Time-sensitive networks over 5G

Bachelor's thesis

Häme University of Applied Sciences

Information and Communications Technology

Spring 2020

Kaarlo Skogberg

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja viestintätekniikka
Hämeen Ammattikorkeakoulu

Tekijä Kaarlo Skogberg **Vuosi** 2020

Työn nimi Aikakriittiset verkot 5G:n yli

Työn ohjaaja/t Marko Grönfors (HAMK), Toni Huusko, Juhani Kerovuori

TIIVISTELMÄ

Opinnäytetyön tarkoitus oli tuottaa vertailu reaaliaikaisista kommunikaatiokeinoista nosturin ja etäohjausaseman välille 5G-mobiiliverkon yli. Kenttäväyliä tarvitaan nosturin kanssa kommunikointiin, mutta koska nämä ovat pääosin tason 2 protokollia ja eivät reitity luontaisesti 5G-verkossa täytyy kenttäväylän verkkoliikenne tunneloida. Työssä tutkittiin erilaisia Ethernet-pohjaisia kenttäväyliä sekä tunnelointiteknologioita, jotka kykenevät tunneloimaan tason 2 verkkoliikennettä. Tason 2 tunnelointi mahdollistaa suoran kommunikaation kahden paikallisverkon välillä. Kaikkien työssä tutkittujen Ethernet-pohjaisten kenttäväylien sekä tunnelointiprotokollien täytyi olla sopivia käytettäväksi teollisessa ympäristössä valituilla verkkolaitteistolla.

Työtä varten tutkitun tiedon perusteella esitetään, että käytettävä kenttäväylä sekä tunnelointiprotokolla tulisi valita saatavilla olevan verkkolaitteiston sekä muun infrastruktuurin perusteella. Kenttäväylää valittaessa reaaliaikaiset vaatimukset olivat käyttötarkoitukseen nähden kevyet, joka avaa enemmän vaihtoehtoja kenttäväylää valittaessa. Yrityksessä käytetään jo Profinetia, joka soveltuu mainiosti käyttötarkoitukseen. Oikean tunnelointiprotokollan valitseminen riippuu suurimmaksi osaksi käytettävissä olevasta laitteistosta. Tunnelointiprotokollan täytyi tukea valittua laitteistoa. Yksi mahdollinen tunnelointiprotokolla voisi olla L2TPv3 IPsecin kanssa. Työn lopputuloksena on mittaussuunnitelma käytössämme olevalle laitteistolle ja kattavaa tietoa eri kenttäväylistä sekä tason 2 tunnelointiratkaisuista, jotka ovat laajasti tuettuja.

Avainsanat Tunnelointi, 5G, kenttäväylä, reaaliaika

Sivut 26 sivua, joista liitteitä 0 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology
Häme University of Applied Sciences

Author Kaarlo Skogberg **Year** 2020

Subject Time-sensitive networks over 5G

Supervisors Marko Grönfors (HAMK), Toni Huusko, Juhani Kerovuori

ABSTRACT

The main purpose of this thesis was to provide a comparison of real-time communication methods between a crane and the remote operating station over 5G. Fieldbus protocols are used to communicate with the crane, but because fieldbuses are mainly layer 2 protocols, they are not routed natively through 5G networks. A tunneling protocol capable of tunneling layer 2 network traffic is therefore needed. Layer 2 tunneling makes it possible to directly communicate between two local area networks. All of the researched Ethernet-based fieldbuses and tunneling protocols must be suitable to use with chosen industrial network equipment.

With the gathered information, I present that the fieldbus and tunneling protocols to be used should be chosen with available network equipment and rest of the infrastructure in mind. Regarding fieldbuses, the real-time requirements were for soft use in our case, which opens up for more choices when choosing the correct fieldbus. The company has Profinet already in use, which is more than suitable for this purpose. Choosing the correct tunneling protocol however largely depends on the available equipment. In this thesis, the tunneling protocol had be supported by our chosen equipment. One possible choice for tunneling would be to use L2TPv3 over IPsec. The outcome of this work provides a measurement plan for our setup and knowledge of various fieldbus protocols and layer 2 tunneling solutions that are widely supported.

Keywords Tunneling, 5G, fieldbus, real-time

Pages 26 pages including appendices 0 pages

TABLE OF CONTENTS

ABBREVIATIONS

AH	Authentication Header
CIP	Common Industrial Protocol
CN	Controlled Node
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
eMBB	Enhanced Mobile Broadband
ESP	Encapsulating Security Payload
GRE	Generic Routing Encapsulation
HMI	Human Machine Interface
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IKE	Internet Key Exchange
IMT	International Mobile Telecommunications
IPsec	Internet Protocol Security
IRT	Isochronous real-time
ISO	International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
LAN	Local Area Network
LTE	Long Term Evolution
L2TPv3	Layer 2 Tunneling Protocol version 3
MAN	Metropolitan Area Network
mMIMO	multiple input, multiple output
mMTC	massive Machine Type Communications
mmWave	millimeter wave
MN	Managing Node
MU-MIMO	multiple-user MIMO
NMT	Network Management
NR	New Radio
NRT	Non real-time
NSA	Non-Standalone
ODVA	Open DeviceNet Vendors Association
OSI	Open Systems Interconnection
OT	Operational Technology
PDO	Process Data Object
PLC	Programmable Logic Controller
PPTP	Point-to-Point Tunneling Protocol
Profinet	Process Field Network
QoS	Quality of Service
ROS	Remote Operating Station

RPC	Remote Procedure Call
RT	Real Time
SDO	Service Data Object
SMTP	Simple Mail Transfer Protocol
SRT	Soft real-time
SSL	Secure Sockets Layer
TAP	Terminal Access Point
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TLS	Transport Layer Security
TSN	Time-Sensitive Networking
UDP	User Data Protocol
URLLC	Ultra Reliable Low-Latency Communication
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network

1 INTRODUCTION

This thesis was made for a global crane manufacturing and service company which manufactures and services lifting equipment and machinery for various industries, ports, terminals and shipyards.

The company is looking to deploy crane automation over a 5G network using one control software for several devices in a restricted environment. Private 4G & 5G networks are becoming popular amongst industrial companies. Therefore the following research will be useful with the future in mind. 5G enables wireless control and is more advanced than 4G in terms of capacity and latency. The network's performance between the crane and control software should be stable and have low latency to enable reliable connection. Fieldbus protocols are used to communicate with the crane, but the problem is that fieldbus protocols are mainly layer 2 protocols therefore they are not routed natively through 5G networks. To route the traffic, a tunneling protocol capable of tunneling layer 2 traffic is needed. In this thesis I am researching different fieldbus and tunneling protocols suitable for use in industrial environment, measure their performance and see what kind of solutions can be built on top of them.

In the beginning of the thesis in chapter two, I explain some basic networking theory that are of use later on in the thesis. In chapter three, I present overall information on 5G and its features of interest. Chapter four is all about time-sensitive networking, ethernet and fieldbus protocols. I present three potential fieldbus protocols to consider for this thesis since they are bound to have some difference performance-wise. I explain tunneling protocols and present three potential protocols to use regarding this thesis in chapter five. Chapter six has the measurement plan for our chosen setup.

2 NETWORK TECHNOLOGIES

Some basic networking theory that will be used in this thesis is presented in this section. The OSI model is introduced first, its layers and how it works and after that various network topologies are presented that will be of interest for this thesis.

2.1 The OSI Model

The OSI (Open Systems Interconnection) model was developed by ISO (International Organization for Standardization) and it provides a standard that enables communication between various computer systems. The OSI model is split into 7 layers each of which use the services offered by the layer below and in turn offer their services to the layer above. The layers can be split into two, the lower layers consist of the layers 1-4 and the upper layers are 5-7. The lower layers focus on sending information and the upper layers focus on applications. See the figure 1 below for an example of the OSI model and its layers. (Cisco, 2011);(Cloudflare, 2018)

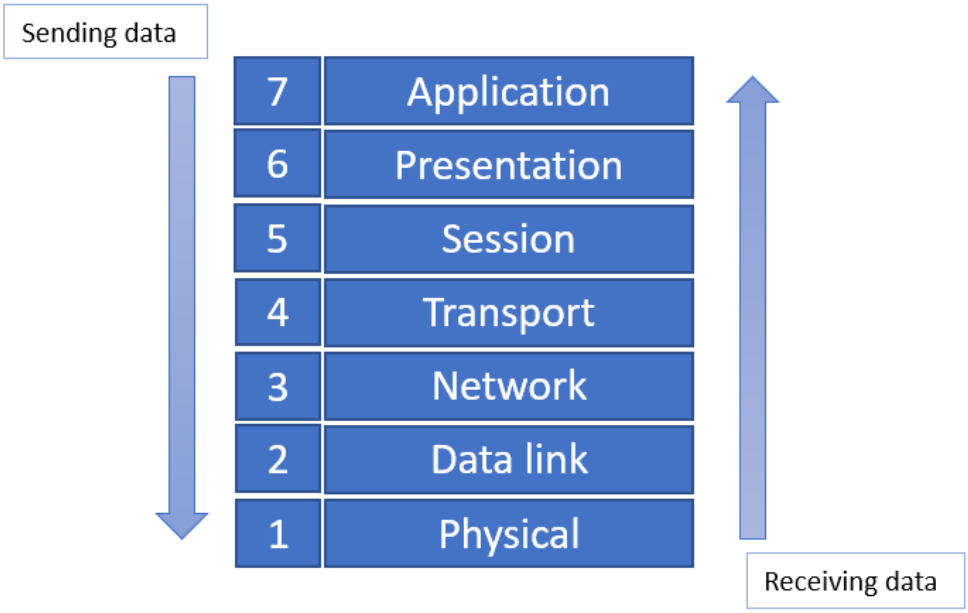

Figure 1. The 7 layers of the OSI model.

2.1.1 Physical layer

The physical layer is defined as the physical part of transferring information. It includes the physical equipment such as the Ethernet cable. Its duty is to convert data into a bit stream and conduct the bit stream to receiver. (Cisco, 2011);(Cloudflare, 2018)

2.1.2 Data link layer

The data link layer provides reliable data transfer using the physical link. Its responsible for flow control and error control in internal network communications. The data link layer also breaks down the network layer's packets and breaks them into frames. Network switches usually operate on this layer. (Cisco, 2011);(Cloudflare, 2018)

2.1.3 Network layer

The network layer's responsibility is making the data transfer from two different networks possible, however the network layer is unnecessary when the two devices communicating are on the same network. The network layer breaks down the transport layer's segments into smaller pieces, also known as packets. IP (Internet Protocol) is perhaps the most known protocol on this layer. Most people are still using the first major version of IP which is IPv4. The newer major version is called IPv6 and it is not used widely yet, but its main advantage over IPv4 is having a lot more possible IP addresses. Routing is done here as well by finding the best physical path for data to reach its destination. Network routers operate on this layer. (Cisco, 2011);(Cloudflare, 2018)

2.1.4 Transport layer

The transport layer offers connectivity within two end devices. It takes data from the session layer breaks down the data from layer 5 into segments for the network layer. The transport layer uses the TCP (Transmission Control Protocol) and UDP (User Data Protocol) protocols amongst others to transfer data. TCP is used when data is planned to be transmitted. TCP uses the three-way handshake to negotiate starting the connection. UDP is different though as its used when the assignment is so simple that it is not necessary to inform about forming the connection and it does not use the three-way handshake. The Transport layer is also responsible for flow control and error control in the external network communications. (Cisco, 2011);(Cloudflare, 2018)

2.1.5 Session layer

The session layer is responsible for opening and closing communications between the two devices. Session means the time between the opening and closing of the communication. The session layer ensures that the session stays open as long as necessary to transfer all the necessary information and then closes the session. The session layer also secures the connection by creating checkpoints within the data transfer. For instance, the checkpoint could be set to happen every 5 MB and in the case of a disconnect, the session would continue from the last checkpoint. (Cisco, 2011);(Cloudflare, 2018)

2.1.6 Presentation layer

The presentation layer's job is to prepare the data for application layer. If the two devices are using different encoding methods, the data is translated on this layer. If the two devices are communicating over an encrypted connection, then the encryption is added on the sender's end and decoded for the receiver's end to be able to present the data on the application layer. The data is also compressed when delivered to layer 5. (Cisco, 2011);(Cloudflare, 2018)

2.1.7 Application layer

User interaction is done on the application layer. This layer includes the protocols that are responsible of presenting meaningful data to the users. These protocols include protocols like HTTP (Hypertext Transfer Protocol) and SMTP (Simple Mail Transfer Protocol). (Cisco, 2011);(Cloudflare, 2018)

2.2 Network topologies

Network topologies define how the network is physically built and how the nodes are connected to each other. The most common network topologies are the bus, star, ring, and mesh. Different network topologies come with their advantages and disadvantaged. (Cisco, 2011)

2.2.1 Bus

The oldest of currently used network topologies. In bus topology every node is connected to a single central cable, hence the name bus. Every device connected to the bus receive the sent packet at the same time. The weakness of the bus topology is, that its designed to be use with CSMA/CD, which makes it so that the network can only be used by one device at a time. Another problem with the bus topology is that if a cable breaks down or gets damaged then the network does not work. For bus topology, either a coaxial or an optical fibre cable is often used. See the figure 2 below for an example of the Bus topology. (Cisco, 2011);(Singh, 2019)

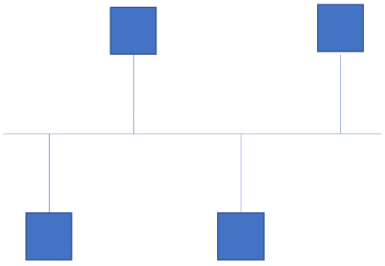

Figure 2. Bus topology.

2.2.2 Star

In star topology, every device has its own connection to the node in the middle (For example, a hub or a switch). It is the most popular of the Ethernet network topologies in use. Its most notable benefit is that one cable breaking does not affect rest of the network. It is easy to install. Easy fault detection. However, if the hub in the middle goes down, then the whole network goes down. See the figure 3 below for an example of the Star topology. (Cisco, 2011);(Singh, 2019)

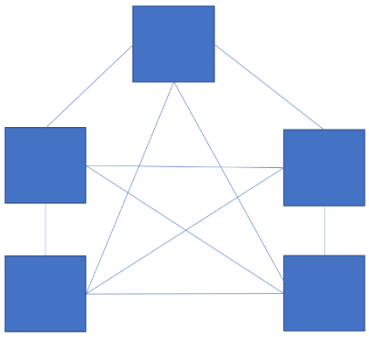

Figure 3. Star topology

2.2.3 Ring

In ring topology, the network has been physically formed as a ring. Data travels around the ring in on direction and so the data passes through every device in between of the source and the destination devices. The devices in between repeat the data to keep the signal strong. It is better than the bus topology when the load on the network increases. It is easy to install. A failure in one of the links can break the whole network though as the signal will not travel forward in a failure. Also there can be issues with the network traffic as the data circulates the ring. See the figure 4 below for an example of the Ring topology. (Cisco, 2011);(Singh, 2019)

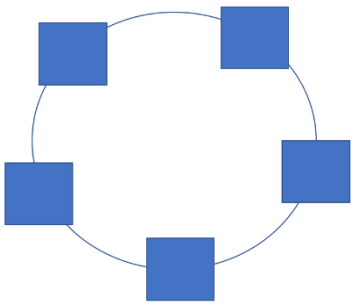

Figure 4. Ring topology.

2.2.4 Mesh

In mesh topology, every node is connected to each other. It has no network traffic issues since there is a dedicated link between every device. Its

reliable as one link failing does not break the whole network. It has easy fault detection as if one cable breaks for instance, it can simply just be replaced. There is a downside to mesh topology, that is it needs a lot of wiring to be done and can be complicated to plan. See the figure 5 below for an example of the Mesh topology. (Cisco, 2011);(Singh, 2019)

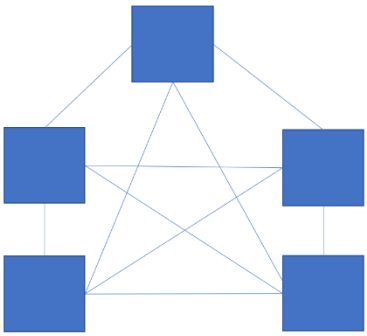

Figure 5. Mesh topology.

3 5G

5G is the 5th generation of wireless communications standards.
Before 5G there was 2G, which was a set of standards about wireless telephone calls. Then came 3G which allowed people to get on the internet on their smartphones. 4G delivered such mobile internet speeds that allowed streaming video, high-quality video calls and quick mobile browsing. The development of 4G was a massive feat for mobile technology, but the leap to 5G will be much greater than to previous generations. 5G-technology is the straight successor to 4G which was launched in 2010. The wide deployment of 5G began late 2019, but currently it is available mostly in major cities. 5G networks will most likely be expanded once 5G-supporting end devices are more widely available and features have been implemented.

5G will be more than welcome upgrade over 4G as consumers are transmitting more data than ever mostly due to video streaming, but there are other reasons to upgrade as well. Consumers have more and more devices that require internet connectivity and the future internet will require networks that must handle a lot more devices. Energy efficiency must be better. Network operators want to reduce operational expenses as consumers do not want the price of internet to keep going up. The mobile communication technology can enable many more use cases to be implemented. Ultra-low latency and high reliability are crucial for critical applications and it can improve industrial automation to be more cost effective and flexible. (Qualcomm, 2017)

3.1 Throughput and coverage

5G allows for better throughput. The download speed ranges from around 50 Mbps (Megabits per second) to over 2 Gbps (Gigabits per second) but is also expected to grow even up to 100 Gbps. 5G operates on wireless bands which are basically just blocks of frequency. 5G utilizes a wide range of bands from low bands (less than 1 GHz) to mid bands (3.5 GHz to 6 GHz) to high bands (24 GHz – 40 GHz).

Low bands are less affected by obstacles or other conditions, which makes them a good choice for covering a large geographic area. Low bands range in speed from 30 to 250 Mbps.

The most common 5G band "Sub-6 GHz 5g" also called the mid band or NR (New Radio) overlaps and extends 4G LTE (Long Term Evolution) frequencies. It covers an area of several kilometres while delivering speeds from 100 to 900 Mbps, which makes them a great choice if you take into account that you need less radio towers than high bands do while getting relatively high speeds.

High bands also known as mmWave (millimetre wave) delivers the fastest speed out of the three bands. You can get up to 1-3 Gbps if you happen to be near one of those towers, but nothing comes without a price. The maximum range of high band is 1-1.5 kilometres, 1 kilometre being the reality in most cases. The higher frequencies that high bands use are more susceptible to obstacles than lower frequencies. These bands are most likely to be deployed only in densely populated environments.

There is a technology called beamforming, which is used in 5G networks to address the problem with millimetre waves. Cellular signals cannot pass objects very well and tend to get weaker over long distances. Beamforming helps on this matter. It focuses a signal in a single concentrated beam towards the direction of a user, rather than broadcasting the signal to many directions at once. Beamforming improves the signal's chances to stay intact and it reduces the interference for others. This is however only one specific implementation of beamforming. Beamforming is used in mMIMO as well.

Massive MIMO or mMIMO (multiple input, multiple output) technology means a system that has a greater amount of antennas than users. Massive in mMIMO means that there are 32 or more logical antenna ports in the base station. It can be expected that network equipment manufacturers will begin with 64 logical antenna ports in 5G. Having many antennas on the base station helps focus energy, which in turn brings drastic improvements in throughput and efficiency. 5G will benefit from mMIMO in several ways. Increased network capacity with MU-MIMO(multiple-user MIMO) can be expected, as MU-MIMO allows for multiple users to be

served within the same time and frequency resources. Also the deployment of 5G NR (5G New Radio) for the mid and high bands.
The coverage will be better with mMIMO and users should be noticing high data rate service almost everywhere. The user experience should be better overall. (Contreras, 2020);(Nordrum, Clark, & Staff, 2017);(Passoja, 2018)

3.2 Latency

One of the key features of 5G that is presented in this thesis, is latency and what can be achieved with new low latency technology. Main improvement for industrial users is reliable and low latency connectivity. The feature is called URLLC (Ultra Reliable Low-Latency Communication). Latency as a networking term can be defined by the overall time it takes for a packet to move from one source to the destination. This is also called one-way latency. Round-trip latency in the other hand is one-way latency and the time that is needed for the packet to return back from the destination. Basically, the lower the latency you have, the better it is. (KeyCDN, 2018)

3.3 Standardization

Standardization is a process to develop a foundation of agreements that must be followed by all relevant groups within an industry or organization to ensure that all processes associated with the creation of a service or the product are achieved within the agreed guidelines. Standardization can improve the quality, compatibility and safety of the product in question. (Grant, 2019)

On June 19th 2015 ITU (International Telecommunication Union) established the long term roadmap for the development of 5G and it was named as IMT-2020 (International Mobile Telecommunications-2020). ITU has since declared certain requirements for 5G implementation for IMT-2020.

- The peak data rate under ideal conditions for downlink should be 20 Gbit/s and for uplink 10 Gbit/s.
- Peak spectral efficiency basically means how effectively and usefully you can take use of every Hz of frequency available and is important because the available spectrum for communication is limited. The requirement is 30 bit/s/Hz.
- Users should be experiencing a minimum of 100 Mbit/s data rate for downlink and 50 Mbit/s for uplink.
- The latency requirement for eMBB (Enhanced Mobile Broadband) is 4 ms and for URLLC (Ultra Reliable Low Latency Communication) it is 1 ms.
- Maximum mobile station speed at which a defined QoS (Quality of Service) can be achieved is 500 km/h e.g. in high speed trains.
- The number of devices that must be able to be connected at the same time is 1 000 000 devices per km^2

- Energy efficiency or in other words, the data transmitted per unit of energy consumption must be equal to 4G. (International Telecommunication Union, 2017)

3.3.1 Release 15

Starting with 3GPP release 15 standard covering phase 1 of 5G deployment – it was the first big step towards 5G. Released during the second quarter of 2018. Release 15 classified the first networks and devices to support 5G as NSA (Non-Standalone), which means that they will support 5G networks using existing 4G infrastructure. Meaning that your smartphone needs to have 5G capability to connect to 5G frequencies for data-throughput improvements, but it will still use 4G for communicating with cell towers and servers.
The most interesting features of release 15 are eMBB, mMTC (massive Machine Type Communication) and URLLC. First is eMBB which results in high bandwidth internet access with wireless connection. mMTC and URLLC are developed with industrial IoT communications in mind. mMTC is a service that aims to enable connectivity with a massive amount of devices within a small area. The requirement has been set as up to 1 million devices within a square kilometre. URLLC's key feature is the low latency part, it is developed to be used with time-sensitive networking to provide latency as low as 1 ms. This requires time synchronization within the devices in the network, but it will be a great feature for industrial purposes such as automated factories. (3GPP, 2018); (Allen, 2018); (Gigabyte, 2018)

3.3.2 Release 16

Release 16 is another major release and it is part of phase 2 of 5G deployment. Completion date for release 16 is later this year.
It delivers some new features and several enhancements to existing features. Beamforming and MIMO get enhancements for better throughput, reduced overhead and increased robustness. Reduced handover delays will be applied for mmWave bands. Dynamic spectrum sharing enables the use of same carrier with LTE and NR. NR can be used in unlicensed spectrum (5GHz and 6GHz bands). URLLC gets enhancements to latency and reliability, the support for time-sensitive networking. (Ericsson, 2019); (3GPP, 2019a)

3.3.3 Release 17

Release 17's content was approved in December 2019 by the 3GPP. It will bring further enhancements to eMBB, mMTC and URLLC. The goal of the release is to provide support to increased use of mobile data and customize NR further for industrial use cases. Release 17 includes a bunch of new features for eMBB, mMTC and URLLC and here is a small take of some of the interesting features: NR's spectrum is extended to support frequencies

from 52.6GHz to 71GHz. Multi-SIM devices are supported. Satellites get support to provide better coverage for rural areas. Broadcast/multicast services are enabled within NR. (Ericsson, 2019); (3GPP, 2019b)

4 TIME-SENSITIVE NETWORKING

TSN (Time-Sensitive Networking) is a combination of Ethernet sub-standards, which have been mentioned in IEEE 802.1 TSN Task Group. TSN focuses on achieving the convergence of IT (Information Technology) and OT (Operational Technology) possible by developing current Ethernet standards.

TSN aims to standardize layer 2 in OSI-model by making the infrastructure usable by multiple protocols. Deterministic real-time communication over Ethernet is made possible with these standards. TSN uses time synchronization and a shared schedule between all of the network nodes. TSN basically guarantees certain latency for scheduled traffic through switched networks. This enables time-critical communication of applications in the network such as digital control systems or motion control applications which generally require cycle times below 1 ms. In control applications with strict deterministic requirements, TSN can transmit time-critical traffic over a standard Ethernet infrastructure. This allows the convergence of all traffic classes and multiple applications in a single network. In other words, the standard Ethernet's functionality is extended to offer significant advantages in network connectivity, scalability and cost of deployment and ownership. (Varis & Leyrer, 2018)

4.1 Ethernet

Ethernet is the most known and used LAN (Local Area Network) technology today, but it is also commonly used in MAN (Metropolitan Area Network) and WAN (Wide Area Network). Ethernet refers to the networking technologies standardized by the IEEE 802.3 standard. It was first introduced commercially in 1980 and standardized 3 years later. The first variant of Ethernet, 10BASE5 used coaxial cable, but nowadays it runs on optical fibre and twisted-pair cables. Ethernet has been constantly evolving sine then to provide better performance and network intelligence. It supports higher bit rates, a greater amount of nodes, longer link distances and downward compatibility to previous Ethernet technologies.

With Ethernet it is possible to choose from four different data rates.

- Ethernet/10Base-T is IEEE 802.3 standard and has a data rate of 10 Mbps.
- Fast Ethernet/100Base-T is IEEE 802.3u standard and provides data rate of 100 Mbps.

- Gigabit Ethernet/GigE is IEEE 802.3z standard and provides data rate of 1000 Mbps.
- 10 Gigabit Ethernet is the fastest and newest of the Ethernet standards. Defined by IEEE 802.3ae standard, it provides with data rate of 10 Gbps.
- (Frenzel, 2009); (Johnson, Determinism in industrial ethernet: A technology overview - Part 1, 2009a)

4.2 Fieldbus systems

Fieldbus is an industrial network system used in automation systems. It consists of multiple industrial computer network protocols which have been standardized as IEC61158. Fieldbuses are a part of a complex automated industrial system such as assembly lines and automation of different machinery. Fieldbus is a way to communicate with input devices such as sensors or switches and output devices such as valves or drives without the need to connect each individual device back to the PLC (Programmable Logic Controller). This means that less cabling is needed and it can therefore lower the costs.

In the past before fieldbuses, industrial controller systems were connected via RS232 serial cables which allowed only two devices to communicate. Today however, it is possible to connect multiple field devices to a single connection point (ethernet switch for example) via an ethernet cable which then connects to a PLC. The ethernet cables used in industrial networks are basically regular RJ45 except they are rugged versions of them to provide reliability that is required in industrial environments.
Fieldbuses work on the bottom level of the control chain, they link the PLCs to the components such as sensors, switches, motors and valves. If the fieldbus devices are sensors, motors or similar devices – they need to be connected to an I/O data block which connects to a Field Distribution device which connects to the PLC. On top of PLC, there is usually a HMI (Human Machine Interface) where an operator monitors or operates the system. These fieldbuses that are connected via Ethernet are called ethernet-based fieldbuses or in other words industrial ethernet protocols.
Fieldbus works on a network that allows for different network topologies. Examples of these are the ring, branch, star, and daisy chain topologies. Each of them having their own advantages and disadvantages. Some industrial ethernet fieldbus protocols do not support all of the topologies so that is one thing to research before committing to one fieldbus. (Anderson, 2019);(Voss, 2019)

4.3 Industrial Ethernet protocols

Ethernet-based fieldbus protocols bring a lot of advantages to the table over traditional fieldbus protocols. Ethernet is a future-proof choice as its everywhere and it is developed continuously. Making the switch to Ethernet results in a greater bandwidth, message size and unlimited address space. Ethernet makes the network faster as any device can communicate when it has to. Since Ethernet networks are switched networks, the network takes care of collision detection and avoidance. Some traditional fieldbus protocols have achieved no-collisions with the use of a master/slave approach. Master is always in charge of the network and the slave nodes will talk only when spoken to. See the figure 6 below for a comparison of some fieldbus protocols and their industrial ethernet counterparts.

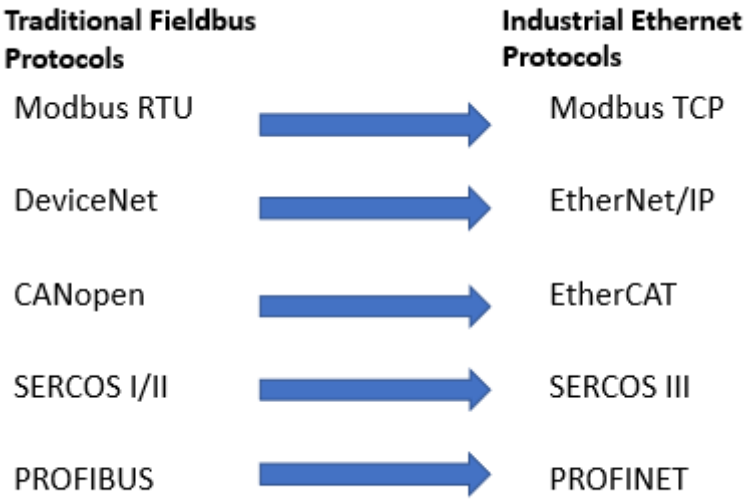

Figure 6. Some fieldbus protocols and their industrial ethernet counterparts.

Back in the day when Ethernet was originally developed in the 1970s, devices could transmit data one at a time and all devices could 'see' all the data as the original Ethernet used bus topology. If two devices would start transmitting at the same time, then the CSMA/CD (Carrier Sense Multiple Access/Collision Detection) access method would mean that the devices would withdraw and retransmit again after a random delay. While suitable for the networks back in the day, nowadays it does not provide any guarantee when an ethernet frame would arrive at the destination.
Today the access method for Ethernet is the same, but switches are utilized in our networks so that the network topology changes from bus topology into a star topology which means that the devices only see the data that is addressed to them. This has made it possible to use ethernet in deterministic applications as the latency and predictability of native ethernet is much better.
The reaction time of TCP/IP networks can limit the usage of Ethernet in real-time crucial applications as the latency can often be higher than

100 ms. Nevertheless with various strategies, the real-time capabilities can be approached. Many industrial ethernet protocols attempt to handle determinism with the master/slave approach at Layer 7 in the OSI model which makes the timing of communication more predictable.

Deterministic applications can be divided into three categories. First of them being NRT (non-real time) applications – where quick response times are not necessary. These consist of business and management applications. The encapsulation approach is great for NRT applications. In this approach, the fieldbus data packet is encapsulated in a standard TCP or UDP packet. As the data is carried by TCP/IP, standard network hardware can be used.

Second category is SRT (Soft real-time), which can provide real-time communication response times up to 100 ms. SRT is used in higher level control applications, where a strict master/slave communication is maintained. In this approach the data is encapsulated directly and it does not use the TCP/IP protocol suite, therefore making the communication more deterministic.

Third category, IRT (Isochronous real-time) provides real-time messaging for systems like motion control and such where response times of sub-millisecond are depended on. In this approach, the Ethernet protocol itself is modified on layer 2 of the OSI model. Examples of these approaches on the figure 7 below. (Johnson, Determinism in industrial ethernet, 2009b); (EPSG, 2016)

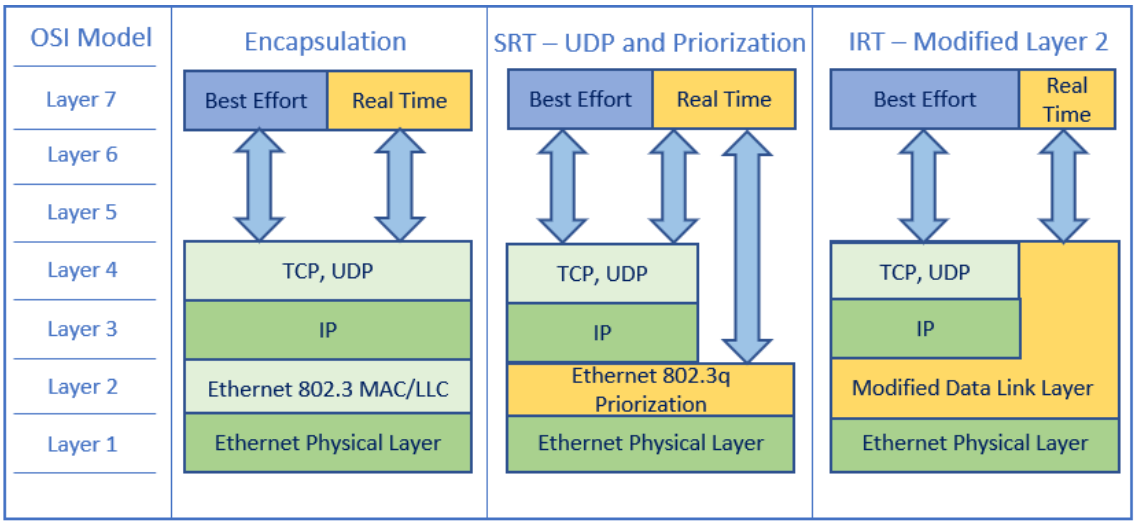

Figure 7. Three different methods to implement industrial ethernet protocols.

4.3.1 PROFINET

Profinet (Process Field Network) is an open Industrial Ethernet standard developed by PI (Profibus & Profinet International). It is based on the IEEE802.3 standard. Profinet provides multiple different communication methods suited to cover various timing requirements.

Profinet NRT (Non real-time) uses standard UDP/IP protocols and in some cases the RPC (Remote Procedure Call) protocol and as the name states it has no real time requirements. It should be used for applications like diagnostic tools and setting up connection between the device and the controller. Response times can be expected to be approximately 100 ms. Profinet NRT uses the whole OSI stack for its communications and while there are benefits such as all the information a UDP/IP packet has inside of it: MAC addresses, IP addresses and UDP port information can all be used to help the network switch handle and process the Profinet data. However, it brings some downsides as well. Each layer in the OSI model adds workload to the transmission of Profinet data as the data needs to be packed and unpacked at the source and destination. Also using the network layer adds some latency between the sender and receiver. Both downsides increase the latency and jitter of the network. Latency meaning the delay between the transmitter and the receiver, that is predictable. Jitter means the variance of time between every packet, thus lower latency and jitter is essential for deterministic networking. Profinet NRT runs on standard network equipment.

Profinet RT (Real Time) should be chosen for soft real time requirements. Such as applications like factory automation. Profinet RT channel skips the encapsulation portion entirely on OSI model's Network, Transport and Session layers. This results in low latency and jitter during the transmission of packets. The RT channel has a major downside though, it does not have any IP address because it does not use Network layer. The lack of IP address means that RT packets cannot be routed between LANs (Local Area Network). Using NRT channel adds flexibility, but it also adds 108 extra bytes for each packet compared to RT channel. The RT channel has cycle times ranging from 5ms to 10ms. Profinet RT uses a standard network switch. See a comparison of network packets on the RT and NRT channels on the figure 8 below.

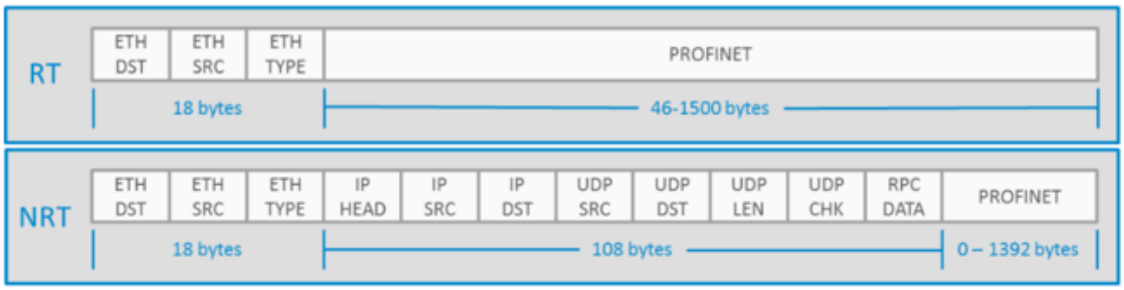

Figure 8. A comparison of packets on the RT and NRT channels. (Profinet University, 2019)

Finally, Profinet IRT (Isochronous real-time) channel should be chosen for applications like motion control because of its ability to achieve cycle times of less than 1ms and jitter of less than 1µs. IRT basically time-synchronizes the network. IRT channel is in many ways similar to RT channel, except that Profinet designed a MAC-layer extension to the regular IEEE 802.3 Ethernet to add an "express lane" of sorts for IRT traffic. As you know the regular

Ethernet uses the CSMA-CD method to avoid collisions on the network and devices can transmit whenever they please. This MAC-layer extension adds TDMA (Time Division Multiple Access) method to work part-time along the CSMA-CD method. How IRT works is say you want to allocate 25 % of the network's bandwidth to IRT traffic. The network would be then split into four time slices, IRT traffic running through one of them and the rest would be regular RT traffic. 25 % of the time other traffic will not go through as the bandwidth is reserved for IRT. Once the IRT traffic has gone through, the buffered RT traffic can continue. To use Profinet IRT, every network device on the IRT network has to be certified to Profinet's Conformance Class C. The network does not necessarily need new switches, but regular switches have to be modified in order to work with IRT. Siemens ASIC-chip is however needed on the switch. (Icpdas, 2013);(Profinet University, 2019); (Profinet University, 2019)

Profinet has other features as well. Profinet is fully downward compatible to Profibus. It supports hot plugging – you can add and remove devices from the network while its running. Tree, star, ring and daisy-chain network topologies are supported. Reduced jitter can be achieved with Profinet IRT. (EPSG, 2016)

4.3.2 EtherNet/IP

EtherNet/IP (Industrial Ethernet Protocol) was formerly developed by Rockwell Automation and is currently managed by ODVA (Open DeviceNet Vendors Association). EtherNet/IP supports all the transport and control protocols used in traditional Ethernet so this makes it usable with most of the Ethernet devices available in the current market. It is also one of the more popular industrial ethernet communication systems.

EtherNet/IP makes use of the encapsulation method, but also modifies regular ethernet by adding CIP (Common Industrial Protocol) at layer 7. CIP allows for plug-and-play interoperability with devices from multiple vendors and multiple subnets. To use EtherNet/IP in time sensitive applications, you need to use CIP and some of its extensions. The extensions needed are CIP Motion, CIP Sync and CIP Safety. CIP Motion provides a real-time closed loop distributed motion control solution. CIP Sync provides time synchronization for EtherNet/IP. Finally, CIP Safety provides us with fail-safe communication between the network devices.
EtherNet/IP has two different data transmission types. The first is called explicit messaging. Explicit messaging uses the TCP protocol. It is used for NRT tasks such as reading/writing configuration parameters. The second type is called implicit messaging and it uses UDP to transfer real-time data such as control data from a remote device. EtherNet/IP also has these following features. Hot plugging to replace devices on the fly. All network topologies are supported. Fully downward compatible to DeviceNet. Jitter can be lowered greatly with IEEE 1588 extensions in all components. See the figure 9 below for the EtherNet/IP and other CIP-based protocol

stacks. (Johnson, Determinism in industrial ethernet, 2009b); (Leinonen, 2017); (EPSG, 2014)

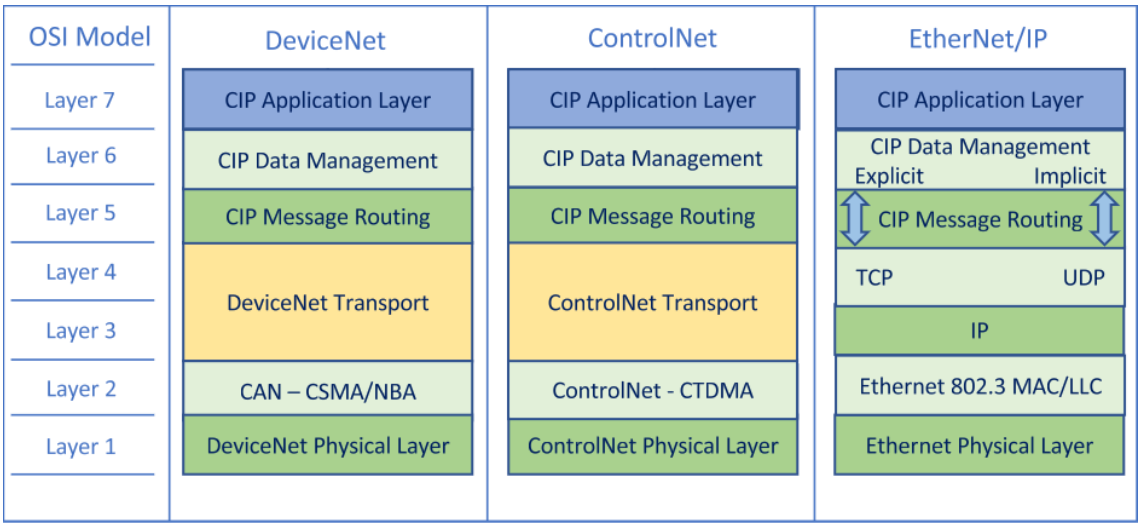

Figure 9. CIP-based protocol stacks.

4.3.3 Ethernet Powerlink

Ethernet Powerlink was formerly developed by B&R and it was first introduced in 2001. EPSG (The Ethernet Powerlink Standardization Group) took over the development of the technology in 2003. Powerlink is vendor-independent, free of any patents and it has a software-based communications system that can deliver true real-time performance. There is also a free of charge open source version available of Powerlink.

Ethernet Powerlink is based on CANopen. It uses the same device description files, object dictionaries, same communication mechanisms PDO (Process Data Objects), SDO (Service Data Objects) and NMT (Network Management). Basically the entire set of CANopen's mechanisms and it integrates it with Ethernet. Every application and device profile can be used in Powerlink environments and applications cannot tell the difference between CANopen and Powerlink, it can therefore be called as CANopen over Ethernet. Powerlink has features such as direct cross-traffic, hot plugging and every network topology is supported.

Powerlink uses timeslotting and polling to achieve these true real-time capabilities. A PLC is designated to be a MN (Managing Node) and it enforces correct time synchronization amongst all the devices. All other devices are called CN (Controlled Nodes) in these cycles. A cycle in Powerlink has three periods. First being the 'Start Period' which is the time synchronization phase. Second period is called 'Cyclic period' and isochronous data exchange is done here which means the time-sensitive network traffic. Third period is the 'Asynchronous phase' which handles rest of the network traffic, all non-time critical data and this is done over TCP/IP. On the OSI model for Powerlink, the data link layer is split into two sub-layers. Lower being the MAC-layer and upper the LLC-layer (Logical link control). See the figure

10 below for the OSI-model for Powerlink. (EPSG, 2016);(EPSG, 2014); (EPSG, 2009)

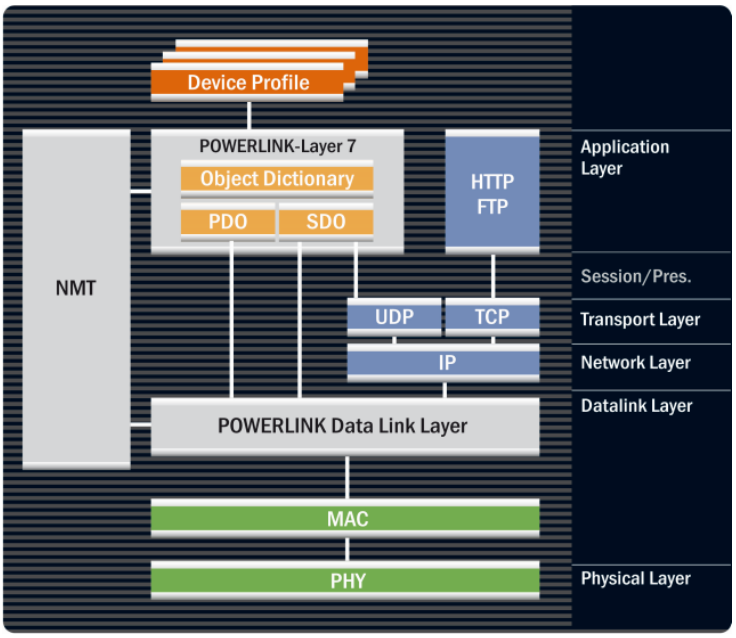

Figure 10. An OSI-model of the Powerlink protocol stack. (openPOWERLINK, 2020)

5 TUNNELING PROTOCOLS

Tunneling protocols essentially make it possible to communicate between two networks by forming a tunnel between them over WAN (Wide Area Network). The point of tunneling is to make it possible to transfer a communication protocol over a network that does not normally support it.

There is a wide variety of tunneling protocols. Layer 2 and 3 being more common. In this thesis, I am interested in layer 2 tunneling protocols as fieldbuses used in automation technology are not routed natively through layer 3.

The network traffic that goes through the tunnel uses pre-configured routes to the destination device. A tunnel has two end points and both ends have a gateway device. The gateway's ports can either be ingress or egress. The port on the transmitting side of tunnel is ingress and it encapsulates the frames that are being sent with a specific tunneling header and then proceeds to send it through the tunnel. The encapsulation makes the transfer of layer 2 frames over layer 3 network possible. As the frames have been encapsulated, every router that the frame goes through will know where to forward the frames. This will also make routing faster as each node does not have to read the frame and search for its next hop. On the other end of the tunnel, there is the egress port. The encapsulation of the frame is removed here and the frame leaves the tunnel. See the figure 11 below for a demonstration of a tunnel's architecture. (Luo, Pignataro, Bokotey, & Chan, 2005);(Leinonen, 2017)

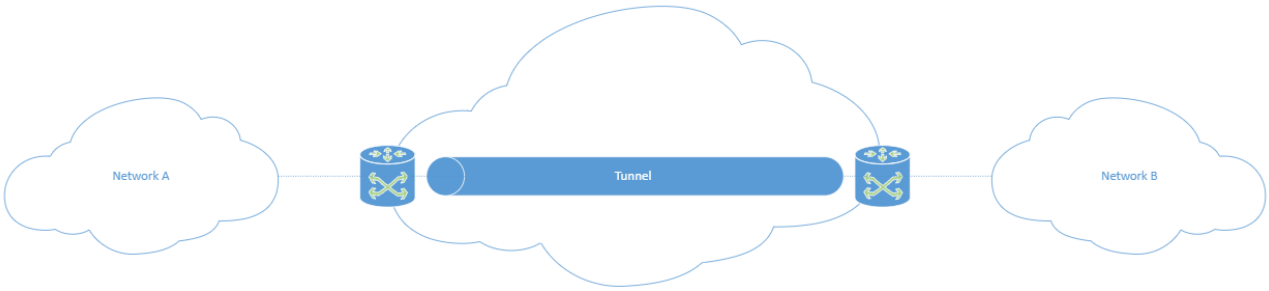

Figure 11. Basic tunnel architecture.

In this section I will be covering several tunneling solutions suitable for automation purposes. The tunneling protocols chosen were selected with the following criteria: The protocols must be suitable for Cisco's network equipment used in the practical part of the thesis and they must be suitable to use with at least Profinet's data.

5.1 IPsec – Internet Protocol Security

IPsec (Internet Protocol Security) is a layer 3 security protocol suite part of TCP/IP stack used to provide secure communication between two devices over an IP network. IPsec provides authentication, integrity and confidentiality for the data. It can be used to encrypt application layer data, to provide secure transmission of data for routers that are sending routing data across the public internet, it provides authentication without encryption or to protect your network data by using IPsec tunneling.

IPsec consists of three components. ESP (Encapsulating Security Payload), AH (Authentication Header) and IKE (Internet Key Exchange). ESP provides connectionless data integrity, encryption, authentication and anti-replay. AH has all the same features as ESP, except it does not provide encryption. IKE is a network security protocol that exchanges encryption keys and it provides message content protection.
IPsec uses UDP port 500 to forward ISAKMP (Internet Security Association and Key Management Protocol) through the firewall. IPsec also uses IP protocols 50 and 51 to forward ESP and AH traffic. (DeSot, 2019)

5.2 GRE – Generic Routing Encapsulation

GRE (Generic Routing Encapsulation) is a tunneling protocol developed by Cisco. GRE is defined by IETF standard (RFC 2784). It is able to encapsulate wide amount of protocols inside layer 3 IP tunnels, which creates a virtual point-to-point link between the routers.

GRE has the following characteristics:

- GRE is hardware reliant. Both end-devices of the tunnel has to support it.
- It is identified as IP protocol 47.
- The encapsulation in GRE includes a protocol type field in its header for multiprotocol support. These are defined as EtherTypes in RFC 1700.
- By default, GRE does not include any flow-control mechanisms.
- GRE does not provide any encryption for the encapsulated packet, so it should be considered to use a separate security protocol along with GRE if data protection is needed.
- GRE's packet header has at least 24 bytes of additional overhead for tunneled packets.

Creating a GRE tunnel is easier than with other tunneling protocols. GRE uses the existing routing tables of two routers to create a tunnel. GRE supports VPN (Virtual Private Network) over the network. It can also transfer broadcast and multicast packets alongside of unicast packets. Meaning that packets can be transferred from one device to another via unicast, from one device to all possible devices via broadcast or from one device to multiple devices via multicast. One major downside to GRE is its lack of encryption for the the encapsulated packet. If data protection is needed and a security protocol is needed, one possible solution is IPsec.
(Cisco Networking Academy, 2017); (Cisco, 2014a); (Leinonen, 2017); (Microsoft, 2009)

5.3 L2TPv3 – Layer 2 Tunneling Protocol version 3

L2TPv3 (Layer 2 Tunneling Protocol version 3) is a tunneling protocol which as the name suggests, allows the tunneling of layer 2 protocols over IP network. L2TPv3 is an IETF standard (RFC 3931). It is the newest version of L2TP and it is developed by IETF. L2TPv3 is identified as the protocol number 115.

In L2TPv3, layer 2 frames are encapsulated within L2TPv3 frames when tunneled. It was originally meant to be used with PPTP (Point-to-Point Tunneling Protocol), but it has since been developed to support many other layer 2 protocols. It is a combination of Cisco's L2F (Layer 2 Forwarding protocol) and Microsoft's PPTP. Version 3 of L2TP includes support for VLANs (Virtual Local Area Network), ability to transfer layer 2 frames over IP network and Ethernet Port-to-Port. A major downside of L2TPv3 is that it supports only point-to-point, but not multipoint tunnels. L2TPv3 also requires certain type of routers that support it.

L2TPv3 does not provide any cryptographic security, which means that a third-party security protocol must be used, if encryption is needed. The

standard RFC 3931 however states that the support for IPsec is mandatory. IPsec is also the recommended security protocol to use with L2TPv3. (Cisco); (Cisco, 2014b); (Leinonen, 2017); (Lakshman & Lobo, 2006)

5.4 OpenVPN

OpenVPN is a software-based VPN solution developed by OpenVPN Technologies Inc. It is open source and the license is free for two devices. The client has to be installed on both devices. One end-device has to be designated as the server and another as the client. OpenVPN supports Linux, Windows, OpenBSD, FreeBSD, NetBSD, Mac and Solaris.

OpenVPN can create either a TCP or UDP tunnel and the data is encrypted inside of the tunnel. OpenVPN supports layer 2 and 3 tunnels, but TAP/TUN network drivers must be used. TAP (Terminal Access Point) operates in layer 2 and will be used to create a layer 2 tunnel. TUN (network TUNnel) operates on layer 3 and is used to create layer 3 tunnels. TUN/TAP drivers are available natively on Linux 2.4 or newer, but is supported on every platform.

OpenVPN makes use of TLS (Transport Layer Security) to exchange keys. OpenSSL library is used for encryption of the data. OpenVPN does not support IPsec or IKE, it uses a custom security protocol based on SSL (Secure Sockets Layer) and TLS instead. (openmaniak, 2011); (Krasnyansky, 2001); (OpenVPN, 2020)

6 MEASUREMENT SETUP

One tunneling technology was chosen for testing in real environment, because it was most relevant for the company. It was decided to create a measurement plan instead of testing in real environment. Jitter, latency, cycle time and throughput are measured to define the performance when the traffic is tunneled. First, a tunnel has to be created between the two LANs.

The plan was to construct a VPN tunnel between a Cisco ISR 5G router and a Cisco ASA. One possible choice would be to create the tunnel with L2TPv3 or by using Cisco's GRE, but that would require some tinkering since later firmware versions of Cisco ASA do not support terminating of GRE tunnels. L2TPv3 and GRE are not secure by themselves so IPsec should be used with them.
A BANY scope (Siemens Bus Analyzer) was planned to be used to monitor jitter and cycle time deviation of Profinet frames when they are tunneled. It is connected to the 5G router on the crane's side. An external PC with iperf3 should be used to monitor the throughput of the connection and

latency with the ping command. See the figure 12 below for architecture of our build network.

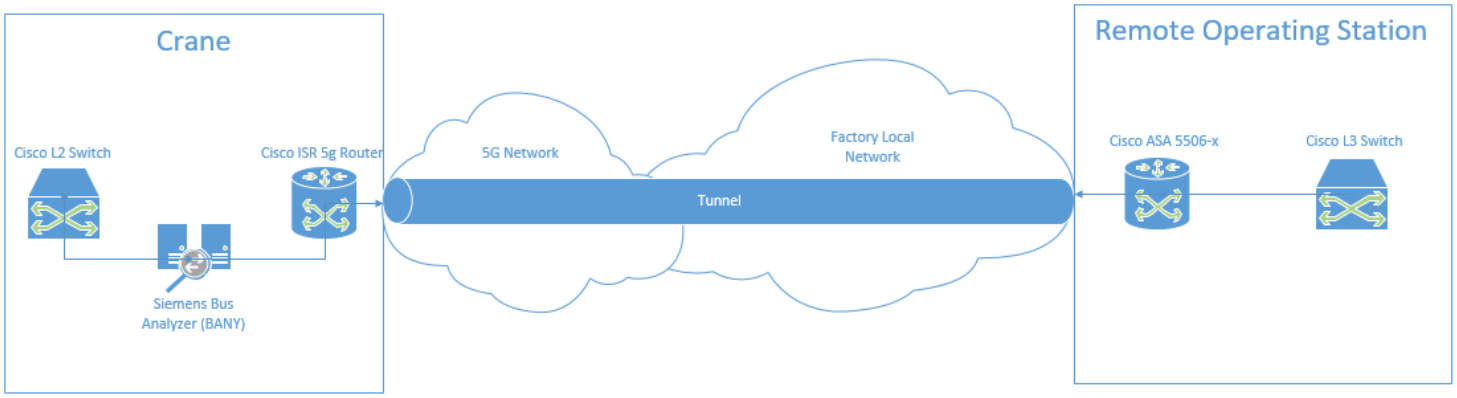

Figure 12. Architecture of the build network.

I also wanted to test what kind of effect would a handover of the connection from one 5G cell to another have on the performance of the connection. The crane site has 5G cells set within certain distance of each other and the handover is set to happen when the crane moves and the signal of one cell starts to weaken. This could be measured either with the ping command or BANY scope. See the figure 13 below for an example of the crane site setup and the table 1 for a table that can be used to report the measurement results. (Andrea, 2012)

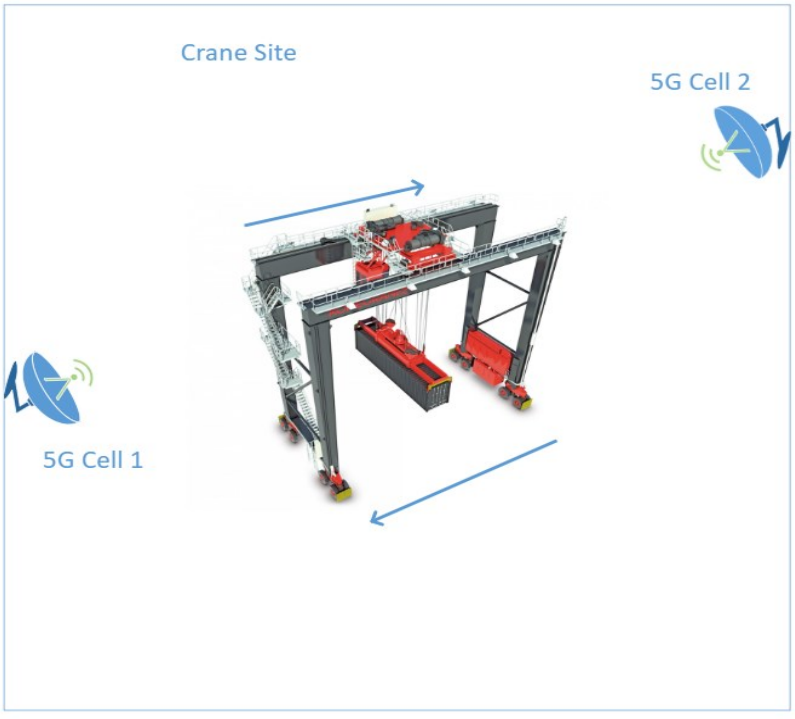

Figure 13. An example of the crane site setup.

Table 1. Table for the measurement results.

	L2TPv3 over IPsec	GRE over IPsec	OpenVPN
Jitter			
Latency			
Cycle time			
Throughput			

7 CONCLUSIONS

The purpose of this thesis was to provide a comparison of different tunneling solutions capable of encapsulating layer 2 traffic and to provide knowledge of various other technologies that could potentially be used.

In the beginning of the thesis I covered some basic networking theory such as the OSI-model, its layers, and how it functions, and also various network topologies that were of interest for this thesis. Then I covered information on 5G, its features, and how it is developed. Next I researched time-sensitive networking, Ethernet, and fieldbus protocols. This was probably the most difficult chapter to research and write on as I knew nothing of automation prior to this thesis. After writing this thesis, I feel like I know at least the necessary basics of networking in automation. After that I wrote on tunneling protocols which was an easier subject for me as I have had some previous experience working with those. I presented three potential tunneling protocols to use. In chapter six, I present our setup and how the measurements could be done.

The thesis shows that, L2TPv3 over IPsec should be used as the tunneling protocol, because it is supported by both end-devices and it should be relatively simple to setup. Additionally, Profinet should be used as the fieldbus protocol, because it is already in use. There is no significant benefit to use any other fieldbus protocol in this case, because the whole infrastructure would have to be changed. However since only soft real-time requirements are needed, the other presented fieldbuses could very well be considered. With the information presented on this thesis it should be easier choose from other protocols in the future. The real environment measuring and comparing of different tunneling protocols should be relatively simple to do with the information researched about the topic in this thesis.

REFERENCES

3GPP. (2018). *Release 15*. Retrieved May 27, 2020, from https://www.3gpp.org/release-15

3GPP. (2019a). *Release 16*. Retrieved May 27, 2020, from https://www.3gpp.org/release-16

3GPP. (2019b). *Release 17*. Retrieved May 27, 2020, from https://www.3gpp.org/release-17

Allen, L. (2018). *Top 5 features of 3GPP Release 15*. Retrieved May 27, 2020, from https://www.rcrwireless.com/20181211/5g/3gpp-release-15

Anderson, M. (2019). *What is fieldbus?* Retrieved April 1, 2020, from https://realpars.com/fieldbus/

Andrea, H. (2012). *Configuring GRE Tunnel Through a Cisco ASA Firewall*. Retrieved May 28, 2020, from https://www.networkstraining.com/configuring-gre-tunnel-through-a-cisco-asa-firewall/

Cisco. (2011). *Networking Fundamentals.* Retrieved April 1, 2020, from https://www.cisco.com/c/dam/global/fi_fi/assets/docs/SMB_University_120307_Networking_Fundamentals.pdf

Cisco. (2014a). *GRE Tunneling Feature Guide.* Retrieved May 14, 2020, from https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/catalyst3850/software/release/16-1/workflows/gre-feature-guide.pdf

Cisco. (2014b). *Layer 2 Tunnel Protocol Version 3 Software Configuration Guide.* Retrieved May 15, 2020, from https://www.cisco.com/c/dam/en/us/td/docs/routers/connectedgrid/cgr1000/ios/software/15_4_1_cg/OL-31238-01.pdf

Cisco. (n.d.). *Implementing Layer 2 Tunnel Protocol Version 3.* Retrieved May 15, 2020, from https://www.cisco.com/c/en/us/td/docs/routers/crs/software/crs_r4-1/lxvpn/configuration/guide/vc41crs/vc41tpv3.pdf

Cisco Networking Academy. (2017). *Branch Connections - GRE*. Retrieved May 14, 2020, from https://www.ciscopress.com/articles/article.asp?p=2832406&seqNum=7

Cloudflare. (2018). *What is the OSI Model?* Retrieved April 1, 2020, from https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

Contreras, S. (2020). *Explaining 5G: Millimeter wave, sub-6, low-band and other terms you need to know*. Retrieved April 1, 2020, from https://www.androidcentral.com/explaining-5g-millimeter-wave-sub-6-low-band-and-other-terms-you-need-know

DeSot, T. (2019). *What is IPSEC?* Retrieved May 19, 2020, from Digital Defense: https://www.digitaldefense.com/blog/internet-protocol-security-explained/

EPSG. (2009). *POWERLINK Basics.* Retrieved April 17, 2020, from https://www.ethernet-powerlink.org/uploads/media/POWERLINKBasics_brochure_e.pdf

EPSG. (2014). *Using Real-Time Ethernet as a Backbone to Optimize Machine Performance.* Retrieved April 14, 2020, from https://www.ethernet-powerlink.org/fileadmin/user_upload/Dokumente/Downloads/Whitepapers/Automation_Machine_Performance.pdf

EPSG. (2016). *Industrial Ethernet Facts.* Retrieved March 31, 2020, from https://www.br-automation.com/downloads_br_productcatalogue/BRP4440000000000000446143/EPSG_IEF3rdEdition_en_Web%20MM-BR-PL-IEF-EN-03.pdf

Ericsson. (2019). *5G evolution: 3GPP releases 16 & 17 overview*. Retrieved May 27, 2020, from https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-nr-evolution

Frenzel, L. (2009). Retrieved April 1, 2020, from https://www.electronicdesign.com/technologies/communications/article/21778595/ethernet-a-history

Gigabyte. (2018). *A Smart City Solution with 5G mMTC Technology*. Retrieved May 27, 2020, from https://www.gigabyte.com/Solutions/Networking/mmtc

Grant, M. (2019). Retrieved April 1, 2020, from https://www.investopedia.com/terms/s/standardization.asp

Icpdas. (2013). *PROFINET Introduction*. Retrieved March 31, 2020, from https://www.icpdas.com/root/product/solutions/industrial_communication/fieldbus/profinet/profinet_intro.html

International Telecommunication Union. (2017). *Minimum requirements related to technical performance for IMT-2020 radio interface(s).* Retrieved April 1, 2020, from https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf

Johnson, G. (2009a). *Determinism in industrial ethernet: A technology overview - Part 1*. Retrieved April 1, 2020, from https://www.processonline.com.au/content/industrial-networks-buses/article/determinism-in-industrial-ethernet-br-a-technology-overview-part-1-678679974

Johnson, G. (2009b). *Determinism in industrial ethernet*. Retrieved April 1, 2020, from https://www.processonline.com.au/content/industrial-networks-buses/article/determinism-in-industrial-ethernet-br-a-technology-overview-part-2-966929628

KeyCDN. (2018). *What Is Latency and How to Reduce It*. Retrieved April 1, 2020, from https://www.keycdn.com/support/what-is-latency

Krasnyansky, M. (2001). *Virtual Point-to-Point(TUN) and Ethernet(TAP) devices*. Retrieved May 28, 2020, from http://vtun.sourceforge.net/tun/faq.html#1.1

Lakshman, U., & Lobo, L. (2006). *L2TPv3 Overview*. Retrieved May 15, 2020, from https://flylib.com/books/en/2.686.1/l2tpv3_overview.html

Leinonen, M. (2017). *Trepo.* Retrieved March 14, 2020, from Tampereen Yliopisto: https://trepo.tuni.fi/bitstream/handle/123456789/25059/Leinonen.pdf

Luo, W., Pignataro, C., Bokotey, D., & Chan, A. (2005). *Layer 2 VPN Architectures.* Pearson Education. Retrieved April 1, 2020

Microsoft. (2009). *What is IPSec?* Retrieved May 14, 2020, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc776369(v=ws.10)?redirectedfrom=MSDN

Nordrum, A., Clark, K., & Staff, I. S. (2017). *5G Bytes: Beamforming Explained*. Retrieved April 1, 2020, from https://spectrum.ieee.org/video/telecom/wireless/5g-bytes-beamforming-explained

openmaniak. (2011). *What is OpenVPN?* Retrieved May 28, 2020, from http://openmaniak.com/openvpn.php

openPOWERLINK. (2020). *Protocol Architecture.* Retrieved April 16, 2020, from http://openpowerlink.sourceforge.net/web/kategorien/POWERLINK/dateien/IMG_POWERLINK_OSI_Model.png

OpenVPN. (2020, May 28). *Site-To-Site Layer 2 Bridging Using OpenVPN Access Server And A Linux Gateway Client*. Retrieved from https://openvpn.net/vpn-server-resources/site-to-site-layer-2-bridging-using-openvpn-access-server/

Passoja, M. (2018). *5G NR: Massive MIMO and Beamforming – What does it mean and how can I measure it in the field?* Retrieved April 1, 2020, from https://www.rcrwireless.com/20180912/5g/5g-nr-massive-mimo-and-beamforming-what-does-it-mean-and-how-can-i-measure-it-in-the-field

Profinet University. (2019). *Isochronous Real-Time (IRT) Communication*. Retrieved March 31, 2020, from https://profinetuniversity.com/profinet-basics/isochronous-real-time-irt-communication/

Profinet University. (2019). *PROFINET Communication Channels*. Retrieved March 31, 2020, from https://profinetuniversity.com/profinet-basics/profinet-communication-channels/

Qualcomm. (2017). *Everything You Need to Know About 5G*. Retrieved April 1, 2020, from https://www.qualcomm.com/invention/5g/what-is-5g

Singh, C. (2019). *Computer Network Topology – Mesh, Star, Bus, Ring and Hybrid*. Retrieved April 1, 2020, from https://beginnersbook.com/2019/03/computer-network-topology-mesh-star-bus-ring-and-hybrid/

Varis, P., & Leyrer, T. (2018). *Time-sensitive networking for industrial automation.* Retrieved April 1, 2020, from http://www.ti.com/lit/wp/spry316a/spry316a.pdf

Voss, W. (2019). *Industrial Ethernet Guide - Introduction to Fieldbus Systems*. Retrieved April 1, 2020, from https://copperhilltech.com/blog/industrial-ethernet-guide-introduction-to-fieldbus-systems/