OULUN AMMATTIKORKEAKOULU

Samuli Ikäläinen

LTE-M-VERKKOKOMMUNIKAATION ANALYSOINTI JA ANALYSOINNIN AUTOMATISOINTITYÖKALU

LTE-M-VERKKOKOMMUNIKAATION ANALYSOINTI JA ANALYSOINNIN AUTOMATISOINTITYÖKALU

Samuli Ikäläinen
Opinnäytetyö
Syksy 2024
Tieto- ja viestintätekniikka
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tieto- ja viestintäteknologia, ohjelmointi puoli

Tekijä(t): Samuli Ikäläinen
Opinnäytetyön nimi: LTE-M-verkkokommunikaation analysointi ja analysoinnin automatisointi työkalu
Työn ohjaaja(t): Manne Hannula
Työn valmistumislukukausi ja -vuosi: Syksy 2024
Sivumäärä: 25

Työn aiheena oli Anicare Oy:n LTE-verkkoa käyttävän Rudolf -laitteen testaaminen ja ajaminen, jotta saataisiin dataa verkkokommunikaatiosta löytyneisiin ongelmakohtiin sekä löydettäisiin mahdollisia uusia ongelmia. Sen lisäksi työssä oli lopputavoitteena saada koodattua ohjelma, joka voisi automatisoida tämän datan keruun ja seulonnan. Työssä käytettiin erikseen testaukseen tehtyä Rudolf -laitetta, jota ajettiin 24 - 48 tunnin testi jaksoissa, sekä Wireshark -ohjelmistoa, jota käytettiin kyseisten testijaksojen datan analysointiin ja seurantaan. Testaus suoritettiin Anicare Oy:n toimiston testaustiloissa.

Työn lopputulokseksi saatiin toimiva ohjeistus tulevia testauksia varten, minkä avulla henkilö, joka ensimmäistä kertaa olisi tekemisissä verkkokommunikaation kanssa, pystyisi suorittamaan testaukset ongelmitta. Sen lisäksi saatiin valmiiksi testauksen automatisointia varten luotu ja toimivaksi todettu testausohjelma.

Asiasanat: Matkapuhelinverkot, testauslaitteet, testausmenetelmät, esineiden internet, langaton tiedonsiirto, langattomat verkot, TCP/IP

ABSTRACT

Oulu University of Applied Sciences
Information technology, software

Author(s): Samuli Ikäläinen
Title of thesis: LTE-M network communication analysis and analysis automation tool
Supervisor(s): Manne Hannula
Term and year when the thesis was submitted: Fall 2024
Number of pages: 25

The subject of this thesis was to test Anicare company's Rudolf -device and its network communication with the company's servers, and to write a guide for the testing. In this testing the main objective was to find key problem points from the communication, and then code a python script to do this automatically by examining pcapng-files generated by the network communication.

The equipment used in the thesis were a special Rudolf testdevice, which was run in 24 to 48 hour test periods, and Wireshark for capturing those communication data which would travel between the device and the server in these tests. Testing was performed in Anicare's own testing environment.

The end results were a successful guide and a working code for the error debugging.

Keywords: Cellular network, testing method, testing device, IoT, wireless communication, wireless network, TCP/IP

SISÄLLYS

1 JOHDANTO

Opinnäytetyön aiheena toimii LTE-M-verkkokommunikaation seuraaminen, sen analysointi sekä lopuksi analysoinnin automatisointia varten luodaan oma työkalu. Työ suoritetaan Anicare Oy:lle tehtynä. Anicare Oy on oululainen teknologiayhtiö, joka valmistaa IoT-laitteita eläinten paikkatietojen ja terveyden seurantaan. LTE-M-verkkokommunikaatiota seurattiin Anicare Oy:n Rudolf-laitteesta muokatulla testilaitteella sekä Wireshark-ohjelmistolla. Työn tavoitteena on saada havaittua LTE-M-verkokkokommunnikaatiossa Rudolf-laitteiden ja Anicaren servereiden olevia mahdollisia ongelmakohtia, ja jos mahdollista, löytää niihin korjausvaihtoehtoja. Työn haluttiin myös olevan eräänlainen opas tuleville tekijöille verkkokommunikaation seurantaan tulevaisuudessa.

Työn alkuperäinen idea lähti liikkeelle tavoitteena saada replikoitua tietyntyyppinen vikatila, joka oli aiheuttanut aikaisemmin laitteiden katoamista kenttäolosuhteissa, mutta valitettavasti tätä kyseistä tilannetta ei saatu, lukuisten testausjaksojen suorittamisesta riippumatta, toistettua testausolosuhteissa.

Työ suoritetaan suurimmalta osin Anicare Oy:n omissa testausolosuhteissa, ja testausvälineiden avulla koetetaan luoda mahdollisimman autenttinen olosuhde, joka vastaisi laitteen normaalia kiinnityspaikkaa eläimillä. Työhön tarvittavat fyysiset välineet saadaan myös käyttöön yrityksen tiloissa.

2 LTE-M-VERKKO JA NB-IOT

Tässä opinnäytetyössä työskennellään verkkokommunikaation parissa, suurimmaksi osaksi LTE-M-verkon kanssa, mutta myös NB-IoT-verkon toimintaa seurattiin testausten ja analysoinnin aikana, koska Anicare Oy:n Rudolf -laite tukee molempia verkkotyyppejä.

2.1 LTE-M-verkot yleisesti

LTE-M (Machine Type Communication) on LTE-teknologiaan (Long Term Evolution) perustuva verkko, joka on suunniteltu erityisesti IoT-laitteiden tarpeisiin. Se tarjoaa kattavan langattoman kuuluvuuden, alhaisen virrankulutuksen, ja kyvyn tukea suurta määrää laitteita samanaikaisesti. LTE-M-verkkoa käytetään laajasti erilaisissa IoT-sovelluksissa, esimerkiksi älymittareissa, seurantalaitteissa (kuten esimerkiksi juuri tässä opinnäytetyössä pääroolissa oleva Rudolf -laite) ja joissain teollisuuden sensoriverkoissa. Monissa maissa se on myös maatalouden käytössä, koska se on edullinen vaihtoehto viljelykasvien ja viljelymaan seurantaan. (1.)

LTE-M-kommunikaatio on myös erittäin yhteensopiva TCP/TLS-protokollien kanssa, jolloin sen toimivuus yleisten turvallisuus- ja autentikaatiomenetelmien kanssa on helppoa. Silti UDP on suositeltava vaihtoehto, jos haluaa mahdollisimman pitkän eliniän laitteelle joka käyttää LTE-M-kommunikaatiota. Tämä on sen ansiosta, että UDP:ssä ei käytetä TCP-kommunikaatiossa käytettäviä datan siirron varmistusmenetelmiä. (1.)

2.2 NB-IoT-verkko yleisesti

NB-IoT (Narrowband Internet of Things) on toinen LTE-teknologiaan perustuva verkko, jota käytetään myös suurimmalta osin IoT-laitteiden käyttöön. Missä se eroaa LTE-M-verkosta, on pidemmät viiveajat, ja se ei pysty LTE-M-verkon tapaan siirtymään paikasta toiseen datayhteyden katkeamatta. Etuina sillä ovat vähäisempi energiankulutus, sekä parempi kuuluvuus haasteellisissa kuuluvuusalueissa. NB-IoT-laitteet pystyvät ottamaan yhteyttä esimerkiksi maakellareista, joista muun muassa matkapuhelimilla ei välttämättä saisi minkäänlaista yhteyttä. (2.)

NB-IoT toimii siten, että se käyttää matalan taajuuden signaaleja, joilla se kommunikoi jo olemassa olevien LTE- ja GSM-teknologioiden kanssa. Sen standardi taajuus on 200 kilohertsiä, joka on suunniteltu juuri IoT-kommunikaatioiden käyttämistä varten. NB-IoT on myös täysin kykenevä toimimaan muiden verkkojen rinnalla, kuten 2G, 3G, 4G, 5G ja LTE-M. (3.)

3 WIRESHARK JA CELLULAR MONITOR

Wireshark on pakettianalysaattori, jonka avulla on mahdollista kaapata, tallentaa ja analysoida tietoliikennettä. Se tunnettiin ensimmäisessä versiossaan nimellä Ethreal, jonka loi alun perin Gerald Combs vuonna 1998. Nykyiseen Wireshark versioon se kehitettiin ja julkaistiin vuonna 2008, yli kymmenen vuoden jatkokehittämisen jälkeen. (4.)

3.1 Wireshark yleisesti

Wireshark on verkkoliikenteen analysointityökalu, josta näkee esimerkiksi lähettäjän ja vastaanottajan IP-osoitteen, portin, datamäärän, datasisällön, sekä kommunikaatioprotokollan. Lisäksi se informoi pakettien sisällöstä niiden jokaisen yksilöllisen tietosisällön, joka kattaa esimerkiksi Flag-osaston, mikä kertoo onko paketti esimerkiksi SYN, ACK tai muu vastaava kommunikaatiopaketti. Näistä kerrotaan lisää luvussa 4.

Wireshark tarjoaa myös mahdollisuuden reaaliaikaiseen verkkoliikenteen seurantaan ja tallennukseen, mikä tekee siitä erityisen hyödyllisen työkalun verkon ongelmien vianmäärityksessä. Ohjelma tukee laajaa valikoimaa eri protokollia, kuten projektissa käytettävää TCP-protokollaa, UDP-protokollaa, ICMP-protokollaa ja monia muitakin viestintä protokollia. Yksi Wiresharkin eduista on myös sen kyky suodattaa ja korostaa tiettyjä paketteja tai liikennettä, jolloin käyttäjä voi keskittyä analysoimaan tarkasti tietyntyyppistä liikennettä tai etsimään spesifejä ongelmia, kuten pakettien uudelleenlähetyksiä tai viivästyksiä, joista kerrotaan lisää luvussa 5.

Wiresharkissa on myös tehokkaat analyysityökalut, jotka auttavat käyttäjää visualisoimaan ja ymmärtämään tietoliikennettä. Esimerkiksi ohjelma tarjoaa tilastotyökaluja, joiden avulla voi tarkastella liikenteen jakautumista eri protokollien kesken, mikä helpottaa erityisesti suurten ja monimutkaisten verkkojen analysointia. Lisäksi Wireshark tukee verkkotallenteiden (.pcap ja .pcapng) vientiä ja analysointia myöhemmäksi, mikä mahdollistaa tietoliikenneanalyysin jälkikäteenkin. (5.)

3.2 Wiresharkin käyttö opinnäytetyössä

Wiresharkin käyttö opinnäytetyön aikana keskittyi pääsääntöisesti testilaitteen ja serverin välisen kommunikaation datan muuttamiseen lukemis- ja tutkimiskelpoiseen muotoon. Data kerättiin pcapng-tiedostomuotoon (joka on Wiresharkin oletusdatatyyppi), jolloin se pystyttiin avaamaan wiresharkin avulla selvästi tutkittavaan muotoon. Wiresharkin avulla voidaan myös avata tarkempia informaatioikkunoita jokaiselle yksittäiselle paketille.

Wireshark auttoi selventämään testausjaksojen aikana tullutta datamäärää huomattavasti, sillä pisimmillä testausjaksoilla datapaketteja saatiin jopa yli 300 000 riviä. Koska Wiresharkissa pystyttiin yksilöimään erinnäiset kohdat omilla värikoodeillaan (esimerkiksi TCP, AT-komennot ja DNS), joka nopeutti datan seulontaan huomattavasti. Sen lisäksi jokaiselle näistä pystyttiin luomaan myös omat palautusnappinsa, joiden avulla pystyttiin ottamaan Wiresharkissa esille pelkästään jonkin tietyn tyypin paketit.

3.3 Cellular Monitor nRF Connectissa

Nordicin nRF Connect on alustariippumaton ohjelma, jonka Nordic on kehittänyt avustamaan nRF-laitteiden kehitystöitä. Sen sisällä oleva alaohjelma, Cellular Monitor, on tärkeä osa tämän opinnäytetyön testauksiin liittyvissä datan seurannoissa.

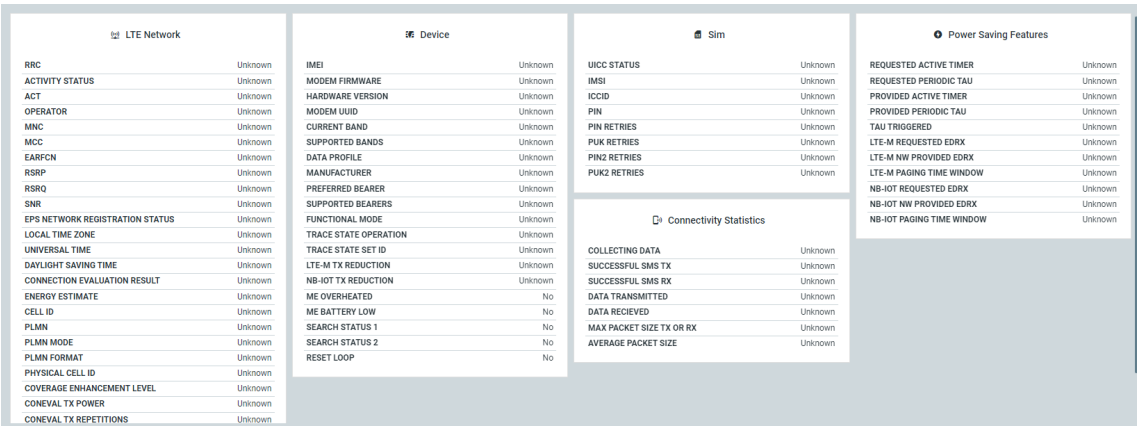
Cellular Monitor on nRF Connect:n sisällä oleva alaohjelma, jota käytetään mobiiliverkkojen dataliikenteen seurantaan ja debuggaukseen (eli virheenjäljitykseen). (6) Opinnäytetyön aikana sitä käytettiin Rudolf-testilaitteen ja serverin välisen dataliikenteen seurantaan.

Kerättävä data kategorisoidaan seuraaviin paneeleihin (kuva1):

- LTE Network
- Device
- Power Saving Mode
- SIM
- Connectivity Statistics
- PDN (Packet Data Network).

Näistä tärkeimmät Rudolfin kanssa ovat LTE Network ja Device. LTE Networkissa seurataan laitteen ja serverin välisen kommunikaation laatua ja vaiheita. RSRP ja RSRQ kertovat, kuinka hyvä kuuluvuus minäkin hetkenä on. RSRP (Reference Signals Received Power) mittaa kuuluvuuden voimakkuutta ja RSRQ (Reference Signals Received Quality) taas sen laatua. Molemmat näistä ilmoitetaan tasoilla Excellent, Good, Fair, Poor. Excellent, Good ja Fair riittävät melkein joka tilanteessa tarpeellisen kuuluvuuden saamiseen. Poor taas tarkoittaa, että jokin häiritsee yhteyttä, mutta se ei tarkoita sitä, että laitteella ei olisi mahdollisuutta saada yhteyttä muodostettua. Ainoastaan silloin, kun Cellular Monitor ilmoittaa No Signal, on yhteyden muodostaminen mahdotonta. Tämän jälkeen laite yleensä hetken odotusajan jälkeen aloittaa uudelleen paikannusrutiinin. (7.)

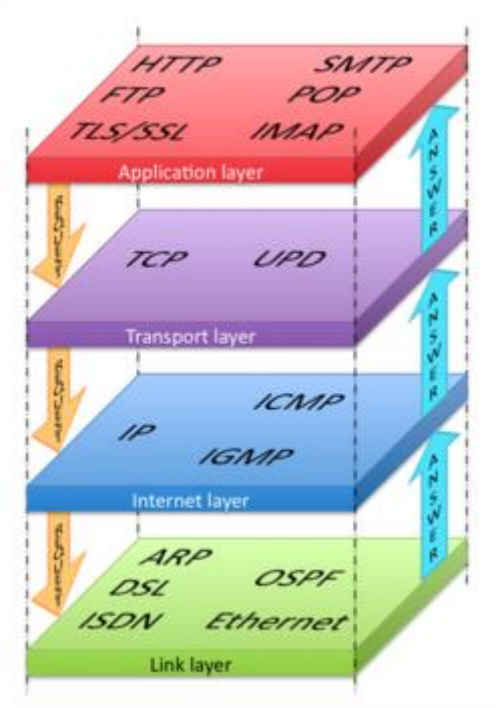
Devicessä taas seuraamme lähinnä ME Battery LOW -kenttää, koska se ilmoittaa heti, jos patteri alkaa olemaan loppuun kulunut. Joissain tapauksissa virran vähyys aiheuttaa ongelmia laitteen toiminnassa pariston loppua kohden.



KUVA 1. Yleisnäkymä Cellular Monitor -ikkunasta ilman päällä olevaa testausjaksoa

4 TCP/IP-PROTOKOLLAT

TCP/IP on internet-liikennöinnissä käytettävä tietoliikenneprotokolla. Siinä IP (Internet Protocol) on alempitasoinen protokolla, ja sen päällä on mahdollista ajaa useita eri kuljetus- tai verkkokerroksen protokollia, tässä tapauksessa TCP-protokollaa (Transmission Control Protocol). (Kuva 2.)



KUVA 2. TCP/IP-protokollapino

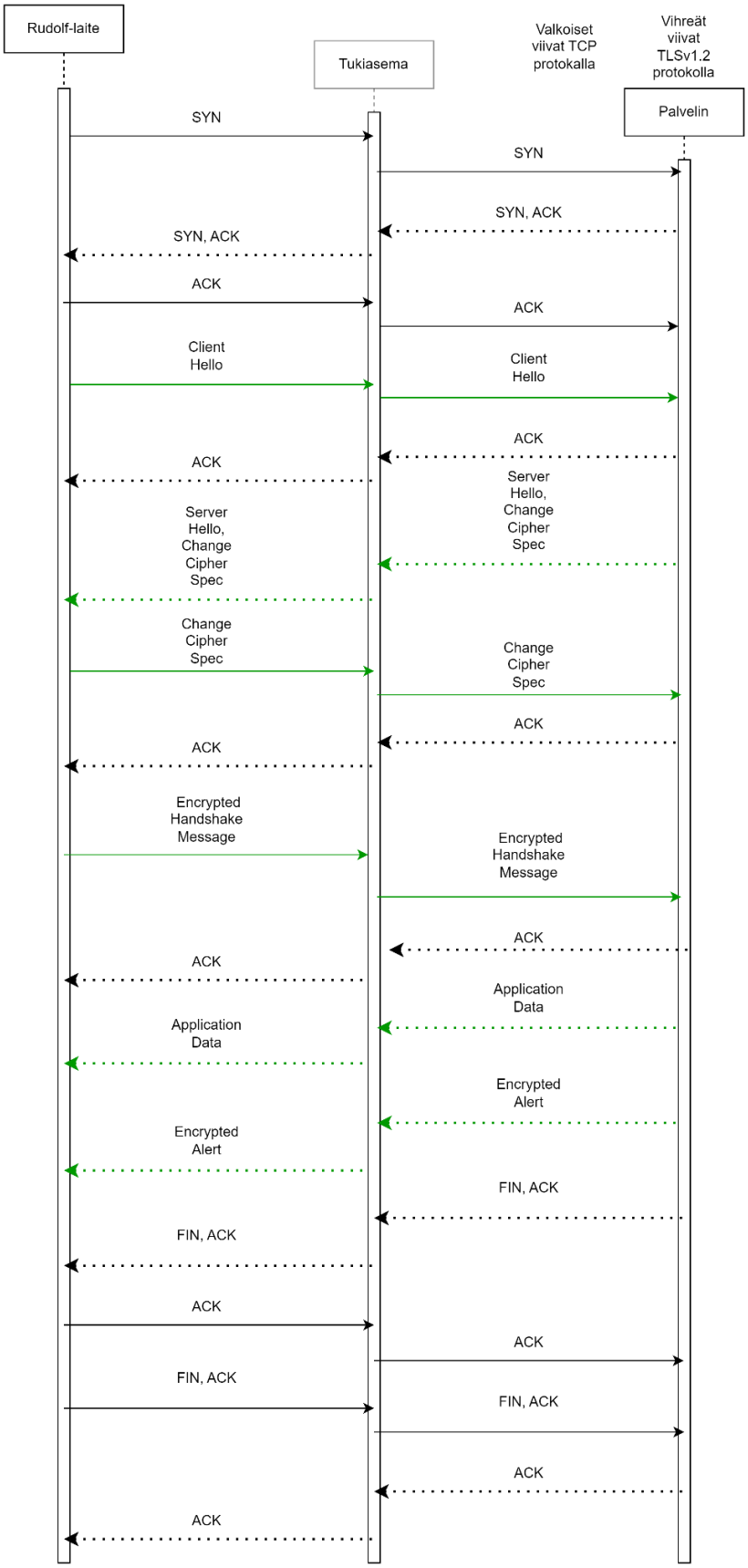
4.1 Projektin protokollat

Muita TCP:n lisäksi projektissa tapahtuvan viestinnän aikana suoritettavia protokollia olivat TLS, AT, RRC, NAS-ESP ja DNS.

- **TLS**: TLS, eli Transport Layer Security, on protokolla, jonka tehtävä on turvata verkon sisällä tapahtuva kommunikaatio.
- **AT**: Attention command eli AT-komento. Se on työkalu modeemien ohjaamiseen, jota tässä projektissa käytetään varmistamaan, että laite tekee oikeat asiat oikeaan aikaan.

- **RRC**: Radio Resource Control eli RRC, on protokolla, joka vastaa verkkojen kommunikaatioiden aloittamisista ja lopettamisista. Se myös huolehtii systeemin informaation jakamisesta.
- **NAS-ESP**: On protokolla, jonka avulla useammat verkon käyttäjät voivat saada yhteyden samaan varastoituun dataan.
- **DNS**: Domain Name System eli DNS, on protokolla, jolla eri laitteet voivat kysellä DNS serveriltä, kenelle mikäkin domain name kuuluu, jonka avulla saadaan selville niiden IP-osoitteet. (8.)

Työssä tehdyssä testauksessa nämä protokollat ovat käytössä laitteen ja serverin välisen kommunikaation aikana, ja myös viestintää alustavassa TCP:n kolmisuuntaisessa kädenpuristuksessa. (Kuva 3.)



KUVA 3. Laitteen ja serverin välisen kommunikaation sekvenssikaavio

4.2 TCP-kommunikaatioketju projektissa

Testauksen aikana käytetyssä firmware-versiossa on normaalissa ajamisessa kahta erilaista TCP-kommunikaatioketjua: yksi jokaisen testausjakson alussa oleva ensimmäinen TCP-kommunikaation, ja toinen kaikissa muissa TCP-kommunikaatioissa oleva. Kuvassa 3 esitetty sekvenssikaavio kuvaa jälkimmäistä näistä kahdesta.

Ensimmäinen TCP-jakso eroaa siinä määrin, että silloin tapahtuu niin sanottu “Key Exchange”, minkä aikana sekä laite että serveri vaihtavat kommunikaatioon tarvittavat avaimet keskenään ja todentavat ne. Sen jälkeen kyseisiä avaimia käytetään lopun kommunikaation aikana todistamaan keskustelun osapuolet toisilleen.

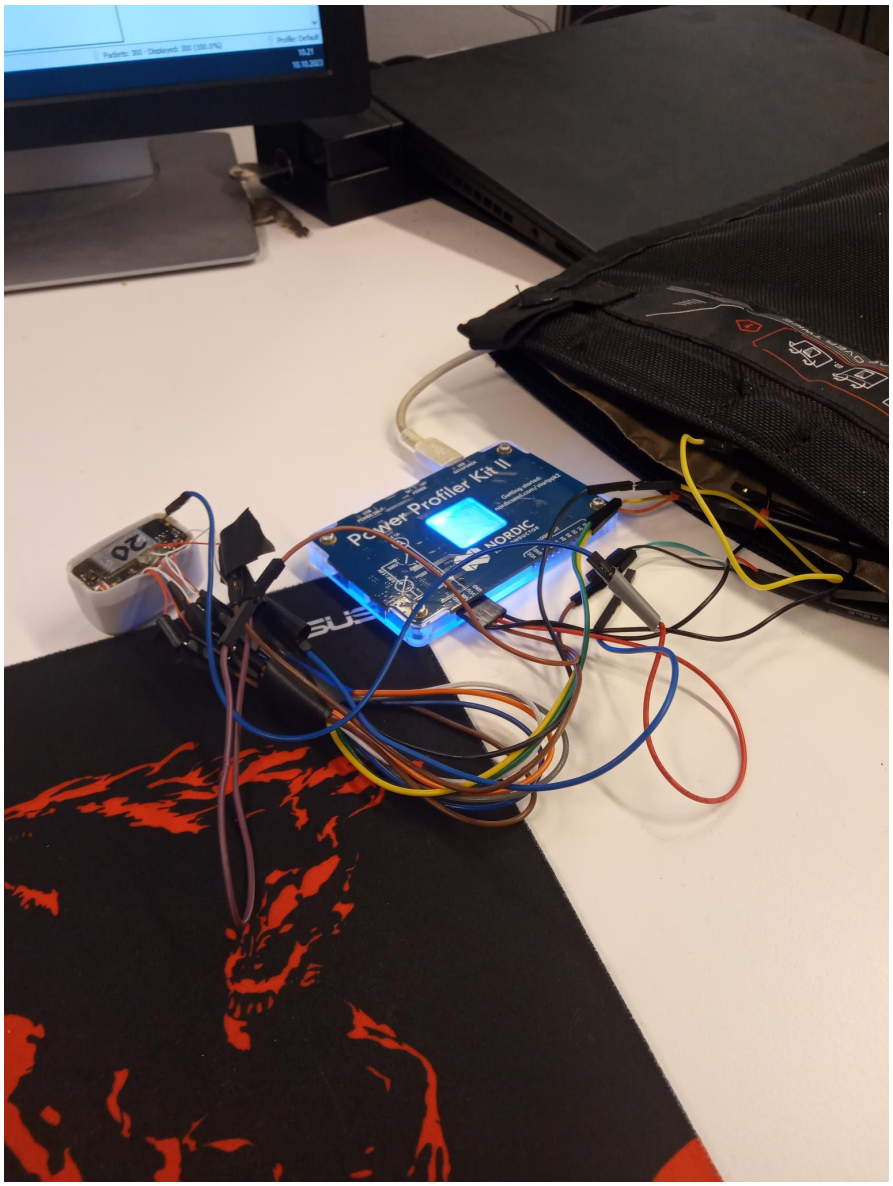
5 TESTAUS

Testaus suoritettiin kokonaisuudessaan Anicare Oy:n Oulun toimitiloissa käyttäen yrityksen omistamia testilaitteita, jotka oltiin ohjelmoitu juuri testiajoja varten sopiviksi. Pääosin testaus suoritettiin 24 tunnin jaksoissa, mutta myös viikonlopun yli vedettyjä noin 72 tunnin mittaisia jaksoja tehtiin.

5.1 Testauksen valmistelut

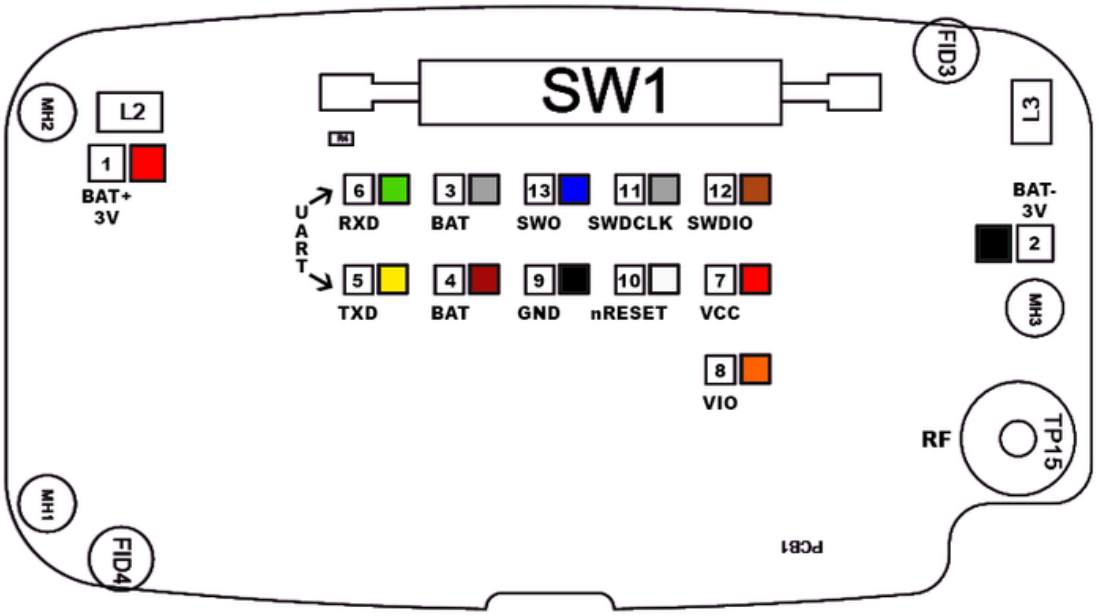
Testausta edeltää testilaitteiden valmistaminen, testausohjelmien ajaminen ja työympäristön viimeistely. Testauksessa tarvittava välineistö sisälsi testilaitteen (Rudolf-laite, testaukseen muokatulla firmwarella ajettuna), Nordic Semiconductorin Power Profiler Kit 2 (PPK2), tarvittavat USB-kaapelit ja hyppylangat, JLINK, sekä RF-säkki (faraday bag). (Kuva 4.)

PPK2 on Nordicin kehittämä laite, jonka avulla voidaan mitata virrankulutuksia. Sen avulla voidaan mitata amppeeri-tilassa ulkoisen virtalähteen kanssa, ja sen virtalähde-tilassa (Source Mode) laitetta voidaan käyttää virtalähteena muille laitteille silti mitaten samalla laitteen omaa virrankulutusta. (9.) RF-säkki, eli faraday bag, on säkki joka estää signaalien kulkeutumisen sen lävitse. Sitä käytettiin työssä aiheuttamaan verkkokommunikaatioon pientä häiriötä, jotta saataisiin tilanne, joka vastaa Rudolf-laitetta käyttävän eläimen liikkumista huonoilla kuuluvuusalueilla.



KUVA 4. Testausympäristö toimintavalmiina

Testilaitteen johdottaminen suoritettiin Anicare Oy:n tuotannon tiloissa. Johdot kolvataan Rudolf-testilevyn alaosan erillisille alustoille kiinni hyppylangoilla, jotta levy voidaan sitten yhdistää JLINK:iin, ja itse testauksessa PPK2:seen ja USB-johdon RXD- ja TXD-johtoihin. Hyppylangat tulee kolvata tarkasti, sillä alustan voi onnistua pilaamaan liiallisella tinaamisella. (Kuva 5.)



KUVA 5. Rudolf-levyn alaosan kytkentäalustat

Testaukseen käytettävä firmware voidaan ajaa tällä tavoin levylle kiinnittämällä hyppylangat kytkentätaulukon mukaisesti toisiinsa Rudolfin ja JLINK:in välillä, jonka jälkeen firmwaren voi käynnistää (Flash-toimenpiteellä) esimerkiksi Visual Studio Coden kanssa tai suoraan nRF Connectissa. (Kuva 6.)

JLINK	Rudolf
PIN 1 Vtref	PIN 8 VIO
PIN 5 TDI	PIN 5 TXD
PIN 7 TMS/SWDIO	PIN 12 SWDIO
PIN 9 TCK/SWCLK	PIN 11 SWDCLK
GND	PIN 9 GND
PIN 13 TDO/SWO	PIN 13 SWO
PIN 15 RESET	PIN 10 nRESET
PIN 17 DBGRQ	PIN 6 RXD

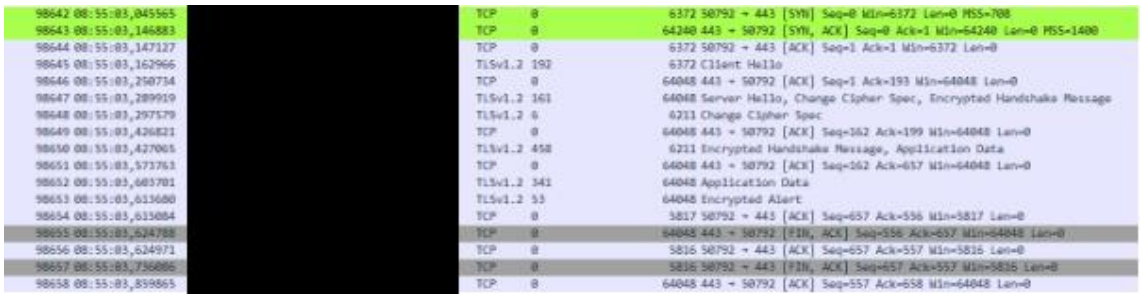
KUVA 6. Rudolf-testilevyn ja JLINK:in välinen kytkentäjärjestys

5.2 Testauksen vaiheet

Testaus aloitetaan järjestämällä testaukseen käytettävä laitteisto tasaiselle alustalle, jotta hyppylangat tai muut johdot eivät irtoa testauksen aikana, mikä aiheuttaisi mahdollisia testikatkoksia tai pahimmassa tapauksessa koko testausjakson epäonnistumista.

Alussa kytketään levystä lähtevät hyppylangat oikeisiin pinneihin USB-johdon TXD- ja RXD-paikoille, sen jälkeen virta- ja maadoituslangat kiinnitetään Power Profiler Kit 2:een.

Tämän jälkeen käynnistetään Cellular Monitor sekä Wireshark valmiiksi. Laite sijoitetaan tarvittaessa RF-säkin suuaukolle, jos halutaan saada testaus samankaltaisiin tiloihin kuin huonoilla kentällä liikkuessa. Viimeisenä laite käynnistetään magneetin avulla. Tämän jälkeen Cellular Monitor aloittaa laitteen tietojen seurannan, ja wireshark aloittaa verkkokommunikaation pakettien kirjaamisen. Testit alkavat AT-komennoilla, jotka starttaavat kommunikaation. Sitä seuraa TCP:n kolmisuuntainen kädenpuristus (kuva 7), joka tapahtuu jokaisen kommunikaatiosyklin alussa.



KUVA 7. Näkymän Wiresharkissa ensimmäisen TCP:n kolmisuuntaisen kädenpuristuksen aikana

6 ANALYSOINTITYÖKALU

Työssä koodattiin myös analysointityökalu Python-skriptinä, jonka tarkoitus oli tehdä suurin osa vikojen ja ongelmien etsinnästä käyttäjän puolesta. Sen pääkohteet olivat TCP-errorit, mitkä aiheuttavat pienissä määrin jonkinlaista laitteen kommunikaation hidastumista ja virrankulutuksen nousua, ja pahimmassa tapauksessa jopa tappavat koko laitteen kesken käytön. Skriptin toteuttamiseen käytettiin apuna Pyshark, joka toimii Pythonin ja Wiresharkin välisenä muuntajana. (10.)

Tärkeimmät ongelmakohdat mitä etsittiin olivat TCP Retransmission ja Spurious Retransmission, TCP Duplicate ACKs, TCP Reset, ja TCP Unseen ACKs.

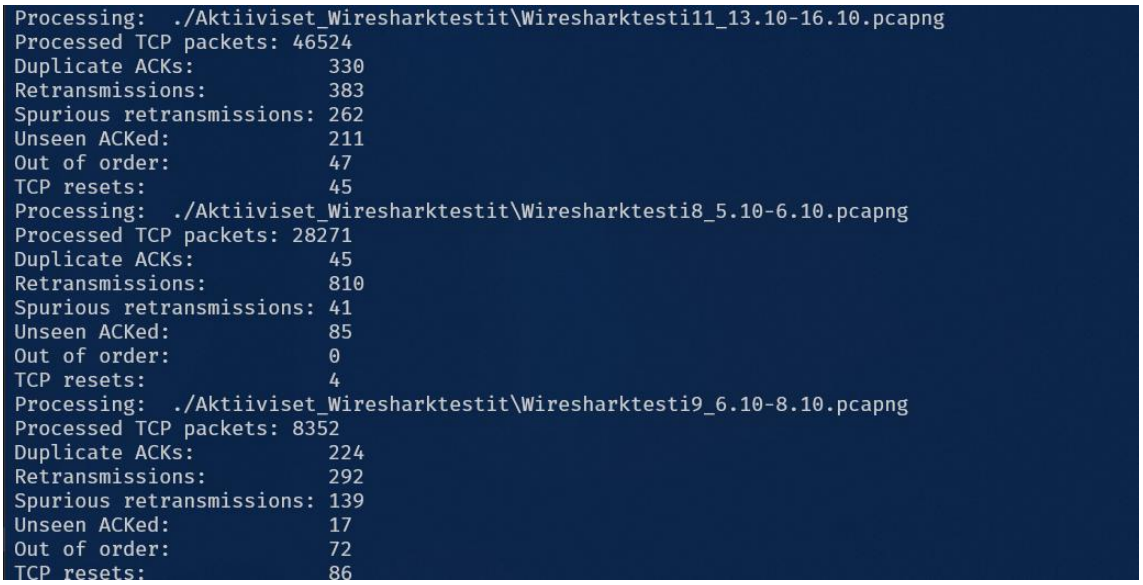
TCP Retransmission tapahtuu, kun paketti ei saavu perille tai vastaanottaja ei kuittaa (ACK) sitä, jolloin lähettäjä yrittää uudelleen lähettää saman tiedon uudelleen. Se tapahtuu, jotta varmistetaan, että viestit saapuu oikeasti perille, vaikka joku paketti olisi kadonnu matkan varrella. Spurious Retransmission taas tarkoittaa, että paketti lähetetään uudelleen ilman varsinaista tarvetta. Se voi tapahtuu esimerkiksi verkon viivästyksen takia, jolloin lähettäjä luulee paketin kadonneen, mutta se onkin jo matkalla, ja lopulta tulee kaksi samaa pakettia perille.

Duplicate ACK tapahtuu silloin, kun paketti saapuu väärässä järjestyksessä, tai silloin kun paketti katoaa matkalla. Sen sijaan Unseen ACK tarkoittaa sitä, että lähettäjä on saanut vahvistusviestin paketille, mutta tämä vahvistus ei näy missään seurannassa.

TCP Reset lähetetään, kun yhteys täytyy resetoida samantien. Se tapahtuu yleensä, jos vastaanottaja saa odottamattoman tai virheellisen paketin, tai jos yhteys ei enää ole tarpeeksi hyvän laatuinen. (11.) Näidenkin lisäksi joitakin mahdollisia hitauksia ja viestintä katkoja aiheuttavia kohtia varmasti on, mutta niitä ei työn testauksen aikana havaittu.

Python-skripti toimii siten, että koodille annetaan Wiresharkin avulla kaapattu pcapng-tiedosto. Tämän tiedoston koodi seuloo läpi, keräten samalla talteen kaikki koodissa vioiksi luokitellut protokollailmoitukset, ja sen jälkeen luettelee ja laskee niiden lukumäärät. (Kuva 8.)

Skriptillä voi myös tutkia montaa pcapng-tiedostoa yhdellä ajokerralla, ottamalla ne sisältävä kansio kokonaisuudessaan seulontaan yhden tiedoston sijasta. Tärkeimpiä kohtia mitä tällä seulotaan ovat TCP:n error-kohdat. Niiden lukumääriä seuraamalla voidaan saada yleiskuva siitä, onko jokin tietyn tyyppinen ongelma luettavissa tiedostoissa.



KUVA 8. Esimerkkinäkymä Python-skriptin ajamisen jälkeen

7 LOPPUTULOS JA POHDINTA

Työn lopputuloksena saatiin tuotettua työn tilaajan haluama ohjeistus verkkokommunikaation testausta varten ja lisäksi tehty myös applikaatio sen helpottamiseksi. Työssä käydään läpi tarvittavat informaatiot testausta varten, ja sen ohjeistuksen avulla saadaan aloitettua ja suoritettua kokonainen testisykli. Omasta mielestäni työ, ja siinä suoritetut testaukset, onnistuivat kelvollisen hyvin.

Työssä avataan myös käytettävien verkkojen (LTE-M ja NB-IoT) sekä ohjelmien (Wireshark ja Cellular Monitor) käyttöä ja yleisiä kohtia. Sen lisäksi käytiin testauksessa olleita protokollia ja niiden perusteita läpi, ottaen esimerkeiksi yleisimmät niistä.

Testauksien tuloksena saatiin monenlaisia testausjaksoja, aina täysin ehjistä jopa tuntien sisällä katkenneisiin. Analysointityökalu-kappaleessa mainitut TCP-errorit olivat ainoita mitä testausjaksojen aikana havaittiin verkkokommunikaatiossa. Harmillisesti testauksissa ei saatu replikoitua LTE- ja NB-IoT-verkkojen välisestä hyppelystä johtunutta reboot-kierrettä, mikä aiheutti laitteiden katoamista kentällä. Tämä ongelmakohta oli alunperin se, mikä käynnisti koko verkkokommunikaation testauksien aloittamisen.

LÄHTEET

1.
EsEye 11.3.2024. LTE-M for IoT and M2M: Everything You Need to Know. Luettavissa: https://www.eseye.com/resources/iot-explained/lte-m-for-iot-m2m/. Luettu: 28.11.2024.

2. UUSITEGNOLOGIA.fi 20.5.2019. NB-IoT:n rinnalle LTE-M-tekniikka. Luettavissa: https://www.uusiteknologia.fi/2019/05/20/nb-iotn-rinnalle-lte-m-tekniikka/. Luettu: 28.11.2024.

3. TechTarget, Elokuu 2023 Alexander S. Gillis. Narrowband IoT. Luettavissa: https://www.techtarget.com/whatis/definition/narrowband-IoT-NB-IoT. Luettu: 28.11.2024.

4. Wireshark, A Brief History of Wireshark. Luettavissa: https://www.wireshark.org/docs/wsug_html_chunked/ChIntroHistory.html. Luettu: 28.11.2024

5. Chris Greer, 25.2.2021 Wireshark Tutorial for BEGINNERS // Where to start with Wireshark. . Katsottavissa: https://www.youtube.com/watch?v=OU-A2EmVrKQ. Katsottu 28.11.2024.

6. Nordic, nRF Connect Cellular Monitor 15.11.2024. Luettavissa: https://docs.nordicsemi.com/bundle/nrf-connect-cellularmonitor/page/index.html. Luettu: 28.11.2024.

7. Nordic, 20.6.2023, Michal. Introducing the Cellular Monitor . Luettavissa: https://devzone.nordicsemi.com/nordic/nordic-blog/b/blog/posts/introducing-the-cellular-monitor. Luettu: 28.11.2024.

8. Geeks For Geeks, 27.9.2024 Domain Name System (DNS) in Application Layer . Luettavissa: https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/. Luettu: 28.11.2024

9. Nordic 2024, Power Profiler Kit 2 . Luettavissa: https://www.nordicsemi.com/Products/Development-hardware/Power-Profiler-Kit-2.

Luettu: 28.11.2024.

10. PyShark 2024, KimiNewt github. Luettavissa: https://kiminewt.github.io/pyshark/. Luettu: 28.11.2024.

11. Darpa Internet Program Protocol Specification, syyskuu 1981, RFC 793 - Transmission Control Protocol (TCP). Luettavissa: https://www.ietf.org/rfc/rfc793.txt. Luettu: 28.11.2024.