanismidest ning nende olulisustest hoonete automatiseerimise ja juhtimissüsteemide turvalisuse tagamisel. Samuti on tehtud ülevaade KNX Secure rakendusest elamutes koos kasutamata jätmise riskide avamisega, vastates küsimustele millistes olukordades on KNX Secure kasutus vajalik ning millistes olukordades on mitte vajalik. Lisaks on tehtud ülevaade KNX-st ning tema lähimatest konkurentidest koduautomaatikas, tuues välja nende positiivseid ning negatiivseid külgi.

Töö tulemusena on näidatud KNX Data Secure ja KNX IP Secure paigaldust valitud seadmetega. Näidatud on ka nende seadmete haldusvõimalus ETS6 tarkvaras. Esitatud on ka sertifikaatide haldamis programmi paigaldamise näidis, koos selle haldusvõimalusega. Samuti saab töö tulemusena väita, et KNX Secure'i rakendamine pakub olulisi eeliseid, kuna see võimaldab krüpteeritud andmeedastust ja autentimist KNX-seadmete vahel, mis aitab vältida volitamata juurdepääsu KNX hooneautomaatika võrgule isegi omades otsest ühendust ja kasutades ülekuulamis programme. Siiski ei pruugi KNX Secure kasutus olla alati vajalik ja sõltub elamus kasutatavate tehniliste süsteemide lahendustest.

Väiksemates elamudes, kus süsteem on välise ligipääsu eest kaitstud ning mille võrgu kaudu ei liigu kriitilisi andmeid pole ilmtingimata vajalik rakendada KNX Secure süsteem. KNX Secure süsteemi paigaldus nõuab teadmisi, ressursse ning aega, mis võib ennast lõppkokkuvõttes mitte ära tasuda. Lisaks nõuab KNX süsteemi muutmine KNX Secure lahendusele süsteemi sobivate seadmete kasutust ning hooldamist, mis võib tekitada elamu omanikul täiendavaid kulutusi. Suuremates elamudes, kus ligipääs seadmetele pole nii kaitstud ning kus andmelekke võib põhjustada palju rohkem probleeme on KNX Secure kasutus vajalik, kuna tõstab elamu turvalisuse taset.

Antud lõputöö teemat on võimalik edasi arendada uurides, millised vabavaralised tarkvarad KNX Securet toetavad ja kuidas nende vaheline suhtlus toimib. Täiendavalt on võimalik vaadelda KNX RF juhtmevabade moodulite kasutamisel tekkivat erisust, pöörates tähelepanu KNX RF Multi S-mode uutele seadmetele, kus KNX Secure on kohustuslikult sees.

KASUTATUD KIRJANDUSE LOETELU

[1] Merz, H., Hansemann, T., Hübner, „C. Building Automation: Communication systems with EIB/KNX, LON, and BACnet“, Berlin, 2009

[2] „KNX Advanced Course Documentation: (1st revised revision)“, KNX Association, 2019

[3] „KNX - the secure solution for your smart building,“ [Võrgumaterjal]. Saadaval: https://www.knx.org/knx-en/for-professionals/benefits/knx-secure/index.php (02.04.2023)

[4] „KNX Online Training Platform,“ [Võrgumaterjal]. Saadaval: https://wbt6.knx.org/mod/scorm/player.php?a=30&currentorg=Rustici%20Software&scoid =498 (05.04.2023)

[5] „KNX Secure Offers Maximum Data Protection for Smart Buildings,“ [Võrgumaterjal]. Saadaval: https://www.knxtoday.com/2017/10/10334/knx-secure-offers-maximum-data-protection-for-smartbuildings.html (05.04.2023)

[6] „KNX Secure – maximum data protection for smart buildings,“ [Võrgumaterjal]. Saadaval: https://www.knx.org/wAssets/docs/downloads/Marketing/Flyers/KNX-News/KNX-News_en.pdf (05.04.2023)

[7] „Interview: Joost Demarest on KNX Secure,“ [Võrgumaterjal]. Saadaval: https://www.knxtoday.com/2018/07/11980/interview-joost-demarest-on-knx-secure.html (07.04.2023)

[8] „KNX Secure – The new era of security for smart homes and buildings,“ [Võrgumaterjal]. Saadaval: https://www.knxtoday.com/2018/11/12702/knx-secure-the-new-era-of-security-for-smart-homes-andbuildings.html (07.04.2023)

[9] „Programming Tips: KNX Secure,“ [Võrgumaterjal]. Saadaval: https://www.knxtoday.com/2019/03/13317/programming-tips-knx-secure.html (07.04.2023)

[10] „KNX Secure Day - 3. First KNX Panel Discussion,“ [Võrgumaterjal]. Saadaval: https://www.youtube.com/watch?v=2UYZf5jEIBQ&list=PL9NWvz0cOjNMks2z8wvvw1TMSk4bDBWhD&index=3 (08.04.2023)

[11] „KNX Secure Day - 4. Interview Per Melander (KNX Sweden),“ [Võrgumaterjal]. Saadaval: https://www.youtube.com/watch?v=wLECmk6jX70&list=PL9NWvz0cOjNMks2z8wvvw1TMSk4bDBWhD&index=5 (09.04.2023)

[12] „KNX Secure Day - 7. Second KNX Panel Discussion,“ [Võrgumaterjal]. Saadaval: https://www.youtube.com/watch?v=KPes7qf64Qs&list=PL9NWvz0cOjNMks2z8wvvw1TMSk4bDBWhD&index=7 (09.04.2023)

[13] „KNX Secure Day - 8. Interview Mark Warburton (KNX UK),“ [Võrgumaterjal]. Saadaval: https://www.youtube.com/watch?v=mJ9zt6dtVKY&list=PL9NWvz0cOjNMks2z8wvvw1TMSk4bDBWhD&index=8 (09.04.2023)

[14] „KNX Association Offers KNX IP Secure and KNX Data Secure for Secure Access to Installations,“ [Võrgumaterjal]. Saadaval: https://www.knxtoday.com/2016/03/7630/knx-association-offers-knx-ipsecure-and-knx-data-secure-for-secure-access-to-installations.html (10.04.2023)

[15] Hugo Krawczyk, Kenneth G. Paterson, Hoeteck Wee, „On the Security of the TLS Protocol: A Systematic Analysis“, Springer, 2013

[16] „What is Certificate-Based Authentication?,“ [Võrgumaterjal]. Saadaval: https://www.yubico.com/resources/glossary/what-is-certificate-based-authentication/#:~:text=Certificate%2Dbased%20authentication%20is%20a,each%20other%20across%20a%20network. (13.04.2023)

[17] Andrey Bogdanov , Dmitry Khovratovich, Christian Rechberger, „Biclique Cryptanalysis of the Full AES“, Springer, 2016

[18] „What is AES Advanced Encryption Standard?,“ [Võrgumaterjal]. Saadaval: https://www.wallarm.com/what/what-is-aes-advanced-encryption-standard (13.04.2023)

[19] „KNX Data Secure system documentation,“ [Võrgumaterjal]. Saadaval: https://partner.gira.com/data3/KNX_Data_Secure_Systemdokumentation _en.pdf (13.04.2023)

[20] Salim Jibrin Danbatta, Asaf Varol, „Comparison of Zigbee, Z-Wave, Wi-Fi, and Bluetooth Wireless Technologies Used in Home Automation“, IEEE, 2019

[21] R. Housley, W. Ford, W. Polk, „Internet X.509 Public Key Infrastructure Certificate and CRL Profile“, NIST, 1999

[22] Christian Paetz, „Z-Wave Essentials: Interoperability in Smart Homes 3rd Edition“, CreateSpace Independent Publishing Platform, 2013

[23] Alina Bradford, “What’s the Difference between Zigbee and Z-Wave?”, Safewise, 25.04.2023

[24] Chef Gadget-Freak, How to improve your Zigbee network, Gadget-Freakz, 2019

[25] Wolfgang Granzer; Christian Reinisch; Wolfgang Kastner, “Future challenges for building automation: Wireless and security”, IEEE, 2010

[26] „KNX Virtual shop software,“ [Võrgumaterjal]. Saadaval: https://my.knx.org/en/shop/software?page=1 (17.04.2023)

[27] „Kodu juhtimise lahendused KNX’iga,“ [Võrgumaterjal]. Saadaval: https://digikogu.taltech.ee/et/Item/b117b00c-8c7c-47d0-bf58-510864ecc608

[28] Osmo Sarjakoski, Designing a KNX-house Automation System for a private residence, Helsinki Metropolia University of Applied Sciences, 2015

[29] „CannX: Why Kloud'nX?,“ [Võrgumaterjal]. Saadaval: https://can-nx.com/en/kloudnx-knx-iotrouter-connects-to-a-secure-cloud/ (17.04.2023)

[30] „KNX IO 511.1 SECURE (1O2I),“ [Võrgumaterjal]. Saadaval: https://weinzierl.de/en/products/knxio-511-1-secure/ (12.05.2023)

[31] „Shop ETS Apps,“ [Võrgumaterjal]. Saadaval: https://my.knx.org/en/shop/etsapps?product_type=service-app-1 (13.05.2023)

[31] „Wireshark,“ [Võrgumaterjal]. Saadaval: https://www.wireshark.org/ (13.05.2023)

[32] „ETS6 integrates JUNG KNX media coupler as segment coupler,“ [Võrgumaterjal]. Saadaval: https://www.knxtoday.com/2023/03/45837/ets6-integrates-jung-knx-media-coupler-as-segmentcoupler%EF%BF%BC.html (13.05.2023)

[33] „Overview: Why the Use of KNX RF is Growing,“ [Võrgumaterjal]. Saadaval: https://www.knxtoday.com/2018/09/12225/overview-why-the-use-of-knx-rf-is-growing.html (13.05.2023)