Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Information Security and Communication Technology

Jens Rønneberg

Reference Topologies and Scenarios for Cyber-Physical Systems in the Norwegian Cyber Range

Master's thesis in Information Security
Supervisor: Prof. Stephen D. Wolthusen
June 2019

NTNU
Norwegian University of
Science and Technology

Jens Rønneberg

Reference Topologies and Scenarios for Cyber-Physical Systems in the Norwegian Cyber Range

Master's thesis in Information Security
Supervisor: Prof. Stephen D. Wolthusen
June 2019

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Information Security and Communication Technology

Preface

This thesis concludes my master's degree in the field of Information Security at Norwegian University of Science and Technology in Gjøvik. It was performed throughout the spring semester of 2019 and deals with performance attacks on smart grid and smart home automation networks. The research questions was formulated together with my supervisor, professor Stephen D. Wolthusen and dr. Vasileios Gkioulos. Performing the research was difficult, but conducting extensive investigation has allowed me to answer the question that we identified. Citations will be shown as the number of specific reference within brackets like this: [1] which will link to the source list at the end of the report.

01-06-2019

Acknowledgment

I would like to thank my supervisors, professor Stephen D. Wolthusen and dr. Vasileios Gkioulos. They were always there to provide me with advice and assistance whenever I needed it. They consistently allowed this thesis to be my own work, but guided me in the right direction whenever they thought it was needed.

Finally, I would like to express the earnest thanks to my parents and my two sisters for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

J.R.

Abstract

Cyber-physical systems (CPS) are engineered systems of cyber and physical components that interact with the possible help of human interaction. CPS is being used in critical infrastructure sectors such as energy systems and health care, but also other areas such as manufacturing, smart cities, and smart home automation. These systems are already subjected to attacks. The primary objective of this thesis was to model and simulate CPS topology for an energy system and a smart home automation system. An understanding of a "normal operation condition" of the two systems has been established, as well as identifying the fundamental architectural characteristics and communication protocols. The created topologies have been translated into network simulation environments using a simulation tool called OMNeT++, and mock control and information flows have been designed to capture the master/slave hierarchies. Both of the simulated systems have then been the test subjects for two selected sets of network attack scenarios, particularly targeting real-time performance characteristic. The attack scenarios are based on TCP and UDP flood attacks, and their impact on the system was evaluated. PMUs in the smart grid system and the surveillance camera and the gateway in the smart home system showed an increase in the end-to-end delay and jitter during the attacks. This caused a temporal delay on the systems and the impact was minor issues and do not affect the overall state.

Abstract

«Cyber-physical systems» (CPS) er systemer som er konstruerte av cyber- og fysiske komponenter, og som samhandler med mulig hjelp av menneskelig interaksjon. CPS brukes i kritiske infrastruktursektorer som energisystemer og helsevesenet, men også andre områder som industri, smarte byer og smart hjem-automatisering. Disse systemene er allerede utsatt for angrep. Hovedmålet med denne oppgaven er å modellere og simulere CPS-topologier for et energisystem og et smart hjem-automatiseringssystem. I oppgaven blir en forståelse av en "normal driftstilstand" for de to systemene etablert, og de grunnleggende arkitektoniske egenskapene og kommunikasjonsprotokollene blir identifisert. De opprettede topologiene er blitt oversatt til nettverkssimuleringsmiljøer ved hjelp av et simuleringsverktøy kalt OMNeT++, og mock kontroll og informasjonsflyt er utformet for å fange master/slave-hierarkiene. Begge de simulerte systemene har vært testobjekter for to utvalgte sett med nettverksangrepsscenarioer, spesielt rettet mot sanntids-ytelseskarakteristikk. Angrepsscenarioene er basert på TCP- og UDP-flomangrep, og deres innvirkning på systemet blir evaluert. PMUer i smart grid-systemet, overvåkningskameraet og gatewayen i det smarte hjemmesystemet viste en økning i ende-til-ende-forsinkelsen og jitter under angrepene. Dette førte til en tidsforsinkelse på systemene, men effekten var mindre problematisk og påvirket ikke den generelle tilstanden.

Contents

List of Figures

List of Tables

Listings

1 Introduction

Cyber-physical systems refer to a new generation of systems which tightly integrate cyber and physical components. Smart grid and smart homes automation systems are areas where cyber-physical systems have been implemented. In this master thesis I have created a topology model for smart grid and smart home with artifacts and real-time operational characteristics. These two topologies have been translated into network simulation environments, using a network simulation tool. This allowed simulation of traffic in the different systems. Two network attack scenarios have been created and were carried out on the simulated topologies and the effects of the attack scenarios has been validated.

1.1 Keywords

Cyber Range; Cyber-Physical System (CPS); Cyber Security; Modelling; Electric Grid; Smart Grid; Attack Strategy;

1.2 Problem description

Cyber-physical systems (CPS) are engineered systems of cyber and physical components that interact with the possible help of human interaction. CPS is being used in critical infrastructure sectors such as energy systems and health care, but also other areas such as manufacturing, smart cities, and smart home automation. It is possible to recreate these types of systems in a controlled virtual environment called cyber range. This virtual environment is used for providing a safe, legal environment for conducting security posture testing. The CPS are already subjected to attacks and these types of attacks are essentially similar to those attacks that targets communication and information technology systems. The difference is the goal and effects of the CPS attacks. The most famous CPS attack is Stuxnet which is said to have been operating undetected for more than three years. Its targes was to make physical damage to an industrial infrastructure.

The purpose of the master thesis is to model and simulate a CPS topology for an energy system and a smart home automation system using simulation tools. The creation of smart electric grid was to meet future demands within electricity for reliable energy and numerous technological advancements. While technologies will help achieve the future demands, they also present a dependency on cyber resources, and these resources may be vulnerable to attacks. The effects of an attack can possibly affect a lot of people, and an example of this is the attack in Ukraine where three Ukrainian regional electric power distribution companies were the victims to coordinated cyber-attacks. This resulted in power outages that affected thousands of costumers for several hours.

A modeled and simulated energy system and smart home system will be the test subjects for conducting a security posture testing within the context of the cyber range established at NTNU.

The security posture testing have contained a selected set of network attack scenarios, particularly targeting real-time performance characteristics, in the simulation framework.

1.3 Motivation

Regardless of the convenience a CPS brings to the user's daily life, might also expose them to a wide range of threats. The CPS can put the system and the users at risk for their own privacy and safety. There are several examples of attacks against CPS, which have been illustrated above.

The master thesis have examined threats and vulnerabilities where the smart grid and smart home systems are exposed to. This will contribute to a better knowledge about the threats and the effects of a network attack, targeting real-time performance characteristics, will have on a system. It will also create awareness of what type of damages a threat can do, which can help the product developers in the energy grid and smart home industry.

1.4 Research questions

Based on the background, problem description and motivation, the following research questions have been examined throughout the thesis:

1. How can reference scenarios efficiently and effectively capture the real-time operational characteristics of CPS in CI sectors?
2. How can topological models capture artifacts and operational real-time characteristics of CPS in CI sectors, providing high fidelity and reproducibility?
3. How can topological models be translated into network simulation environments allowing simulation of traffic over these topologies?
4. What type of real-time information and control flows are there in the chosen cyber-physical systems?
5. How will a CPS in CI real-time performance characteristics be affected by different network attacks, like packet dropping and message delays?

1.5 Planned contributions

This thesis have developed topologies for the environments and created attack scenarios addressing the effects that the network attacks will have on the systems. This may prevent any potential attacks or security threats in the future product release. To create a picture of potentially vulnerabilities and threats in the systems that will help increasing security awareness. The goal of the master thesis is to contribute to the existing literature by giving a practical approach.

1.6 Thesis outline

Introduction: This chapter includes the introduction, keywords, research questions, background, project description, problem description, motivation, and planned contribution.
Related work: Looks at the previous work related to the thesis.
Methodology: This chapter will include project management plan, methodology for experimental

and literature review, and the ethical and legal consideration.
Theory on CPS: This chapter presents what CPS is and the CPS's operations. It will also present the main technologies used in the smart grid and smart home systems. Here we will look at security, privacy requirements and some background on security and privacy challenges for the smart grid and smart home system.
Reference topologies and scenarios for cyber-physical systems in the Norwegian cyber range: This chapter includes sub paragraphs with:

- Analysis of reference scenarios and control systems architectures found in the reference sectors.
- Creation of topological models manually, for the energy system and smart home automation system.
- Translation of topological models into network simulation environments with OMNeT++.
- Real-time information and control flow in the chosen CPS, primarily capturing the master/slave hierarchies in ICS.
- Investigation of a selected set of network attacks scenarios, targeting real-time performance characteristics.

Result: The outcome of the different attack scenarios and the validation.
Conclusion: Discussion and summarizing of the main contributions and results of the work. This chapter also includes suggested recommendation for continuing and expanding the current research.

2 Related work

The main focus of this thesis have been on the energy and smart home system architecture and how different attacks will affect their performance characteristics under different kind of attacks. This chapter will provide a literature review of modelling cyber-physical systems and various cyber-attack methods. The first sections 2.1 and 2.2 will provide the literature review of modelling energy systems and smart home automation. The section 2.3 and 2.4 introduces the different vulnerabilities and attack methods in the smart grid and smart home system.

2.1 Energy system modelling

The European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI) are the three European Standardization Organizations that develops and agrees on standards for smart grid in Europe. They have developed a security standardization document specific for smart energy grid [1]. In this document they present a smart grid architecture model and addresses cyber security on system level.

The components in the system are:

- **Customer relationship management (CRM) controller** – provides a point-of-contact and resolution for customers problems and issues.
- **Distribution management systems (DMS) controller** – refers to the real-time information system. This is used in dispatch centers and control rooms, and it is all the elements needed to support all the relevant operational activities including the functions. It is used to improve the information made available for the human interaction.
- **Head End System (HES)** – a central data system exchanging data of various meters in its service area.
- **Distribution Data Collector** – a device collecting data from multiple sources and modifies/-transforms it to different forms.
- **Distributed (Intelligent Electronic Device) IED** – This component receives data from sensor and power equipment. The IED can issue control commands, such as tripping circuit breakers. This can be done if there is current, frequency or voltage anomalies.
- **Distributed energy resource (DER) controller** – DER represents the distributed electrical resources which is directly connected to the public distributed grid. The DER controller will allow the adjustment of its active or reactive power output according to a received set point.

Figure 1 focuses on “component to component” communication with communication protocols and gives the appropriate data model standard for the information flow between the nodes. This model is developed for the overall information and communication technology architecture.

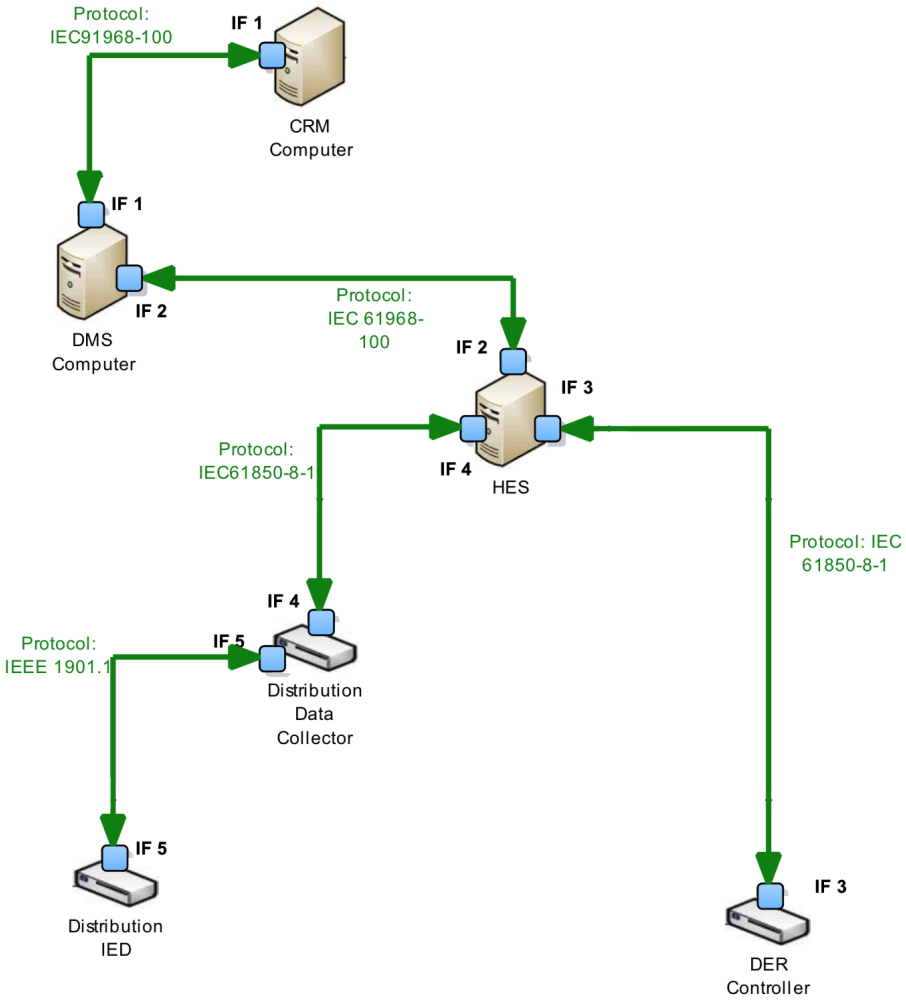


Figure 1: Smart Grid Architecture for communication layer [1].

Another organization that also publishes standards to provide guidance to the smart grid construction is the National Institute of Standards and Technology (NIST). The NIST Special Publication 1108R2 [2] is a roadmap for the standards on smart grid operations. The document presents a conceptual reference model and provides information about expected functions and services in a smart grid system. In addition, it describes the applications and the communication requirements needed in the implementation of smart grid. The document defines the conceptual reference model, specifies the security assessment procedures, identifies the implementation standards and states the importance of the smart grid.

A framework based on the Service Oriented Architecture for proactive transmission grid control

for a smart grid system is presented in [3]. This framework model is able to process, manage and share massive information. The goal of the framework is to construct an architecture that allows computing components to deliver much more automation.

2.2 Smart home automation modelling

Barman et al. [4] presents a home automation system with complete automation of door security, temperature control and lights. This system, with light sensors, allows a user to control the home appliances remotely over the Internet.

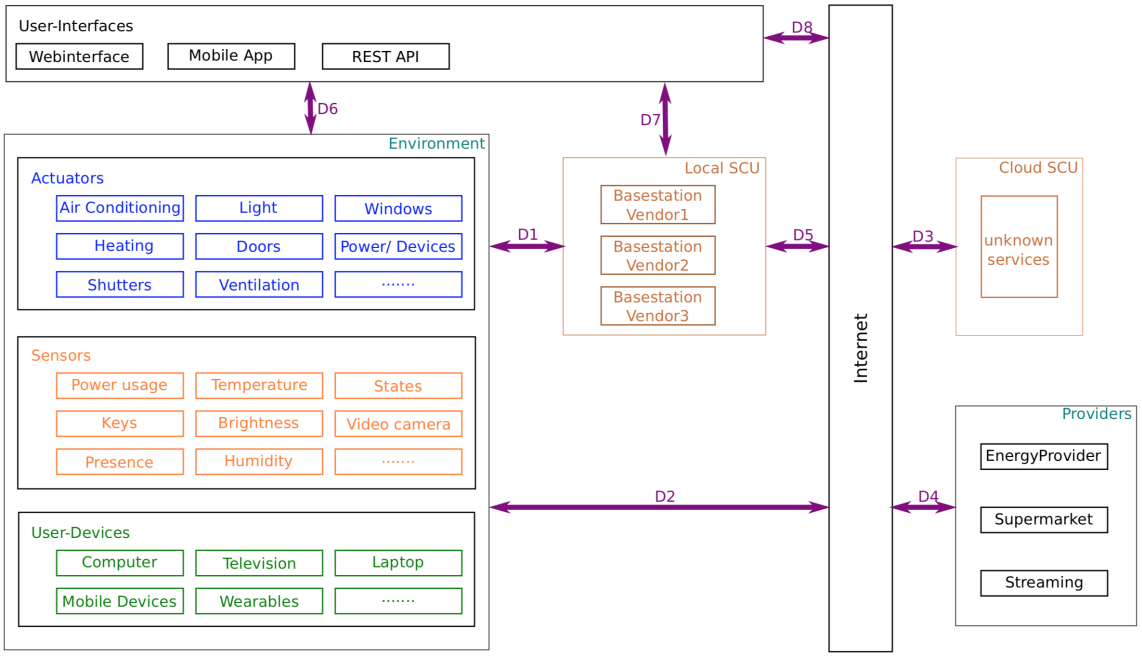


Figure 2: Smart Home Automation model [5].

Since todays home automation systems can control doors, windows and locks it is important to have security and privacy. There is a huge amount of data about the people in their homes. This information is important for making the life of the users easier, but this data can also be used to create movement profiles and to draw conclusions about the persons health situation. Based on this, a model with focus on security and privacy was developed, which is really important in a home automation system [5].

2.3 Smart grid vulnerabilities and cyber attacks

2.3.1 Smart grid vulnerabilities

In smart grids they use wireless sensors, access points and IP-based advances metering infrastructure for information and communication technology. Using this method to modernize the traditional

power grid opens up a way to access the cyber-physical system remotely. This will lead to opportunities for cyber threats and attacks on the system. Some protocols in smart grid systems are used to monitor and send control commands from different control centers to actuators and sensors. The power system infrastructure in smart grid relies on these protocols, which are Modbus and DNP3 [6].

Modbus protocol is a standard for the communication in many smart grids. Vulnerabilities in Modbus is the lack of basic security measures. The protocol makes the system vulnerable to a lot of different attacks. Its data integrity is questionable because of its lack of integrity checks [7]. A lack of encryption exposes the traffic to attacks like eavesdropping [8]. There are no authentication measures implemented in the protocol, which means manipulation of data traveling to actuators or from sensors to controllers is feasible. This could make to actuators act undesirably or send false data from sensors [9, 10, 11], which is also really similar to the DNP3 protocol that has CRC as integrity measure. CRC is a relatively simple integrity measure, but it is better than Modbus which doesn't have an integrity measure. Like Modbus, DNP3 does not have any implemented encryption or authentication mechanisms [12].

Recently IEC 61850 protocol has been introduced in the smart grid as an advancement of the communication protocols. The lack of authentication will open the possibilities to inject the network with nonsense packets that has the purpose of flooding the network, which will lead to denial of service attack [13].

A smart meter installed in the smart grid may have backdoors that an attacker could exploit. This will give the attacker the opportunity to take full control over this trusted device. A smart meter also relies on two-way communication that can give new vulnerabilities, which an attacker can exploit [14].

2.3.2 Smart grid cyber attacks

Communication protocols are vulnerable and there are a number of attacks exploiting these vulnerabilities. Spoofing attacks on address resolution protocol is one example demonstrated on Supervisory Control and Data Acquisition (SCADA) system [15]. This article demonstrates successful attacks through proof of concept on SCADA systems.

The traffic in smart grid systems are really time-critical, and delays in the network flow can have serious consequences. Performing a denial of service attack by flooding the network at different layers is one approach of denial of service attack. Lu et al. [16] performed an experiment to illustrate the impact on the delay performance under traffic flooding attacks in an experimental power network. The result of this experiment was that the delay performance would not degrade gradually as the attack intensity increases. Only when the traffic flood attack pours as much traffic as it could into the communication channel the delay performance in the power network was degraded.

Another denial of service approach is jamming attacks [17]. This experiment showed with real-time experiment and analytical analysis that it generally exists a phase transition phenomenon in time-critical applications under a jamming attack approach. A blackout is considered a denial of service attack in the context of smart grid. The most important security goal of a smart grid system

is to maintain the availability. If an attack is able to compromise the availability for a smart grid, this could result in a large-scale blackout. It could affect a lot of people.

False data in smart grids can lead to consequences like financial losses and service disruption. The article by Liu et al. [18] proposed a false data injection attack that exploits vulnerabilities in the current techniques aimed at detecting and identifying bad measurements for state estimation. This attack assumed that the attacker had access to the current power system configuration information. The false data injection manipulated the measurements of meters at a physically protected location. Through this experiment it showed that the attacker can impact the system by launching generalized false data injection.

Another type of false data injection was done by Li and Tang [9], who analysed a false data injection attack scenario. One scenario was to add a Gaussian noise to the innovation transmitted by the sensor. The other scenario was to attack the sensor to drop data packages and replace the innovation with a Gaussian noise. The attack scenarios showed that there is stealthier to use this type of attack scenario than a denial of service attack, because the false data injection does not undermine the integrity of the system. This will make it more difficult to detect the attack.

2.4 Smart home vulnerabilities and cyber attacks

2.4.1 Smart home vulnerabilities

Smart home automation system has a lot of house appliances with sensors controlled from a centralized unit. This type of technology like in smart grid, opens up for remote access and gives the opportunities for cyber threats and attacks on the system. A smart home automation system is heterogeneous and complex and therefore is deploying security a challenge. To implement security to the different devices varies. The environment consists of many devices with different mechanisms and purposes. Currently, there are a lot of protocols for the wireless network, used by different devices in the system. The protocols are used to make the devices communicate with each other. In regards of wireless technologies, there are: WiFi (802.11), IEEE 802.15.4, Bluetooth (IEEE 802.15.1), ZigBee, 6LoWPAN, Insteon, Wavenis, SimpliciTI, VM-Bus, EnOcean, Z-Wave, MQTT, BidCos, DECT, CoAP, and BACnet. Examples of different transmission mediums used for communication between devices are phone lines, wired links and radio communication. Because the devices often communicate wireless, it makes it possible for an intruder to capture the signals and even tamper with the normal operations of wireless technologies [19].

2.4.2 Smart home cyber attacks

Some smart homes use sensors to monitor and track movements in the home. This is also known as wireless sensor networks (WSN). The WSN has become a target for different kinds of attacks. Jamming, flooding, selective forwarding and replay attacks threatens the service availability of the WSN. While impersonations, Sybil and eavesdropping attacks threatens the authentication [20].

Islam, Shen and Wangs article [21] examines the major attacks on smart home automation environment in their article: (1) eavesdropping, (2) denial of service, (3) node compromise, and (4) sinkhole and wormhole attacks. In addition to this, Can and Sahingoz [22] describes sinkhole

attacks, wormhole attacks, selective forwarding, misdirection and HELLO flood attacks. Eavesdropping is possible because the smart home environment devices often communicate through unsecure medium like wireless technologies. An attacker can get confidential information about the users in the house or manipulate data if the person gets access to it. This can be monitored from both inside and outside of the smart home network. The data can contain confidential information about the users in the smart home. This is the most common security threat found in the smart home automation system [21].

Article [23] evaluates DoS attacks in many different forms over wireless networks. To implement control frame attacks, they make a real testbed and present the amount of damage these attacks can bring to the WLAN. The paper provides an experimental analysis of 802.11-specific attacks based on their practicality, efficacy and potential low-overhead implementation changes to mitigate the underlying vulnerabilities.

3 Choice of methods

In the thesis, I have used qualitative and quantitative methodologies to answer the research questions. A large portion of the time has been used to learn the tools and the technologies in the CPS. This was a prerequisite to be able to understand and complete the task. The success of this thesis lied in the experimenting work and not in the literature. The general methodology employed to study reference topologies and scenarios for the CPS have been discussed in detail to provide the reader a general idea of the work included in this thesis.

3.1 Background study

A background study has been performed in order to capture the operational characteristics of the CPS in the CI sectors. A prerequisite was to find relevant literature within the field of CPS, mainly for the power systems and smart home automation systems that have been studied. This have been needed to create a suitable CPS model in order to gain the best possible experiment results. The background study have provided information about the CPS physical processes and other information about sensors and actuators that have been useful when modelling and simulating the systems. It is important to review the papers. Some pointers have been looked at to review the quality of the papers, if they were good or not. The review was used to see whether the paper was within the scope of the journal and to see whether the science is good enough. Different aspects taken into account was if the paper added value and if the paper was built up the right way. It was also important to look at the result of the paper and what they did to come to this result.

3.2 Modelling procedure

For creating a topological model manually, there was established a basic observation and insight to the CPS. This included knowledge about the environment of the system and the physical processes that is controlled in the system. The model of physical processes represents a real-time system. This phase includes determining which physical process that are controlled and the requirements for the delays, latencies and sampling rates. This makes the measures accurate and the system is properly controlled.

3.3 Simulation

The simulation and analysis have been the key methodology in this thesis, since it is expensive to set up a test environment in real power systems and smart homes. This was solved by using a network simulation tool. The simulation includes: sensors, actuators and physical processes. To model the individual components and subsystems are as important as the end-to-end model. OMNeT++ is an extensible, modular, component-based C++ simulation library and framework. It is used to

build network simulations, and this includes wireless and wired communication networks and also queueing network, on-chip networks and so on. In the simulation tool it is possible to create wireless ad-hoc networks, Internet protocols, sensor networks, performance modelling, etc. There are also extensions to OMNeT++ that allows real-time simulations.

3.4 Scenario development

The attacks targets the real-time performance characteristics such as packet dropping, message delays, retransmission, and jitter for periodic messages. There have been developed attack scenarios that are defined specifically for the cyber-physical system created. The attack scenarios has corresponded to a hacker's capability given the current state of the network. The actions used in the attack scenarios are:

Stage	Action
1	Reconnaissance
2	Determine vulnerabilities
3	Perform attack
4	Attack goal

Table 1: Actions in the cyber attacks.

The first stage is reconnaissance or information gathering and getting to know the target systems. The second stage is to find out where the attacking machines should be located in the network to achieve the best possible result. The third stage is to perform the attack scenario and the fourth stage is to achieve the goal of the attack.

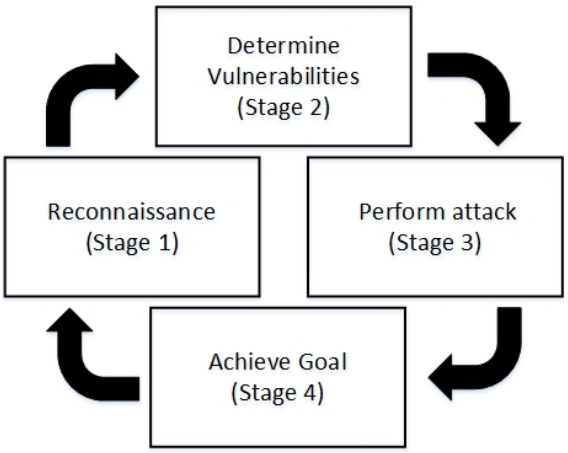


Figure 3: Progression of the actions in the cyber attack [24].

Figure 3 simulates the attack stages in table 1. In general steps, the methodology for the attack

works backwards. The goal of the attack scenario is first defined, which is to perform network attacks, particularly targeting real-time performance characteristics in the networks. Once the goal was defined, the attack vector that can achieve the goal was created. Then the question was, "where should the attacking hosts be located in the network to accomplish the goal?" The host location is based on the information gathered in the reconnaissance stage.

The different attack scenarios consist of a set of attacks that have been performed on the simulated system. The attack scenarios includes an attribute representing time. This is how long in simulation time the simulation will continue running after the attack have been completed. If the simulation stops right after the attack, the last traffic will be associated with the attack step. Adding this time to the simulation will avoid the bias of having the simulation end with the last step of the attack.

3.5 Validation/verification

After defining the CPS structure and development of attack scenarios, the system was used as a basis for setting up and simulating a series of cyber attacks. The attack scenarios created provides the means for detailed attacks to be simulated in the system. Since this thesis focuses on real-time performance characteristics, the traffic moving in the system through the network needed to be effectively modeled. There are a lot of packets moving between nodes in a network. Modelling all possible packages is a time costly process that would reduce the performance of the simulation. This would not add any additional value to the simulation. Therefore, this simulation will only include traffic that is involved in the attack progression. Every attack will have some attributed defined in the attack class:

Number	Attributes
1	Attack name
2	Attack type (manual or automatic)
3	Network used
4	Included in attack scenario
5	Goal of the attack
6	Steps in the attack
7	Start time
8	Total time of the attack

Table 2: Attributes defined in the attack class.

3.6 Data analysis

The last research question, how will a CPS in CI real-time performance characteristics be affected by different network attacks, required experimental and quantitative methodologies. In order to measure and analyse the performance characteristics of the CPS, a proper dataset have been needed. This kind of dataset contains the CPS performance characteristics before, under and after the net-

work attacks. The data in the dataset have been measured and analysed with appropriate metrics with the purpose of this experiment was to obtain results that can answer the research question.

By measuring the real-time performance characteristics for the CPS and the real-time performance characteristics under an attack, it has been possible to estimate the effects that the different attack scenarios had on the system. The experimental result are presented numerically and statistically.

4 Theory on cyber-physical system

Cyber-physical system (CPS) is a system used to monitor and control a physical world. CPS is the new generation of embedded control systems such as smart grid system, medical devices, smart cars and smart home automation system. It can also be identified at as an IT solution integrated into a physical system. Sensor and actuator networks are also functionality embedded in a CPS. CPS is mainly related to a real-time system. This will include real-time control systems integrated with communication and computing capabilities that control and monitor components in the physical world with a minimum of human interaction.

These systems contain software system, communication technology, sensors and actuators that interact with the real world, often including different technology. The CPS consists of two main layers; the cyber layer and the physical layer. The cyber layer will process and analyse the data received from the physical layer and return appropriate commands to the physical layer. The physical layer will execute the commands from the cyber layer through actuators and return information from sensors back to the cyber layer.

A three-layered structure has been discussed. This structure consist of perception layer, application layer and network layer. The perception layer or sensor layer is the same as the physical layer. This layer collects real-time data with actuators, sensors, cameras, laser scanners, etc. The data will be used by the application layer to perform commands. The second layer is the transmission layer. The purpose of this layer is to process data between the perception layer and application layer. This is handled through the network with Wi-Fi, 3G, 4G, ZigBee Bluetooth, etc. The application layer or the cyber layer's purpose is to analyse the data collected by the perception layer and transmitting commands to the physical components. These commands are based on the knowledge it receives from the collected data [25].

4.1 CPS architecture

Lee et al. [26] proposes a design for CPS which is called the 5C architecture. This is a step-by-step guideline for developing and deploying a CPS for manufacturing application. It is important to have a guide that clearly defines the structure and methodology of CPS in its implementation, since CPS is in the initial stage of development. The 5C level architecture presents a workflow manner to construct a CPS from initial data acquisition, to analytics and to the final value creation. The 5C level architecture is illustrated in figure 4.

1. **Smart connection level** is the first step in developing a CPS application. This level acquires accurate and reliable data from machines and their components. The data is obtained from controllers, enterprise manufacturing systems or directly measured by sensors. There are two important factors at this level that have to be considered. The first factor is how to manage

data acquisition procedure and the transferring of data to the central server. Second, it is important to decide how to select the proper type and specification for the sensors.

2. **Data-to-information conversion level** is the second level of the 5C architecture. Meaningful information has to be identified and collected from the data. Several tools and methodologies exist to collect the meaningful information. Development of algorithms specifically dedicated for prognostics and health management applications has had extensive focus in the recent years.
3. **Cyber level** acts as a central information hub in the 5C architecture. The hub and the machines connected to it form a network where the connected machine push information to the hub. To extract additional information from the massive information collected, specific analytics have to be used. These will provide a better status overview for specific machines in a large machine farm. Historical information and similarities between machine performance can be measured to predict the future behaviour of a machine.
4. **Cognition level** generates a thorough knowledge of the monitored CPS. Acquired knowledge has to be explicit presented to expert users, and with this knowledge they are able to make better and more correct decisions. The expert users will be able to prioritize tasks based on the available individual machine status and comparative information to optimize the maintaining process, when this acquired knowledge is available.
5. **Configuration level** is the feedback from cyber space to physical space. This level acts as a supervisory control to make machines self-configure and self-adaptive. Decisions made in the cognition level are used in this level to apply the corrective and preventive decisions to monitor the system.

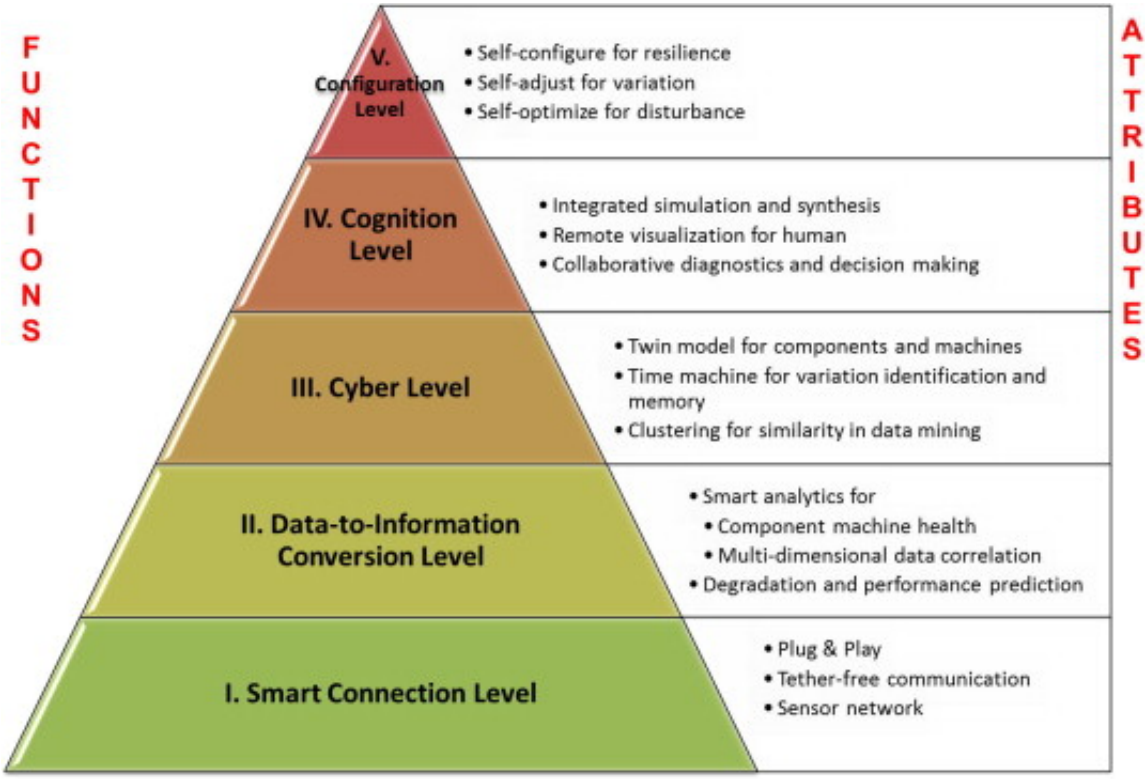


Figure 4: 5C architecture for implementation of CPS [26].

4.2 Theory on smart grid

The way people receive their electricity hasn't changed much in the last hundred years. The basic operating structure of the power grid has largely remained the same over the decades. The basic operation elements are a power plant, a transmission substation, a transmission line, a distribution substation, a distribution line/transformer, and an end user [27]. A cold, nuclear or hydro power plant sends electricity through transmission lines to substations and further on to transformers. The power goes through finer and finer wires and the voltages gets lower until the electricity reaches a home and further to an electric device plugged into the wall. The main difference between the electric grid before and a smart grid today is that a smart grid system has a variety of operational and energy measures. This is measurements like smart meters, smart appliances, renewable energy resources, and energy efficiency resources. An important aspect of the smart grid is overview of the electrical power conditioning and control of the production and distribution of electricity [28]. Manufactures has to take it to the extreme, since electricity travels close to the speed of light and every kilowatt must be used the instant it is created. For the smart grid this means balancing and trying to match supply and demand of electricity perfectly and nearly instantly. When the demand outpaces the supply, everything goes dark. Backup power plants has spinning reserves ready to be pumped into the system at a moment's notice. Since the 1980s the power grid has been getting smarter and smarter. Sensors have been installed in factories and other places that used a lot of energy, and these sensors could return real-time data about energy usage. This allowed the utilities to get a heads up on the demand side of the equation. Over the years as wireless communication become widespread and sensors become more sophisticated and cheaper, the smart grid was able to gather more and more information [27]. This enabled the smart grid to quickly locate power failures, reroute electricity or avoid overheating power lines by analysing the data from the sensors. Sensors are likely to be everywhere in some years. Smart meters are now installed in homes and will perform the same function as the utilities have long done in factories. This is a two-way communication that will give power suppliers and costumers a better view over who's using what and when [29]. The quickly evolving electric grid gets more and more "intelligent", and with the new technology, the power grid will improve its efficiency and performance. However, the quickly evolving technologies also make the smart grid more vulnerable to cyber attacks.

4.2.1 Advantages of smart grid

- More efficient transmission of electricity
- Increased integration of large-scale renewable energy systems
- Provides the consumers the choices and incentives to modify their electricity purchasing patterns and behaviours.
- Autonomous control actions that increase the smart grids reliability. This makes the system more resilient against natural disasters and component failures.
- Improved security

4.2.2 Substation

Electrical substation is an important component in a smart grid power system. This is where electricity voltage on the transmission line is increased or decreased. Transformers are the actual mechanisms in substations that increases and decreases the electricity voltage and controls the power flow in the transmission system. Other elements found in the substation are capacitors, voltage regulators and circuit breakers. Automated substation control is implemented to provide real-time monitoring and control through local area networks. Specialised sensors are attached to the equipment to take status samples. The information sampled will be transmitted with a continuous data stream or isolated packets through the local area network to the control station. When the control center receives the status samples it may create a response to be sent back to the electric equipment [30]. Timing is crucial for the communication in the substation, and this is the fundamental difference from other communication networks. Some of the information sent is only valid and useful within a short amount of time. If the sampled value exceeds the short time frame, then the information does not server its purpose any more. This will, in worst-case scenario, cause damage to the grid [30].

4.2.3 System assets

Programmable logic controller (PLC)

Programmable logic controller, or PLC, is a special purpose computer without display, keyboard and hard drive. PLC consists of a power supply unit, processor unit, input/output devices, communication interface, and a programmable memory to store implemented functions and instructions. These functions can be sequencing, logic, arithmetic, timing, and counting to control machines and processes. This controller is often used to automate functions in smart grids and can be specialized to do specific tasks. It is typically used to control real-time operations and is designed for simple efficiency [31]. A written PLC program consists basically of instructions for the PLC to turn on and off outputs based on the information from the input and the internal program. Once the PLC program is installed, it will run in a continuously loop for an indefinite time. A PLC inside a machine will therefore run automatic for years with little human interaction.

An example is a facility where they store water in a water-tank. Another system is using the water from this tank, as needed. The PLC needs to manage the water level in the tank by controlling the valve that refills the tank. The refilling of the tank from the valve will be the on and of output from the PLC, and the water measure will be the input.

Remote terminal unit (RTU)

A remote terminal unit is a multipurpose device used for monitoring and controlling various systems and devices remotely. It is typically found in a substation, along a pipeline, or some other remote location and serves a similar purpose as PLC. RTU consists of all the basic parts of a computer, like a processor, storage, memory, and it includes remote communication technology. The purpose of a RTU is to monitor field parameters and send this information to a central monitoring station. This could be a PLC or directly to a human-machine interface (HMI). The RTU is often found in

places that does not have easy access to electricity and can therefore be supplied with a local solar power generator and storage facilities. It needs to be robust because it is often found outside. This means that the RTU is exposed to extreme environmental conditions e.g. lightning, humidity and temperature [6].

Phasor measurement unit (PMU)

Phasor measurement unit is a device which measures the magnitude and phase of an electrical Phasor quality. This can be voltage or in smart grid where it is used as time source for synchronization. PMU uses GPS signals to get a high-precision time synchronization. This allows real-time measurements and observation of multiple remote measurement points on the grid with high fidelity. The data from each individual PMU is routed to a phasor data concentrator (PDC). The PDC checks the validity of the message and aggregate and time-align the data before it is forwarded using WAN to a super phasor data concentrator (SPDC). SPDC has a direct connection to the controller [32, 33].

Human machine interface (HMI)

Human machine interface is used in industry to control and monitor PLCs and RTUs. A common HMI is the screen at an ATM machine, and the screen has push-buttons or touchscreen that allows us to operate the machine to withdraw a certain amount of money. HMI uses a graphical representation of digital control used to sense and influence processes. The graphical representation replaces manually activated switches and other electrical controls. Operator or maintenance personnel can operate and monitor the machines by starting and stopping cycles, adjust set points, and set functions required to adjust the control process, from the HMI. The HMI can give display information about temperature, process steps, material counts, and pressure. It can also give very precise levels of information and exact positioning of machines. HMI will allow the information to be displayed in one place instead of using multiple indicators, and the possibilities are only limited by the software and hardware used. A HMI will replace a lot of physical wires and controls with software parameters. The HMI can be used for troubleshooting purposes if it is connected to a PLC. This can reduce time-critical work compared to connecting a computer to the PLC each time a situation occurs. A HMI can be used to control and monitor multiple machines or other equipment's in an industrial site, which is a benefit. The HMIs computer console do not use general authentication with password. The reason for this is a password lockout, or any other lockouts related to other mechanism, would be unsafe and violate basic principles for availability in case of an abnormal event. The authentication and password are usually not an issue because the HMI is often installed in areas with strong physical security and only operated by trained and trusted personnel [6].

Supervisory control and data acquisition (SCADA)

A supervisory control and data acquisition is a type of software application for process control. The system consists of controller's network interfaces, software, input and output, and communication equipment's. The SCADA system is used to control and monitor equipment in the industrial process, like power generation transmission and distribution in smart grid. SCADA is a software package installed on a server which will gather information and send out commands based on the information

received. Most of the control actions are done automatically by the PLCs and RTUs [34]. The SCADA system performs the following functions: data acquisition, data communication, information and data presentation, and monitoring and control. Real-time systems often consist of numerous components and sensors. The data acquisitions function is to know the status of certain components and sensors. The data communications function is the communication between the devices in the system. This can be wired network and communication over internet using specific protocols. A real-time system has a lot of sensors and alarms which will be impossible to handle simultaneously. The information and data presentation function will use a human machine interface to show information gathered from various sensors. The SCADA system is implemented with monitoring and control function to work automatically without human involvement. This will be operations like start/stop pumps along a pipeline, open/close valves when filling a reservoir, and changing the set point of a process temperature.

Data historian

Data historian is a software application that stores information about real-time processes from automation processes in industrial devices and system. This could be information like alarm events, batch records, point value, and other information. The stored data is structured in a database for concurrent and later analysis. The data historian runs on a server and uses a standard operation system like Windows or Linux. The software application is designed for fast collection of data [34]. Benefits of using a data historian allows us to have access to historical data for better understand how the plant has been running. It can also provide information that enables us to handle the system better, rewind to a point in the past where something happened and investigate the specific issue.

Energy management system (EMS)

EMS is used for analysing and operating the transmission power system reliable and efficiently. This computer will monitor, control, and optimize the performance of the transmission system in real-time. The EMS computer can also be referred as SCADA/EMS. In this case the EMS technology excludes the monitoring and control functions. The EMS will be more used for scheduling applications and collection of power network applications and generation control [35].

Distribution management system (DMS)

DMS is used to analyse and operate the distribution system efficiently and reliably. It will act like a support system to the control room and field operating personnel in the electric distribution system. The DMSs main function is to improve reliability and quality of the services. This involves reducing outages, minimizing outage time, and maintaining an acceptable frequency and voltage. The DMS works as a complement to SCADA and EMS system and has functionalities like distribution state estimation, unbalanced power flow control, fault identification and location, integrated volt control, and service restoration [36].

4.3 Theory on smart home

A home is considered smart when it is possible to remote control of functions and/or devices from smartphone, tablet, computer or even better, when things manages themselves without interaction with a human. Examples of this can be (1) lights being turned on and off automatically when you come home or (2) smart plug is turned on at a certain time so you can have fresh coffee in the morning. A smart home will make everyday life a bit easier. For example, when you are in a hurry and have to leave home quickly and then start worrying if you forgot to turn off the lights and the TV. This can be remotely turned off regardless of where you are with a smartphone connected to the Internet. A smart home can also be used to reduce the energy cost and energy consumption through more efficient operation. For the user this can typically be offering a medium to control the home systems climate, lighting and other appliances [37].

4.3.1 Advantages of smart home

- Remotely control - A user can control all the house functions from one location. Heat control, lights and stereo systems can be controlled at the same time.
- Safer homes - Alarms connected to the smart home and light sensors outside, turning on if people move too close to the house. It is also possible to install pre-programmed routines to turn off and on lights and pull the curtains up and down to simulate that someone is at home.
- Reduce energy costs - By using motion sensors it is possible to turn on lights that stays on as long as there is registered movement in the room/area. Sensors provide regulation of heat and air conditioning and the possibility to lower the temperature at night or in the middle of the day when no one is home, which will result in lower consumption and reduced expenses.
- Beneficial for the elderly - Providing monitoring that can help seniors to remain in their homes comfortably and safely, rather than having 24/7 home care or moving to a nursing home.

4.3.2 Smart home architecture

A home needs three things to make it smart. The first one is an internal network. This is wire, cable or/and wireless communication options that allows devices to communicate and exchange information with each other. The second one is an intelligent control, which will be the gateway that manages the featured systems. The third one is home automation which indicates products within the home network and links to services and systems outside the home [38]. There are a lot of different options when it comes down to the implementation of these smart home features. Different taxonomies have been proposed by DTU [39] to divide smart homes into three main categories. This is based on the methods used to control by interact and manage the appliances, and also the overall complexity level of the infrastructure. The main three categories are controllable houses, programmable houses and intelligent houses. Controllable houses is the first category and this is often the first stage when an ordinary house is transformed into a smart home. It is a house where the user is able to control different devices in a more efficient way. Three sub-classes of such controllable houses have been identified:

- **Houses with one integrated remote control**. The number of subsystems and appliances can

be controlled remotely from one control device. Simple wired or remote communication has to be established between the devices and the control unit.

- **Houses with interconnected devices**. Different electronic devices are connected with each other to allow the exchange of information between these devices. This will allow a more accessible and easy communication between the devices in the different parts of the house. This kind of infrastructure requires a broadband network, but both wired and wireless communication are commonly used. Also, functionalities from the house with one integrated remote control are required as there is a need for an easy control over all interconnected devices.
- **Houses controlled by voice, gesture or movement**. Such an infrastructure could be similar to the other sub-classes in the controllable houses category. The difference in this sub-class is that a visible control unit is replaced with an invisible one. These controlling units react on voice commands, movements or gestures.

The second category is the programmable houses. These houses contain programmed devices that are adjusted or switched on or off when a certain condition occurs. The identified sub-classes for this category is:

- **Programmable houses reacting to time and simple sensor input**. Devices are programmed to be turned on or off at a certain time. Another feature is sensor inputs, for example a simple thermostat, which switches on and off when the temperature passes a certain value. Lights that are turned on when it gets dark outside belong to this sub-class.
- **Programmable houses assessing and recognising situations**. Information from several sensors is used to recognize events. Scenarios have to be defined and programmed in advance for the house to act in given situations. For example, if you go to bed, a sensor or camera will register this and turn off the light, music and check if the door is locked. This technology is dependent on reliable software that will analyse the situation correctly.

The third category is the intelligent houses. Such infrastructure is similar to the previous sub-classes. The difference is that within these houses there would be no need to program any functionalities as the house would learn by itself. The devices in the house will work together and observe and learn from the users repeated actions in the everyday life. When a repeated action is identified the house will program itself to automatically switch on or off certain equipment when the scenario reoccurs.

4.3.3 System Assets

Cloud

The cloud involves storage and maintenance of data over the Internet. This will give the user access to the data inside and outside the home network. A smart home automation system connected with the cloud will allow users to send commands to the gateway from a remote location. The gateway will then send the control command to the specified sensor for triggering the specific action the user requested. Once the action is performed, the gateway will send a status update back to the cloud network [40].

Gateway

Most of the smart home devices works as standalone. The devices needs to be connected to a "base station", and this is called a gateway. This gateway works as a hub for the smart devices in the network. It provides connectivity from distributed nodes back to the Ethernet backbone. All the devices communicate with the gateway through their own network. The gateway is the only device in this group that is actually connected to the home Internet router, any other smart home device can be connected to the router as well [40].

Sensors

Sensors presents the function that allows smart devices to interact with their surroundings. A sensor is observing and detecting events or changes in its environment. The sensor converts the detected events from analogue signals to electric values, these are transferred to other electronic components. It is very important that the generated readings are as accurate as possible [40].

Actuators

An actuators is another component which allows smart devices to interact with their surroundings. Unlike the sensors, actuators are the physical implementation of the action function. This means that the device can control and carry out changes in the real world. Loudspeakers and power switches are examples of actuators that receives a control signal which is converted into an action. The received commands will come directly from the end-user's device or indirectly through sensor data processed either by the cloud or locally [40].

IoT devices

Glass-break sensor

The glass-break sensor is a sensor using sound to recognize glass breaking. When a glass breaks it produces a special sound, which have a certain frequency sound wave. Different glass types produce different sound wave frequency. The glass-break sensor is able to detect these sound waves and it is often installed close to a window or a door.

Smoke detector

Smoke detector uses a sensor to distinguish if there is any presence of smoke or fire. The most normal sensors to use in a smoke detector is a carbon monoxide and carbon dioxide sensors [41]. The sensor will identify and measure the gas concentration in the room. An electronic signal will be sent to the controller if there is identified a certain concentration of dangerous gas.

End-user devices

Smartphones, tablets and computers main functions are computing and providing the end-user a status overview, of which device can be monitored and control in the smart home system.

5 Reference topologies and scenarios for cyber-physical systems in the Norwegian cyber range

5.1 Analysis of reference scenarios and control systems architectures found in the reference sectors

The purpose of this section is to get a better understanding of what "normal operational conditions" of the two systems are, as well as identify the fundamental architectural characteristics.

5.1.1 Smart grid

Topologies

Figure 5 is a communication overview that provides a high-level, overarching perspective of a few major relationship in the smart grid domain. The figure is a tool created by Bryson and Gallagher [2] to identify actors and possible communications paths in the smart grid. The figure had originally seven domains, but the markets and service providers domain are removed to focus on the cyber-physical communication and control interactions. The top of the figure shows the necessary communication for the operational control system of the smart grid, to the domains below. The domains on the bottom of the figures are the typical power system domains, which is generation, transmission, distribution and also the customer domain. The costumer domain includes localised grid-connected distributed generation and advanced metering infrastructure (AMI). The operations domain on the top in the figure 5 is responsible for the operations of the power system. The majority of these functions is today the responsibility of a regulated utility, and it will be more and more usual to outsource some of these functions to service providers. But, no matter how the markets or service provider domains evolves, the basic functions of the operations domain for planning and operating the service delivery. The transmission operations are responsible for the transmission domain. It will use energy management systems (EMS) to analyse monitoring, and control the transmission power system reliably and efficiently. Distribution management system (DMS) is used in a similar way in distribution operations. The DMS will analyse and operate the distribution system.

Communication protocols

IEC 61850

IEC 61850 is a standard for object-oriented substation automation. The standard is used in electrical substations to define how to describe the devices and how to exchange information regarding the devices. IEC 61850 used in smart grid is evaluated to the high requirements of intelligent electronic devices inside the smart grid. The protocol is based on two levels of modelling. The first one is the breakdown of a real or physical device into a logical device. And the second one is to breakdown the logical devices into logical nodes, data objects and data attributes. The meaning of this is to decompose the application functions into the smallest entities. These entities will be used

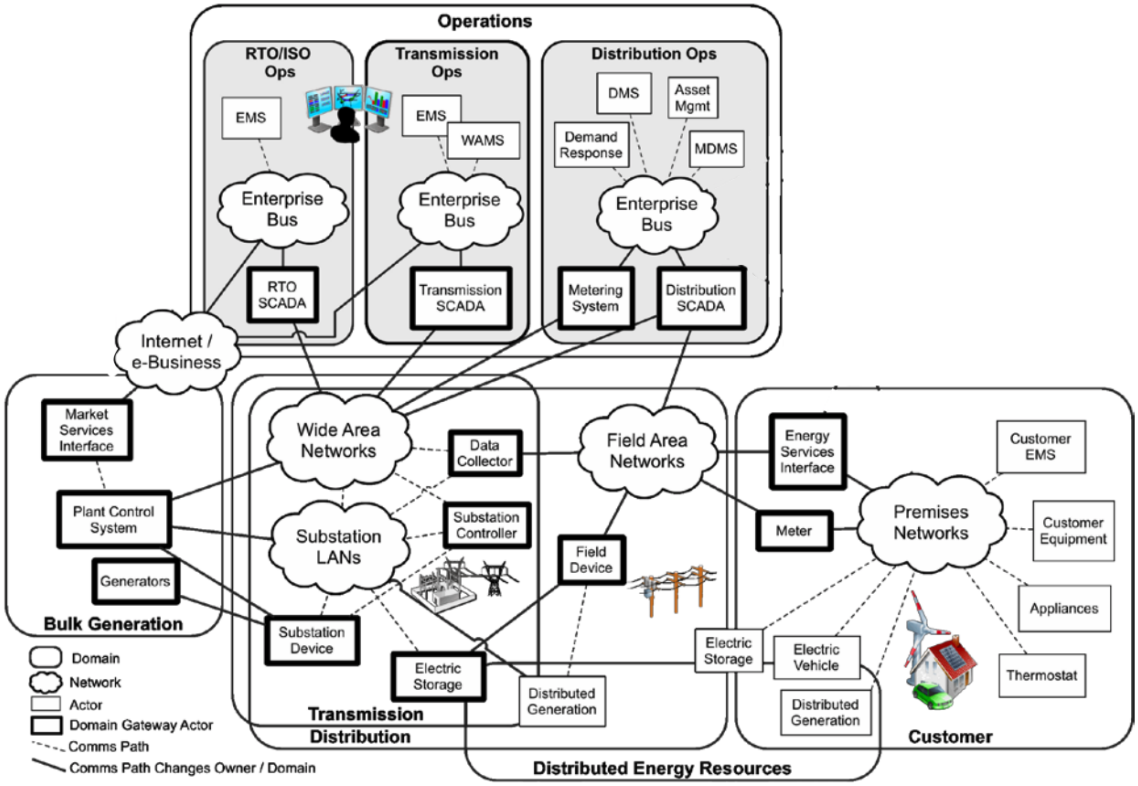


Figure 5: Smart Grid communication overview [2].

to exchange information. For example, each node contains one or more elements of data, and each element of data has a unique name. These names are determined by IEC 61850 which are functionally related to the power system purpose, like XCBR logical node which is a circuit breaker model. This node contains data for determining if a operation is remote or local (Loc), operation count (OpCnt), position (Pos), block breaker open commands (BlkOpn), block breaker close commands (BlkCls) and circuit breaker operating capability (CBOpCap) [42]. IEC 61850 is also a standard for communication services. This will allow compatible exchange of information for the components in the power system. IEC 61850 uses SV and GOOSE messages. SV is an abbreviation for sample values which uses publisher subscriber mechanism. The current and voltage will be measured by merging unit and transported as analogue signal into a digital one tagged with synchronised time. This voltage and current measurement could be used by the control center which need the information [43]. GOOSE is an abbreviation for generic object-oriented substation event. The GOOSE messages are used to send urgent messages which are directly linked to the link layer to deliver very quick information. The message is multicast and it is received by intelligent electronic devices (IED), which has to be subscribed to it [44]. The GOOSE message frame is shown is figure 6 and

the acronyms stand for:

- DEST/SRC - Destination/Source MAC Address
- TPID - Tag Protocol Identifier
- TCI - Tag Control Information
- APPID - Application identifier
- APDU - Application Protocol Data Unit

DEST	SRC	TPID	TCI	Ethertype	APPID	Length	Reserved 1	Reserved 2	APDU
6 Bytes	6 Bytes	2 Bytes	2 Bytes	2 Bytes	2 Bytes	2 Bytes	2 Bytes	2 Bytes	n Bytes

Figure 6: GOOSE message frame [44].

IEEE C37.118

IEEE C37.118 is a protocol on the transport layer used for reporting the synchrophasor measurement. A synchrophasor is a time-synchronized measurement to measure the quantity described by a phasor, which is the magnitude and phase angle of voltage and sinusoidal waveforms at a specific point in time [45]. Synchrophasor is used in smart grid to measure the frequency in the power grid. IEEE C37.118 is a protocol in the transport layer. The standard consists of two parts. The first part defines format, form and quality requirements for the synchrophasor, and the second phase defines the communication protocol. IEEE C37.118 describes four message types for real-time transfer of data and configuration from a phasor measurement unit or phasor data concentrator. These are data, configuration, header, and command message. Data, configuration and header are sent form the data source, and the command is sent from the receiver to control the data flow or request information [46].

Modbus

Modbus is a communication protocol in the application layer that enables process controllers to communicate with real-time computers. Modbus provides a master/slave communication between devices and uses an interconnected assets based on a "request/reply" methodology. It operates widely independent of the underlying network protocol. Modbus is one of the most popular protocols used in ICS architecture. The reason for its popularity is that the protocol is easily adaptable for serial and routable protocols, and it does not rely on authentication. This makes it suitable for small devices, such as sensors or monitors with little processing power to communicate with complex computers [6]. Modbus is an open standard, which is freely distributed and widely supported by members of the Modbus Organization. The request response model of Modbus supports three Protocol Data Units:

- Modbus Request

- Modbus Response
- Modbus Exception Response

It also uses Function Codes and Data Request for various commands like read I/O devices. The transaction for the Modbus protocol is shown in figure 7.

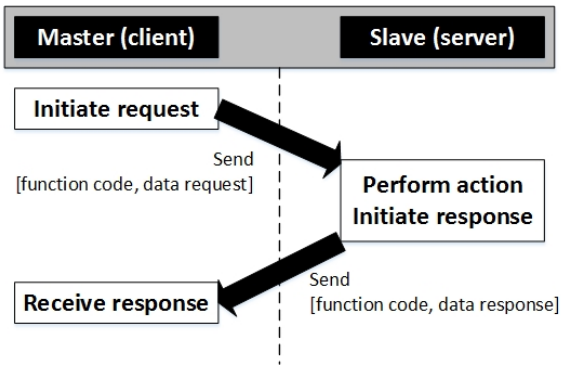


Figure 7: Modbus protocol transaction (error-free) [6].

DNP3

DNP or Distributed Network Protocol was in the beginning much like Modbus, a protocol between master/slave devices. DNP3 was introduced and the protocol provided reliable communication in environments within the electric utility industry. These systems had a high level of electromagnetic interferences, at the time poor transmission media like analog telephone lines. After numerous revisions the protocol became widely used in other industries because of its features to apply to other industries including report by exception, time-stamped data and data quality indicators. DNP3 is very reliable, while it is remaining efficient and is really suited for real-time data transfer. The protocol defines a set of data classes at the slave node. At the beginning of the communication phase, the master will collect all buffered data points from the slaves to get up to data, which is shown in the initial phase of figure 8. After this the master can query one or more classes separately to make the process more effective. This is the subsequent request phase in figure 8. Another difference between Modbus and DNP3 is that DNP3 supports a two-way communication. This means that the slave node can contact the master in case of high priority events and is the unsolicited response phase in figure 8. While in Modbus the slave has to wait for the master's request to notify the event. This two-way communication requires both source address and a destination address [6]. DNP3 packets are transmitted in TCP/IP packets but are not limited to this transmission protocol.

IEC 60870-5

DNP3 was based on early drafts of the IEC 60870-5 standard. This standard is widely used for transmission in SCADA control and information. The standard is mostly used in Europe and China.

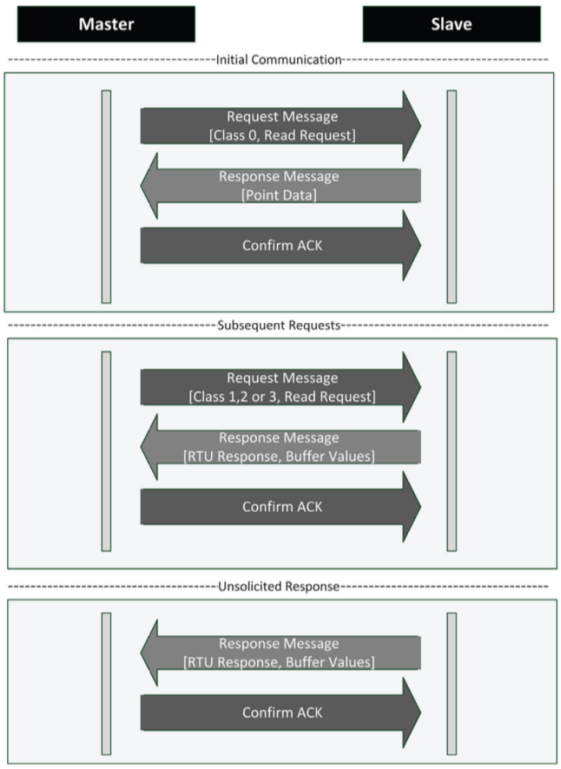


Figure 8: DNP3 communication protocols [44].

IEC 60870-5-101 is a transmission protocol used in basic telecontrol tasks for telecontrol outstation and telecontrol station. IEC 60870-5-104 is widely used in smart grid for communication from remote field locations. It is a combination of the transport functions provided by TCP/IP and the application layer of IEC 60870-5-101 [44].

Physical view

Figure 9 shows the components that constitute the system along with their interconnections. This figure is based on the Bryson and Gallagher [2] and McLaughlin et al. communication overview [44]. The top of the figure represents the cyber system and communication interconnections. This is necessary to operate the control of the power system components found in the bottom of the figure. These control systems are interconnected by bidirectional cyber system infrastructure comprising software, hardware and communication network. The bottom of the figure represents the classic power system components with power generation, transmission and distribution. The customers side is to be found in the bottom of the figure. This domain consists of a number of smart meters.

The acronyms found in figure 9 is:

- AMI - Advanced Metering Infrastructure

- DMS - Distribution Management System
- EMS - Energy Management System
- HMI - Human Machine Interface
- MDMS - Meter Data Management System
- PMU - Phasor Measurement unit
- RTO - Regional Transmission Operator
- SCADA - Supervisory Control and Data Acquisition

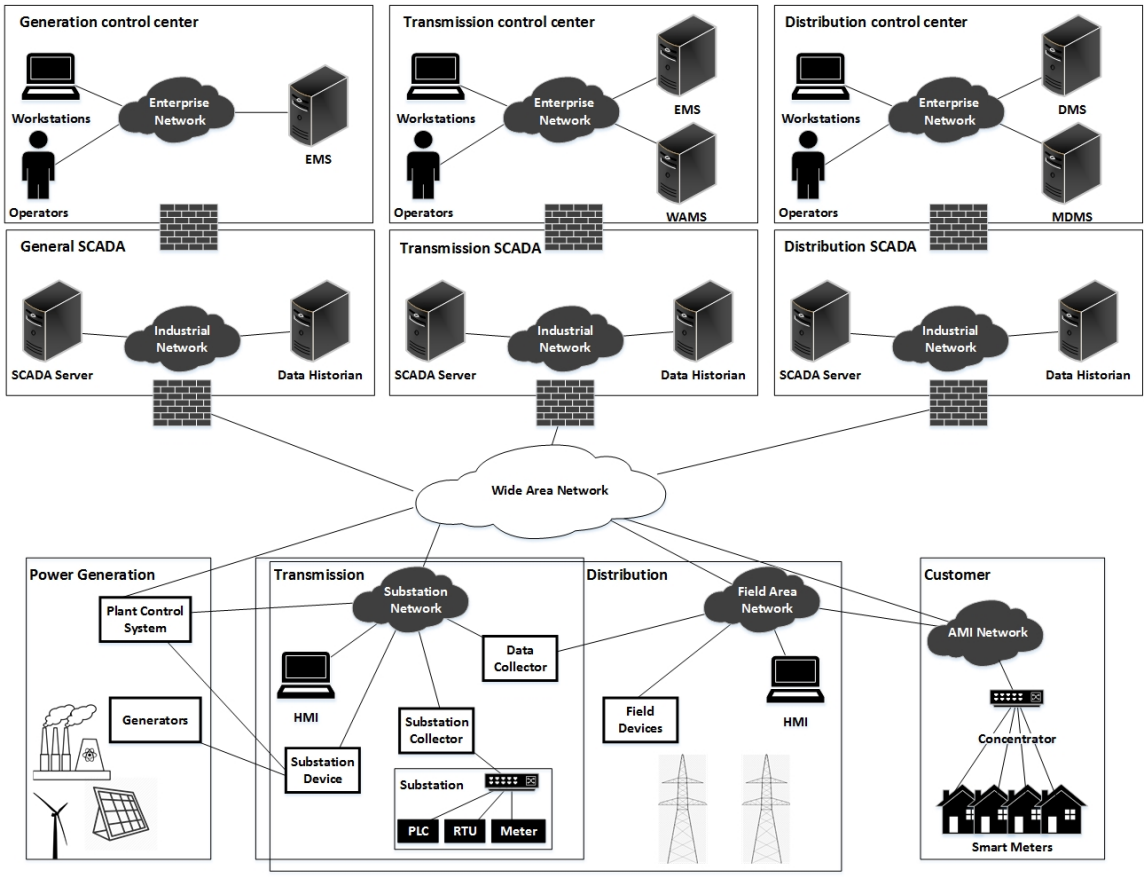


Figure 9: Smart grid physical view [2, 44].

Connectivity

The smart grid is a complex system and it is therefore important to understand the systems connectivity and interaction to be able to create and attack the system. A connectivity is any form of data exchange, either logical or physical between devices. If there is a physical medium between the communication of two nodes, then the connectivity is physical. Logical connectivity is

the interdependence of applications including SCADA (Supervisory Control and Data Acquisition) management, ADR (Automated Demand Response) and distributed management.

5.1.2 Smart home

Topologies

A star type topology is the most common used topology in smart home automation system. This will make the central control unit (CCU) interact with all the other available remote control units (RCU) in the system. The CCU will make the decisions making responsibilities. The RCU responsibilities are to send data collected from sensors to the CCU. The CCU will then use these data from the RCUs to make the decisions and return commands to the RCU [47]. An example of a star topology is shown on the left side in figure 10. The advantages of using star topology are that it is very flexible and easy to set up. In addition any node except CCU, can have a malfunction without affecting the connection for the other nodes in the network. The downside of this topology is the single point of failure. If the CCU has a malfunction, it will affect the whole network.

Mesh topology is show on the right side in figure 10, and this is another topology used in smart home automation system. Every device in this topology makes its own decisions based in the information shared by the other devices, so there is no CCU. The communication between the devices is sent through other devices and the data will be shared with all the other units in the network. The data will hop form device to device to reach its destination.

It is possible to have multiple types of typologies in one single network.

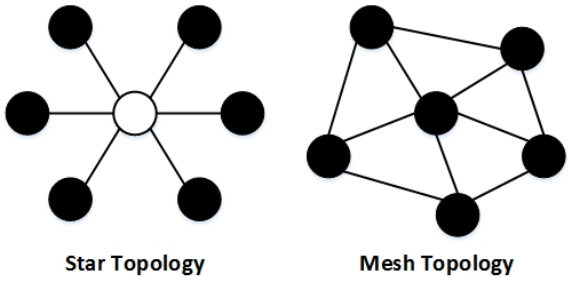


Figure 10: Example of a star and mash topology.

Protocols

There is a wide variety of communication protocols that have been either adopted by the smart home automation system or have been specifically made with smart home communication in mind. This section will present some of the protocols in the different layers that can be found in a smart home network. These protocols provide end-to-end data communication for the nodes in the network and specify how the data is encoded, formatted, and transported [40].

Ethernet

Ethernet is part of the link layer which provides the building blocks for communication across a variety of physical media. It groups signals or bits from the physical layer into frames or packets [48]. Ethernet is a communication standard that was first published in 1980 to network computers and other devices in a local environment such as a building or a home. The local area network (LAN) connects multiple devices together so that the devices can create, store, and share information with each other. In the beginning the Ethernet wired system used coaxial cable. Today, it is more usual twisted pair copper wiring and fiber optic wiring. The standard Ethernet or IEEE 802.3 has defined the physical layer and MAC portion of the data link layer. The physical layer consists of the components devices and cabling. Switches and routers act like directors of the network and is able to connect multiple nodes or networks together. This enables the opportunity for communication between all the different devices. Ethernet transmits data packets in the data link layer by using an algorithm called carrier sense, multiple access with collision detection or simply CSMA/CA. CSMA/CA stations listen on the medium to see if it is free, if so, then the node has the opportunity to transmit data over the medium. If the transmission media is busy, the CSMA/CA will wait for a random amount of time before it checks the media again [49].

Wi-Fi

Wi-Fi is part of the link layer and is a communication technology that allows devices to exchange data using radio waves. The radio signal is half-duplex. In other words, the wireless device can either receive or transmit data, it cannot receive and transmit simultaneously. Wi-Fi networks are easy to set up, and almost all portable devices like smartphones and computers have included the necessary hardware to access. Wi-Fi is based on the IEEE 802.11 standard. As any other 802.x protocol the 802.11 protocol is a series of specifications for media access control and physical layer as shown in figure 11. IEEE 802.11 operates in the 2.4GHz unmanaged ISM band. ISM stands for industrial, scientific and medical radio bands. Later versions can also operate in the 5GHz band. The original IEEE 802.11 standard came out in 1997 and allowed up to 2Mbit/s [50]. Current standardised 802.11as allows up to 6.75Gbit/s.

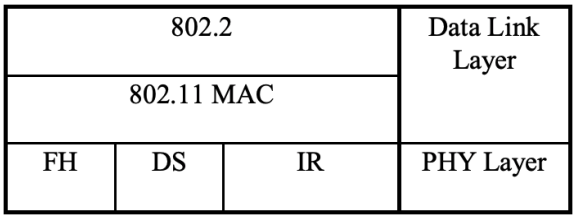


Figure 11: IEEE 802.11 layers description [51]

In the wireless network it is much more challenging to detect collisions then in a cabled network. Wi-Fi uses the layer two medium access control method CSMA/CA. The approved security mecha-

nism for Wi-Fi is Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2). WPA replaced the way keys where used with encryption blocks. To ensure that every frame is encrypted with a different encryption key, WPA uses a scheme called the Temporal Key Integrity Protocol (TKIP). The TKIP protocol mixes initialization vector with the root key. It also includes a message integrity check. WPA2 replaced WPA. WPA used RC4 encryption while WPA2 uses Advanced Encryption Standard (AES) algorithm. This encryption is aimed to provide privacy between station and AP. CCMP or Counter Mode Cipher Block Chaining Message Authentication Code Protocol is what replaced TKIP when WPA2 implementation was released. This was a more advanced encryption standard. It had a larger key size (128-bit) and a larger block size (128-bit) [49].

Internet protocol

Internet protocol or IP offers a connectionless and unreliable protocol. IP specifies the technical format of packets and the addressing scheme for communication between computers over the network. In most networks IP is combined with a higher-level protocol like TCP, which establishes a virtual connection between source host and destination host. It does not have any mechanisms to guarantee a successfully transmission of data. Higher layers have to deal with the packet losses, duplication, or packets out of sequence. Both IPv4 and IPv6 use this basic best-effort delivery model. Multiple data link layers support IP, and IP is the only network layer protocol in the Internet architecture. The IP specifies protocols and methods used to transport data packets form the sender host to the destination host specified by IP addresses. The packets have an IP header which contains all information for sending individual packets to the destination host. This includes source host and destination host address. IPv4 relies on a 32-bit address and IPv6 uses 128-bit addresses. The maximum IP packet size is 65535 bytes including header [49].

UDP

User datagram protocol (UDP) is part of the transport layer which provides host-to-host communication over the network. UDP is conectionless, this means that UDP doesn't create a connection first before sending out data. UDP has a primitive form of error detection which is a 16-bit checksum in the packets. This checksum is found in the UDP header, as shown in figure 12. When UDP detects corruption, it will not try to recover from it. In most cases the corrupted segment will just be discarded. If a packet is dropped than its gone. UDP will not attempt to compensate for the lost packet. UDP do not guarantee in order packet delivery. Packets won't necessarily arrive in the application in the order they were sent. There is also no congestion control in UDP. This means that if the network is really busy, UDP will just keep on trying to send those packets. UDP may be lightweight but it's not that reliable [49].

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Length				Header and Data Checksum			

Figure 12: UDP datagram header format [52]

TCP

Transmission control protocol (TCP) is part of the transport layer and as certain features that makes it more reliable than UDP. TCP is connection based, which means that it establishes a connection before sending the data. This procedure is known as the three-way handshake. Figure13 shows an example of the three-way handshake.

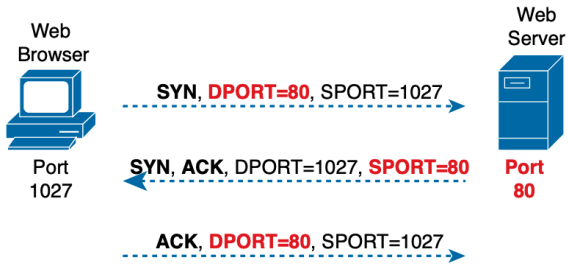


Figure 13: TCP connection establishment [53].

A similar procedure takes place when the connection is closed. TCP has delivery acknowledgment when data is sent from the source host to the destination host. When the packet reaches its destination, the receiving host will acknowledge that it got the data packet. Another feature in TCP is retransmission. If the sender doesn't get a delivery acknowledgment within a certain amount of time, it will assume that the packet got lost and resend it. Segments are numbered in TCP to be able to order delivery although packets arrive out of order. TCP will rearrange them before sending them to the application [53]. TCP has a congestion control unlike UDP. This feature will delay transmission of data packets if the network is congested. This will ease the strain on the network and help minimize packet loss. The disadvantage of this is that data will not always be sent out immediately [54]. Figure 14 shows all the information included in the TCP header. The TCP protocol require more information and overhead then the UDP header to guarantee data delivery.

ZigBee

ZigBee is based on IEEE 802.15.4 and is a low-data-rate short-range wireless network standard which defines a set of communication protocols. ZigBee's characteristics are low data rate, low cost, and long battery life. The standard allows 250 kilo bits per second and operates in 868MHz, 915MHz, and 2.4GHz frequency bands. ZigBee devices are capable of being operational for several years before the batteries have to be charged or replaced. The reason for this is that the devices

Bit #	0	7	8	15	16	23	24	31
0	Source Port				Destination Port			
32	Sequence Number							
64	Acknowledgment Number							
96	Data Offset	Res	Flags		Window Size			
128	Header and Data Checksum				Urgent Pointer			
160...	Options							

Figure 14: TCP segment header format [52]

spends most of their time in power-saving modes also known as sleep mode [55]. This makes ZigBee devices ideal for smart home automation and is one of the most popular and supported protocol for smart home device communication. A typical range for a ZigBee device is between 10 and 100 meters. ZigBee is simplifying the communication protocols and reducing the data rate. It also has a minimum requirement specification that are relatively relaxed compared to other standards which reduces the implementation cost. The ZigBee standard defines protocols from the physical layer to the application layer. IEEE 802.15.4 is used in physical layer and link layer, While Zigbee defines network, transport, and link layer [56]. In ZigBee the devices can take three different roles: coordinator, router and end device. The coordinators responsibilities are selecting the channel, PAN ID, security policy, and stack profile for a network. Each ZigBee networks has a coordinator in the Network, since the coordinator is the only device type that can start the network. The router is a device that is capable of relaying messages. Both coordinator and routers will remain active during the communication between nodes. A device that is neither a coordinator nor a router is called an end device. This device is normally the least expensive device in the network because the device has the least memory size and fewest processing features and capabilities. The three ZigBee roles for devices are shown in figure 15.

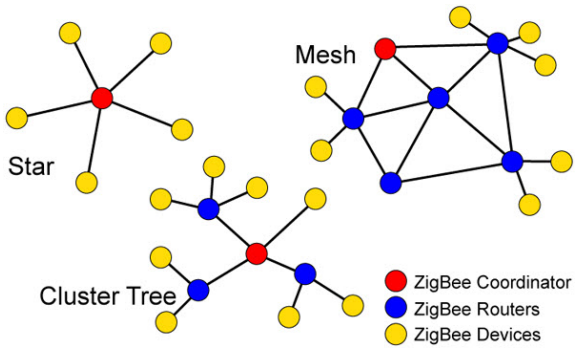


Figure 15: ZigBee network topologies [57].

Bluetooth

Bluetooth is also a low cost, low-power wireless radio frequency standard, also known as IEEE 802.15.1. The standard has a typical data range between 2 and 10 meters and allows 1 to 3 mega bits per second [55]. Bluetooth operates in the 2.4 to 2.485GHz ISM band. Seven devices can be connected to one device and this will form a network called piconet. Every Bluetooth device has a transmitting and receiving antenna. The files transferred between the devices are transferred by the spread frequency hopping technique. This means that parts of the file are sent by small bursts of radio waves which the frequency can change up to 1600 times per second to avoid interference in a crowded environment. Bluetooth uses a master/slave model to control when and where devices can send data. Master devices can be connected to seven slave devices. The slave devices can only be connected to a single master device. The role of the master device is to coordinate the communication throughout the piconet. It can send a request to any of the slaves to request data from them. Slave devices cannot communicate with other slave devices and are only allowed to receive from or transmit data to their master [58].

Interfaces

In a smart home automation system the interface is a very crucial requirement. The interface is the way for the user to communicate with the devices. There are many options of interfaces to execute communication between user and the components. The design and options of the interface depends on the system size, range, etc. The user will have access to the interface through web, wall-mounted control units, physical access, or application.

Physical view

Figure 16 shows the components that constitute the system along with their interconnections. The system consists of a control system, which is a control home device that can be accessed through a phone and over the Internet.

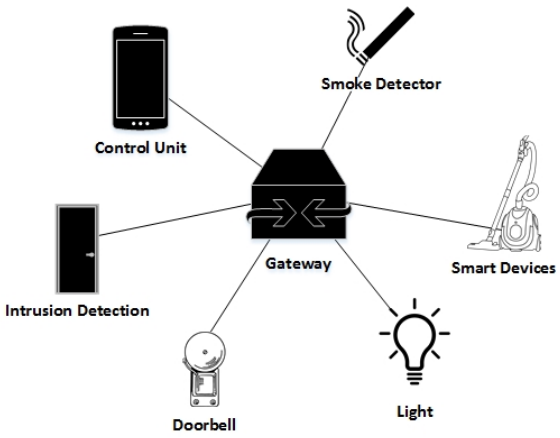


Figure 16: Smart home physical view.

Connectivity

A smart home consists of many devices with an extremely close interaction. These devices have a lot of different technologies for delivering smart personalized services and applications. The information gathered from the user and the environment must be processed in real-time or close to real-time for satisfying the personalized well-being services. Connectivity in a smart home is related to the availability of a reliable data channel between devices and the human and also the interface to the network and cloud for the personalized information. Remote and local is two types of connectivity you will find in a smart home [47]: Remote connectivity is when the user controls the system and appliances remotely. The system can also push useful notification and information to the user. This could be information about updates faults, intrusions, etc. Local connectivity is all the communication between the devices like central control unit and room control units. There are multiple options available for establishing communication between the devices. The choice will depend on topology, cost and other elements.

5.2 Creation of topological models manually, for the energy system and smart home automation system

5.2.1 Quality of service

Quality of service (QoS) is a method for traffic shaping and prioritizing traffic as it goes over the network. QoS sets a priority on packets and give the opportunity to reserve a certain amount of bandwidth for each of the applications that is running. For example in smart grid the real-time communication between HMI and PLC can be prioritized over less critical traffic in the network. The QoS is able to give the different packets priority and processed first higher priority traffic. This will typically give high-prioritized traffic a lower latency and less latency variation. This will not make a network perform over its baseline capabilities. It will ensure that high prioritized or critical traffic is successfully transmitted [6].

5.2.2 Latency and jitter

Latency is the elapsed time it takes for a packet to get from the source to the destination host in the network. A network will consist of many routers, switches and firewalls, hierarchy build up "horizontally" and "vertically". For a packet to get from its source to its destination, will have to "hop" between appliances. Every hop in the network will add latency. The further the packet needs to travel in the network, the more latency will be added. There is difference in latency in a layer 2 switch and a layer 3 router. The switch will add less latency then the router, and a firewall which is on the application layer will add more latency then a router. This is not always the case, it depends on the appliance's futures like performance. But it is a good rule of thumb [6]. The variance in the latency over time is called jitter. If you measure jitter it is positive with low values. A zero-jitter network will have a consistent packet transfer over time.

5.2.3 Packet loss

A packet loss occurs when one or more data packet traveling through a network medium and fail to reach its destination. This can either be caused by errors in network congestion or data transmission.Packet loss rate is the percentage of packets lost with respect to packets sent. The reliability for various applications in smart grid often needs to have a reliability range from 99.99% to 99.9999% [59]. While in smart home all the data isn't that important like in a SCADA system. It isn't that alarming if the video quality goes a little down because of package loss.

5.2.4 Smart grid

Smart grid model

Figure 17 shows the model created for the smart grid. The hierarchy layers of the model are SCADA master, communication media, and local control. The SCADA master consists of a SCADA console and a SCADA server. A SCADA console is the HMI where operators receives information and system functions are initiated. It is with the HMI the real-time network management is done. The SCADA server contains the database for historical trends of relevant data.

The communication media layer is the communication channel between SCADA master and local control. This communication can be done through multiple forms: fiber optic transmission, satellite, microwave radio leased line, etc. The local control consists of devices like remote terminal units (RTU) that convert electrical signals from the equipment to digital values. The substation in the local control layer is divided in to two extra layers. It is the primary substation and the secondary substation. The reason for this is that substations are located in different locations in an area. Some substations are located close to the control center, while others are more distant from the control center. This will add extra transport time for the substation with long travel distance.

Latency and quality of service

PMU and SCADA

Having PMU in the network presents a stringent delay requirement. PMUs require the communication to be flexible, scalable, and resilient to be able to handle huge amounts of data movement providing real-time data delivery. The path length has an impotent impact on the PMUs latency since multiple hops will accumulate delays. A PMU can be taken at rates of about 30 to 120 samples per second [60]. So, PMU needs to send at least 30 samples every second to measure the quality of power delivery [61]. Yaghmaee et al. [62] proposes latency, bandwidth and packet size values for PMU and SCADA, shown in table 3.

Traffic Type	Latency (ms)	Bandwidth (kb/s)	Packet Size (byte)
PMU	16	2048	53
SCADA	200	512	64

Table 3: Smart grid PMU and SCADA proposal [62].

Table 3 classifies the QoS for PMU and SCADA to require high bandwidth, low delay and low packet loss. The bandwidth requirement depends on the number and the location of the PMUs

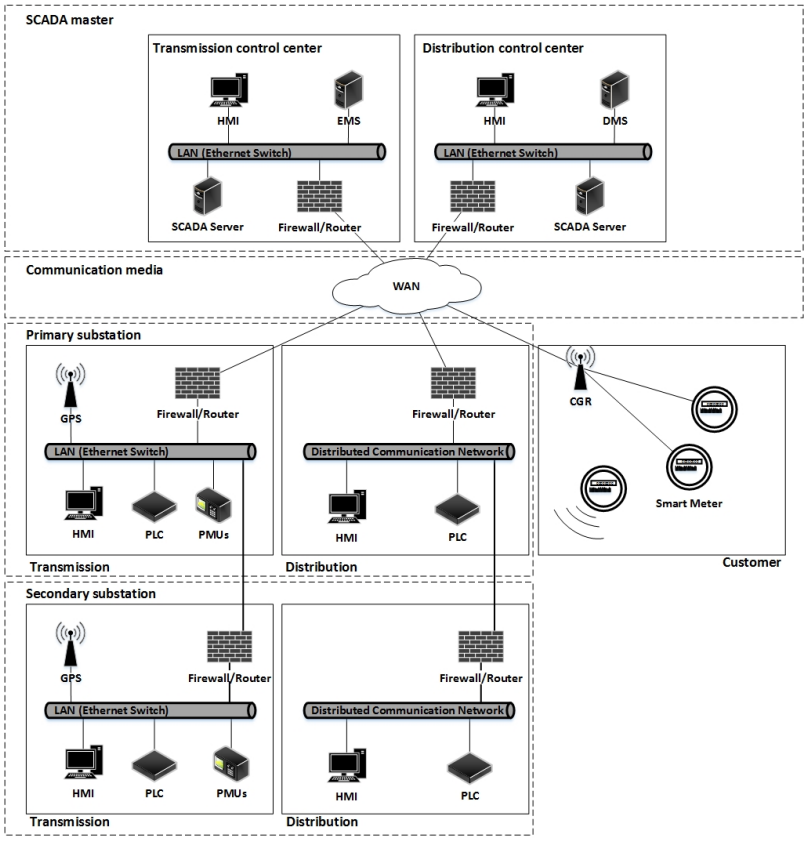


Figure 17: Smart grid model.

deployed. The primary requirements for SCADA in smart grid are to have a latency between 100 to 200 ms [63].

The PMU technology is characterized by a set of delays, which is shown in table 4.

Signal acquisition	Synchrophasor estimation	Communication	Data frame time-alignment	Bad data detection	State estimation
30 ms	< 1 ms	Variable	0-20 ms	< 1 ms	1-5 ms

Table 4: Latency components of PMU process [64].

- PMU signal acquisition - This PMU operation is a delay associated to correspond half of the window length used by PMU to measure a GPS-timestamp synchrophasor.
- PMU synchrophasor estimation and data encapsulation - The latency in this PMU operation depends on a number of input channels that PMU measures like voltages and currents.
- Communication network delay - The latency in the communication depends on the commu-

nication technologies used and the physical distance.

- PDC data frame time alignment - The phasor data concentrator task is to consistent feed datasets to the state estimation. This will compensate for possible network delay's and jitter. The phasors measured at the same instance in different grid locations must be delivered in the range of 0-20 ms apart form each other. This is important to time-align the data.
- Bad data detection - This process identifies corrupt and/or missed measurements. It can eventually replace measurements.
- State estimation - The delay in this operation depends on size of the network and the number of different parameters.

PMU is estimated to have a maximum total latency of 100 ms [64]. After the signal acquisition, synchrophasor estimation and the other operations, there is approximately 35-55 ms left for the communication infrastructure. Chai et al [64] estimated the mid-point of 10 ms as the requirement for PMU data delay jitter.

Smart meter

Smart meter are part of a service-based AMI. This is the interaction between customer and provider. Sally Lu et al. [65] propose five fundamental message classes: control, request, billing, electricity usage and warning messages. These message classes are divided into three categories, which are:

- Operation event
  - Control message
  - Request message
- Non-operation event
  - Billing message
  - Electricity message
- Asynchronous event
  - Warning message

There is a lot of messages generated from a wide range of devices to the control center and vice versa. The asynchronous events that consist of warning messages are generated by the smart meter to warn about physical events. These messages are unpredictable generated and the degree of urgency can vary. Some messages need very low latency while others can have high latency. Operational events consist of control messages that can tend to be constant in volume. The control messages are important and therefore needs low latency. While non-operational events need less strict latency requirements. To summarize, the smart meter isn't sensitive to jitter and needs best effort latency. It has a low data rate which is under 50Mbps.

5.2.5 Smart home

Smart home model

The figure 18 shows the model of a smart home automation. It uses cloud and brings the home appliances on the web and then it is possible to control any device from anywhere. The model consists of sensors, actuators and control entities. The context of cloud control is that the device in the environment communicate with the cloud. The cloud can be reached on the Internet and the actuators, sensors and user-controlled devices therefore needs to be connected to the Internet. There is also common that local and cloud control devices communicate together. This is also handled through the Internet and can be used for requesting information or trigger a purchase.

This paper proposes a framework with smoke detector, glass-break sensor, power plug and cameras. The cameras are directly connected to the cloud, while the smoke detector, power plug and glass-break sensor is connected to a gateway. The power-plug uses Zigbee to communicate with the gateway. The gateway enables devices that are not directly connected to the Internet, a way to reach the cloud and user web app. The data from these devices is sent to the cloud where it is processed.

The model consists of security and safety devices like smoke detector and glass-break sensor. These devices have sensors that can detect risk situation and trigger an appropriate action in response. For example, a glass-break sensor has a microphone to record sound. The sound recorded is analysed in order to detect sound of broken glass. If the glass-break sensor registers a glass breaking, it will trigger an alarm.

Latency and quality of service

There is a lot of different services running in the smart home network. It is therefore a need for quality of service solution to prevent congestions in the network. The users of the network will produce media stream, which should have low priority so it doesn't disturb other services with higher priority. The QoS will maintain an appropriate data rate for each service based on the priority of the application.

Video surveillance

A standard security camera using MPEG-4 uses a bandwidth of at least 1 to 2Mbps per camera, and 2 to 8Mbps with motion JPEG. For security cameras using High Definition (1920/1080) like H.264, assumes to use at least 4 to 6Mbps per camera. According to Cisco [66], the standard packet loss is defined below 0.5 of 1 percent can be acceptable. 1/10th of 1 percent can be noticeable for a high definition camera.

The latency for a surveillance camera depends mostly on the transport protocol. MPEG-4/H.246 transported in UDP/RTP between a camera and the network digital video recorder is less demanding then MPEG-4/H.264 transported in TCP. In a standard LAN environment, less then 10ms latency should be maintained. Latency in most WAN environments should be less than 50ms. Latency over 50ms in a WAN environment may cause poor video quality or other issues with usability. The Cisco web page [66] states that the jitter is of little concern if sufficient bandwidth is available. But the

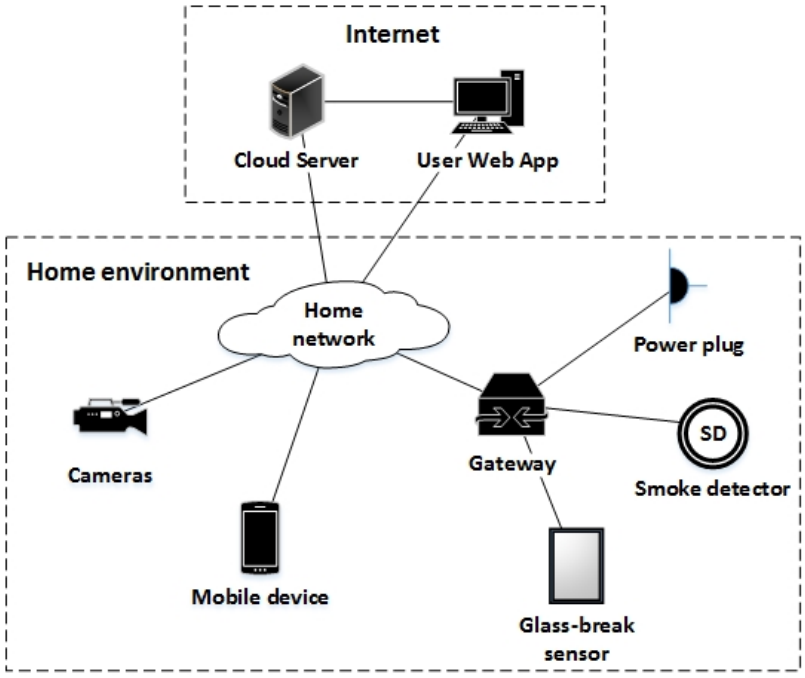


Figure 18: Smart home model.

jitter should be roughly less than 10 percent of the measured latency value. Cisco looked at a HD camera using MPEG-4/H.246, and reported the average packet size to be 1 397 bytes and there where sent 383 packets per second. This corresponds to a data rate around 4.3Mbps. The video surveillance traffic should be given preferable treatment over other data traffic from for example file transfer and sending E-mail. The communication direction is one-way.

Smoke detector

The smoke detector is a safety critical device. This means that failure or faulty execution by the device could result in injury or loss of human life. Smoke detectors are event-driven, which means the device reacts to certain critical event. The communication direction is one-way. The devices data flow only outward with and alarm. When there is no smoke detected no message is sent. Exception for this is a periodic ping of existence. The communication is primarily one-way, but other communications like updates to firmware can also be done. Some smoke detectors need a two-way communication. This will enable better fault management and a higher level of reliability. Since the network will provide acknowledgements of a received message when the smoke alarm sends out the alarm signal. The latency requirements are 100ms to 500ms and is not jitter sensitive. The data rate is under 100kbps [67].

5.3 Translation of topological models into network simulation environments with OMNeT++

The simulation was implemented with OMNeT++ version 5.4.1 and INET framework version 4.1.0. OMNeT++ is an open-source simulation toolkit for evaluating protocols and algorithms for wired and wireless networks. It is based on the C++ language and has a rich set of libraries and tools to simulate and develop network components and protocols. The INET framework provides pre-existing configuration which consists of a hierarchical mixed wireless and wired network.

5.3.1 Smart grid

From the OMNeT++ point of view, the network described in 5.2.4 can be seen from the simulator interface as shown in figure 19. This chapter will cover the different OMNeT++ and INET modules used in order to reproduce this network.

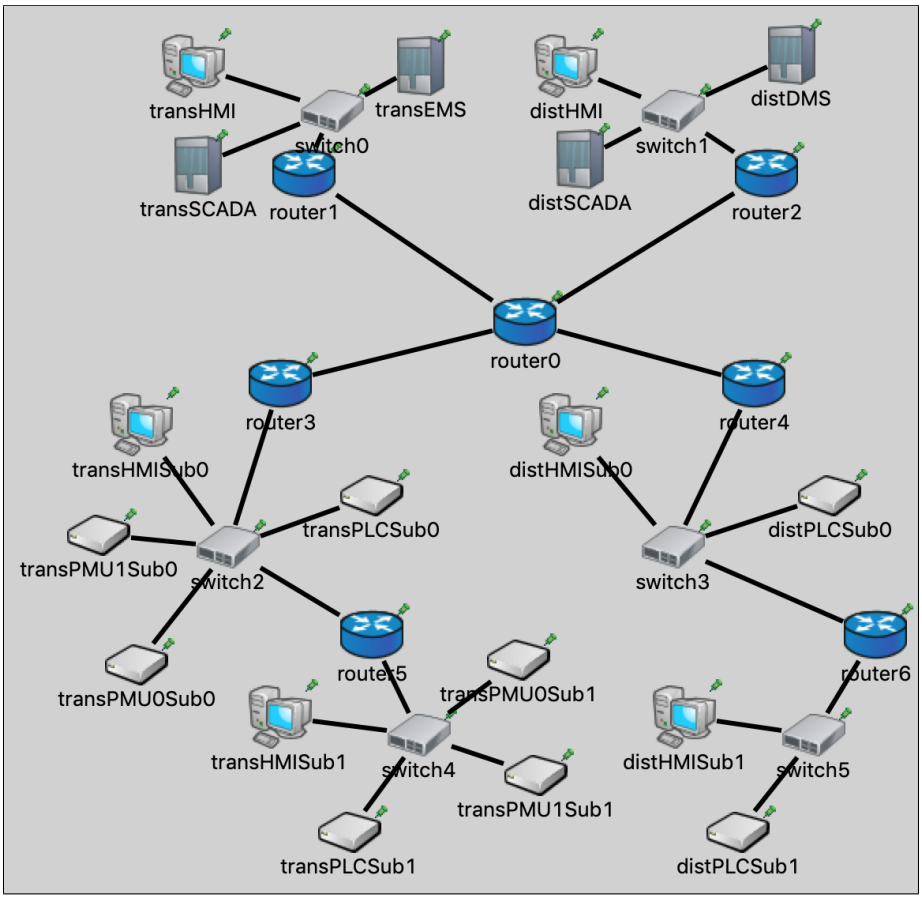


Figure 19: Smart grid model in OMNeT++.

PLC

The PLC will pass status value to the HMI and the SCADA server with DNP3 communication protocol. The PLCs will use the "SmartTcpSessionApp" module which is described under, to send TCP packets. The PLCs will use the "SmartTcpSessionApp" module which is based on the "TcpSessionApp" to send TCP packets. "TcpSessionApp" is a module in OMNeT++ that represents a single-connection TCP application. The module will open a connection, send the given number of bytes and then close the connection. "SmartTcpSessionApp" will keep this connection open and send packets in an interval between 10 to 70 milliseconds with a packet size between 60 and 70 bytes. The HMI machine and the SCADA server will use the "TcpEchoApp" to answer the packets. "TcpEchoApp" accepts the TCP connection, and sends back the message that arrived. The "IPv4Configurator" module is used to configure IPv4 addresses and routing tables. The IP addresses are assigned automatically.

The "SmartTcpSessionApp" module consists of the same functions as the "TcpSessionApp". The difference is that there are five more input parameters: *minInterval*, *maxInterval*, *minBytes*, *maxBytes* and *stopTime*. These parameters are used in the *parseScript* function, and is shown below:

Listing 5.1: *parseScript* function in SmartTcpSessionApp module

```
void SmartTcpSessionApp::parseScript(double maxInterval,
    double minInterval, int maxBytes, int minBytes,
    double stopTime, double tOpen2)
{
    double i = tOpen2;
    double randomInterval = 0;

    while(i <= stopTime){
        //Compute random interval between minInterval and
        //maxInterval
        randomInterval = (maxInterval-minInterval)*
            ( (double)rand() / (double)RAND_MAX);
        randomInterval = randomInterval + minInterval;

        i = i + randomInterval;

        simtime_t tSend = i;

        //Compute random bytes between minBytes and maxBytes
        long numBytes = rand() % maxBytes + minBytes;

        // add command
        EV_DEBUG << "␣add␣command␣(" << tSend << "s,␣" <<
            numBytes << "B)\n";
        commands.push_back(Command(tSend, numBytes));
    }
```

```
    EV_DEBUG << "parser finished\n";
}
```

The integer variable *i* is used for the while loop. The simulation is set to last 900 seconds and the while loop will be run through until the simulation time is more or equal to the value of *stopTime*. The TCP packet will be sent in a random interval between *minInterval* and the value of the *maxInterval* variable. The packet will be a random size between *minBytes* and the value of *maxBytes*. The output of the script is the variables *tSend* and *numBytes*, which is the time the packet is sent and the number of bytes the packet will contain. All of these variables must be defined in the initialization file in OMNeT ++

PMU

The PMUs will use the IEC 61850 to communicate with the HMI and the EMS server. The "EtherAppGoose" module is used by PMUs to send GOOSE messages. The module is a simple traffic generator for the GOOSE publisher model. The HMI machine and the EMS server uses "EtherAppServer" to respond to the GOOSE messages. The "EtherAppServer" module generates packets containing "EtherAppResp" chunks with the number of bytes requested [68]. PMU will also send out sample values to the HMI and the EMS server using the "EtherAppSv" module which will be answered with "EtherAppServer". The packet size created by the modules"EtherAppGoose" and "EtherAppSV" will be between 50 to 60 bytes.

5.3.2 Smart home

Figure 20 represent the model created in OMNeT++. This model is a representation of the smart home model created in chapter 5.2.5. Table 5 shows on the left side the components found in the smart home model in figure 18. And the right side of the table is the representing names in the OMNeT++ simulation.

Model	Simulation model
Cloud server	server0
User web app	server1
Home network	router1
Cameras	camera1
Power plug	sensor0
Smoke detector	sensor1
Glass-break sensor	sensor2
Mobile device	wirelessHost0

Table 5: The name of the devices in the simulation.

There are two radio mediums in the simulation. One is for the communication between the access point and the wireless host which uses the IEEE 802.11 communication protocol. The second radio medium is for the communication between the sensors and the gateway. These components will use the IEEE 802.15.4. This is a technical standard which is used in low-rate wireless personal

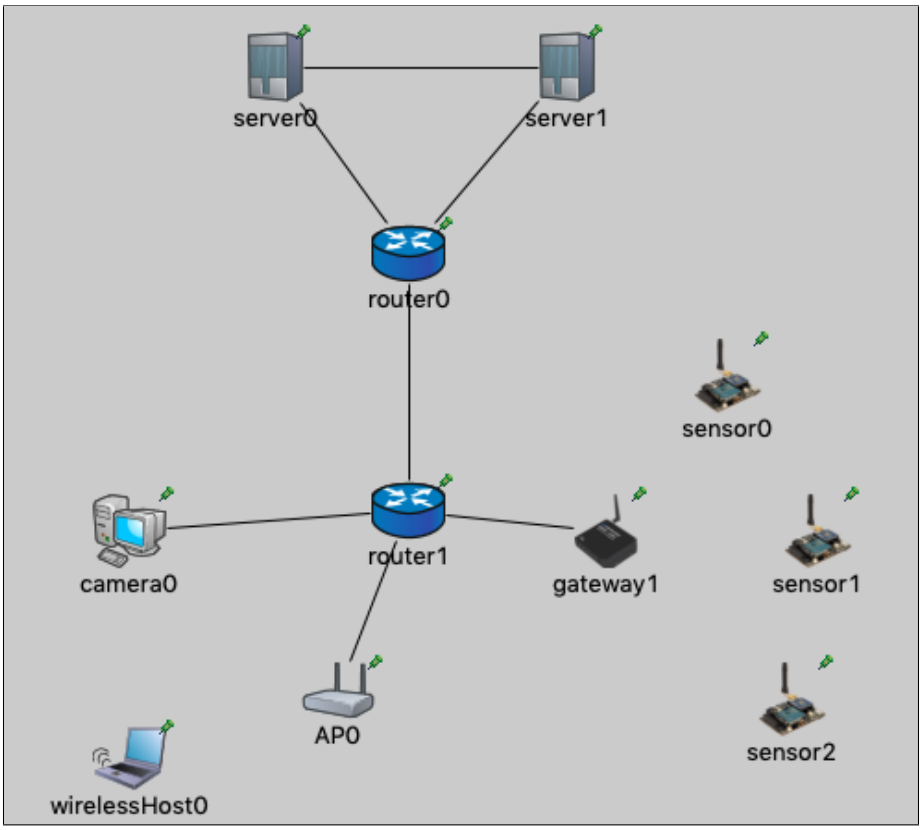


Figure 20: Smart home model in OMNeT++.

area networks and is the basis for Zigbee.

IP address attribution

For the network in the simulation to function properly, each nodes of the network must have a defined IP address. To do so, "IPv4NetworkConfigurator" module from the INET framework is used to configure IPv4 addresses and routing tables. The attribution can be either configured manually or automatically by the module. In the smart home simulation network, the "wirelessHost0" have been assigned to an IP address manually while the other devices have been assign to a IP address automatically. Each node in the network must have a network layer module named "IPv4NodeConfigurator" that sets the node's interface table and routing table based on the information defined by the "IPv4NetworkConfigurator" [69].

Quality of service in routers

The router's PPP interface contains the key elements of differentiated services in this network which is a queue and a traffic conditioner (egressTC). Both of them are used and is shown in figure 21.

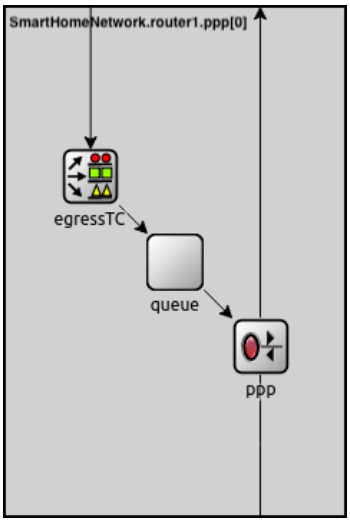


Figure 21: Router PPP interface [70].

To separate the packets of different flows the "mfClassifier" submodule is used in the traffic conditioner. "mfClassifier" contains a list of filters that identifies the flow and determines their classes. It can be classified on source and destination address, source and destination ports and IP protocol number [70]. "mfClassifier" determines the index of the out gate. If there is no match, the packet will be sent through the default out gate and if there is a match, the packet will be sent through "efMarker" and "efMarker2" which is prioritized gates. In this simulation the filter will send packets with source address "camera0" through the "efMarker". Packets with destination address to "server0", with TCP protocol and destination port "1234" will be sent through "efMarker2".

Communication between surveillance camera and cloud

The cloud server will use the "UdpVideoStreamClient" module. This module will send one video streaming request to the camera at a start time, and it will later receive a stream from the surveillance camera. The surveillance camera will use the "UdpVideoStreamServer" module. This module will wait for an incoming video stream request from the client, and it will then send a video stream to the source address, which is the cloud server. The packet length of the video stream is specified with the *packetLen* parameter. The packet length are 1367 bytes sent in an interval of 2,54 milliseconds.

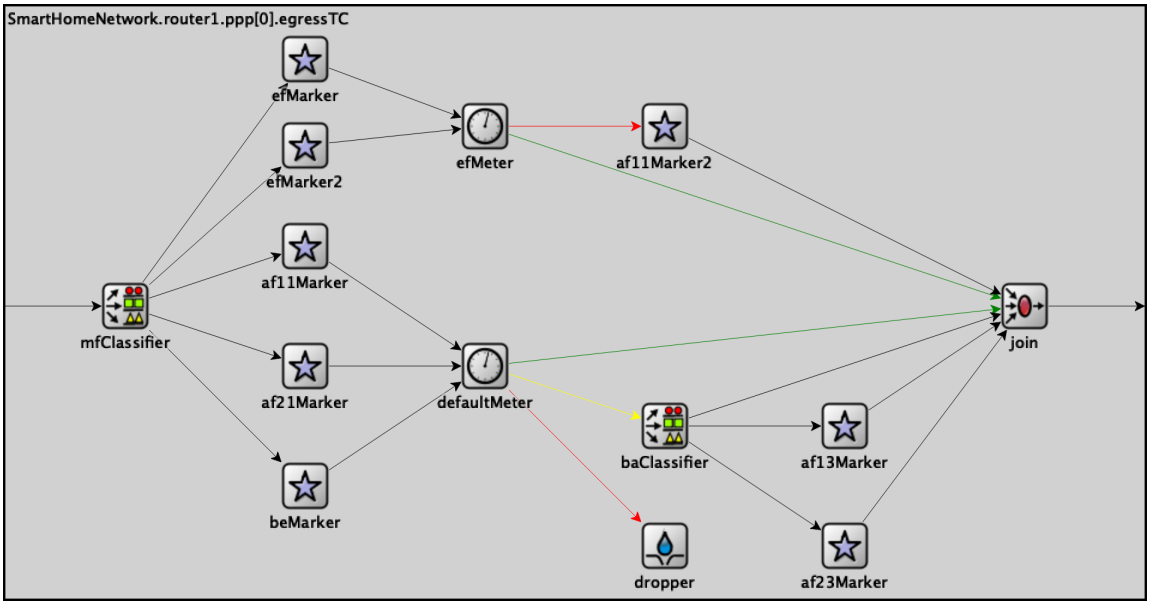


Figure 22: Traffic conditioner [70].

Communication between gateway and cloud

The communication between the gateway and the cloud will use TCP. The gateway will use the module "SmartTcpSessionApp" to communicate with the cloud server. It will open a connection and send packets with a packet size between 500 and 600 bytes to the cloud server in an interval between 50 and 500 milliseconds. The cloud uses the "TcpSinkApp" module which will accept the incoming TCP connection, and discard the data that arrives. The port number is specified, which is where the server will provide its service and the local address it is where it will bind to.

Communication between gateway and the sensors

The sensors will use the "UdpBasicApp" module to send messages to the gateway. This module sends UDP packets to a destination address in an interval set by the *sendInterval* parameter. The sensors are set to send UDP packets with a message length of 30 bytes which will be sent in an interval between 20 and 500 milliseconds. The gateway will use "UdpSink" to print the source, destination and the length of each packet received.

Communication for mobile device

The mobile device will use "HttpBrowser" to simulate browser operating on a single host. It operates with the user web app to provide a realistic simulation of web usage. The user web app uses "HttpServer" to respond the HTTP page request. The user web app server will respond with

a 200:OK HTML response, if the browser message is marked as bad, the server will respond with a 404:Not found message. The body of the 200:OK HTML response is a list of resource references [71]. The mobile device will also send TCP packets directly to the power plug with "TcpSessionApp". This will happen randomly four times in the simulation with a packet size of 60 bytes.

5.4 Real-time information and control flow in the chosen CPS, primarily capturing the master/slave hierarchies in ICS

5.4.1 Smart grid

Communication flow

There is a flow of information within the smart grid network. This information flow gives deep insight on power usage and enables predictions for future actions to increase energy efficiency and low overall cost [72]. Figure 23 illustrates the information and operation loops in a typical smart grid structure. Where measurements from sensors in the physical systems is sent to the control center and control commands are sent to the actuators based on the measurements.

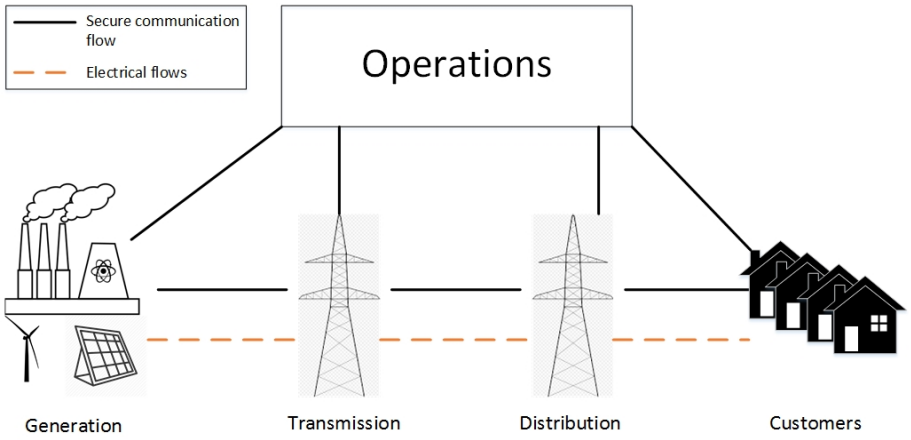


Figure 23: Smart grid information flow [2].

The smart grid system uses a two-way communication flow between the different domains. Most of this information flow is due to a massive use of sensors, actuators, and also smart meters in the customer domain. The information flow between the SCADA system and the distributed PLC is communicated through an Ethernet bus. Information about measurements from generation, transmission, distribution, and customers domain are received in the control center or operations domain. And control commands to actuators goes from the operations domain to the generation, transmission, distribution, and customers domain. Actuators in particular domains communicates with actuators in other domains. Figure 24 shows how the PLC communicates with the overall industrial control system architecture. The SCADA server and the HMI machine are able to start and stop cycles, adjust set points, and are also able to perform other functions that are required to

adjust control processes with control flow to the PLC. While PLC sends information flows back to the SCADA and HMI machine [6].

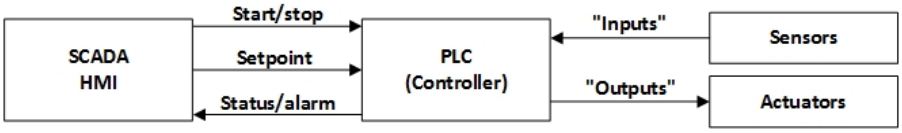


Figure 24: PLC information flow [6].

Smart grid hierarchy

Figure 25 reflects the control data flow in a primarily hierarchical manner. The field devices are subordinate to the substation and the substation is subordinate to the control center. The substations and field devices are able to make locally preprogramed actions. Some decisions are more complex and they therefore require broader grid considerations. The decision goes beyond the field devices and substation self-preservation like tripping circuit breakers. Substations to some extent and field devices exclusively rely on commands from the control center higher in the hierarchy [73]. The hierarchy mainly has a master-slave structure [74], which means that one device or process has one-way control over one or more devices. The master device will act as the controller and the slave devices are the ones being controlled [75].

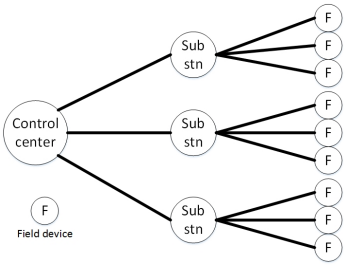


Figure 25: Hierarchical grid control data flow network [73].

5.4.2 Smart home

The flow of information in the smart home automation system can be divided into two categories: data flow and control flow. The data flow indicates the flow of data between a source to a destination, using a common communication protocol. Control flow is packages sent from a source device to a destination device with control signal to enable on or off the destination devices functions. The information flow in the network can be implemented through wired or wireless communication channels.

Communication flow

Figure 26 is a model of the communication flow between the different devices in the network. The smart home environment uses different types of sensors, actuators and user-devices. The arrows represent the flow of information between the different devices. The actuators and sensors are controlled by the cloud control or a local control entity. The user can control the system through different user interfaces like an app on the phone or a web interface located outside the home environment.

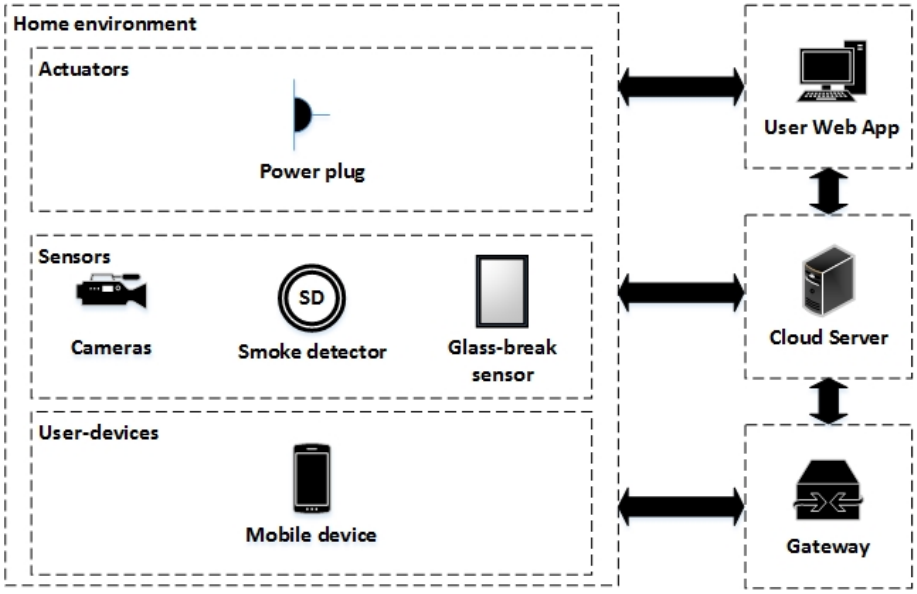


Figure 26: Smart home communication flow [5].

Control unit and devices

All the devices in the environment will exchange data with a control unit the whole time. Otherwise there will be no control of the environment. The control unit is localised in the cloud and in the local environment. This will often be on the user's mobile device.

Cloud and home environment

The devices within the home environment will communicate with the cloud. The cloud is located outside the home network and the devices therefore needs to be connected to the Internet.

User web app

The user web app will often be located outside the home environment and will communicate through the Internet. The user web app will communicate with the local environment and the cloud.

Smart home hierarchy

Figure 27 shows the smart home automation system hierarchy levels. At the lower level we find sensors and output devices. These devices will typically possess limited processing capabilities and limited power. The devices will therefore not be suited for complex processing tasks. It will instead be used to perform relatively simple processing tasks. The lower level devices will typically be implemented to perform specific tasks. For example, a smoke detector is a type of sensor that is employed with a sensor to analyse if there is a fire or not. If the device in the lower level is unable to process the input data, then the device will forward the data to a device on a higher level than itself which is the intermediate level.

The intermediate level consists of gateway entities like, mobile devices and control panels. These devices have much more processing power than the devices on the lower level. The devices on the intermediate level can perform a more general analysis compared to the lower level of the hierarchy. Devices located in the intermediate level can also be overwhelmed of information and data processing request. The information can therefore be pushed to the higher level.

The higher level can perform more complex analyses and tasks for the system. Moving real-time or near-real-time from the lower level to the higher level can decrease the reliability. The quality of service can be managed between lower level and intermediate level, but moving data to the higher level means moving data over an external network where the quality of service cannot be guaranteed.

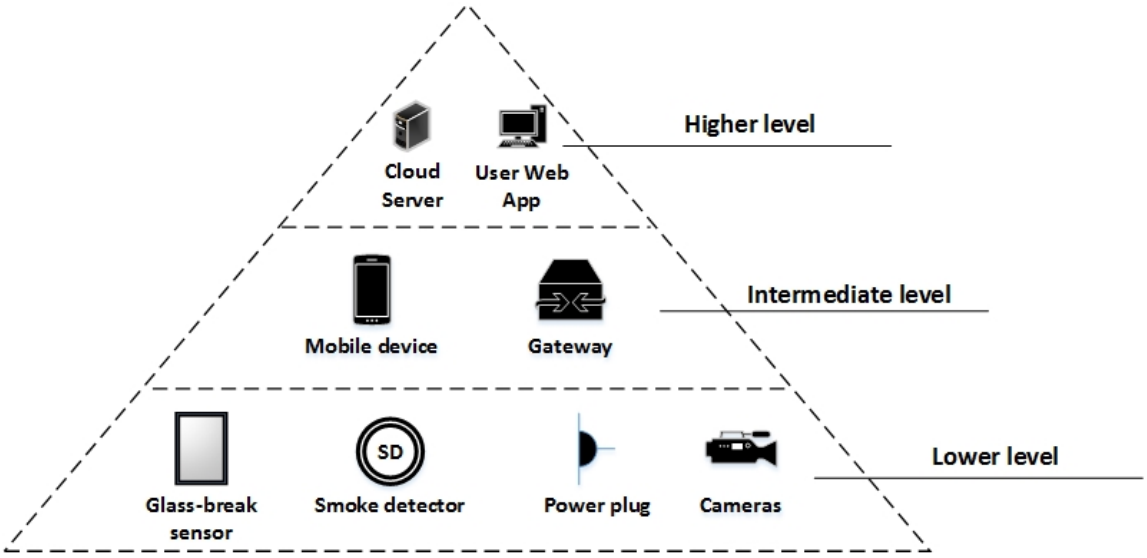


Figure 27: Smart home hierarchy [76].

Video surveillance transport layer protocol

TCP and UDP are two primary network protocols that can be used in the communication between the video surveillance and the server. The video surveillance will in this project use the UDP protocol. The TCP protocol will break down the stream of bytes from the video surveillance into segments. The segments will be organized and reconnected in the correct order on the host side. Lost packages will be resubmitted by the surveillance host. The UDP protocol is a connectionless protocol that keeps sending real-time data to the server. The downside of using the UDP protocol is that it is ignoring data confirmation and packet loss. The positive side of using the UDP protocol is the fast transmission.

5.5 Investigation of a selected set of network attacks scenarios, targeting real-time performance characteristics

5.5.1 Attack scenario

This chapter will justify the attack scenarios. The attack scenarios will assume that the attacker already has access to necessary controllable actuation points to send packets through the network. To obtain results of the attack scenarios in the smart grid and the smart home network, these thesis will focus on two scenarios as follows for the two networks:

- **Scenario A** – TCP end-to-end delay disruption
- **Scenario B** – UDP end-to-end delay disruption

Each scenario will study the effect of the attack over the two network architectures.

Performance measures

In order to characterize the influence the different attack scenarios have on the networks, there will be used three metrics which are defined as follows:

- **End-to-End delay** is the amount of time a packet uses to travel from a sender node until it is successfully received at the destination node.
- **Packet loss ratio** is the average number of packets that fails to reach their destination divided by the total number of packets sent.
- **Jitter** is small intermittent delays during data transfers.

The end-to-end delay, packet loss and jitter regarding the nodes network traffic are collected from the simulation.

End-to-end delay

The end-to-end delay is measured of a certain data flow by calculating the time it takes for every packet to reach its destination. The definition is found in section 5.2.2. The formula used to calculate the end-to-end delay is:

$$Latency_n = Arrivaltime_n - Sendingtime_n \tag{5.1}$$

The equation shows that end-to-end delay is the arrival time subtracted by packet sending time.

Packet loss

A definition of packet loss is found in section 5.2.3. Packet loss is measured by subtracting the total amount of packets sent by the node from the total amount of packets that were received by the destination node. This will give a percentage of the overall packet loss [77].

Jitter

The definition of jitter is found in section 5.2.2. Jitter or average delay jitter is the variation of the inter-arrival intervals form on packet received to the next packet received. Each node in the network will calculate the delay jitter from the packets received from the same origin source [78].

5.5.2 Scenario A

In scenario A the attacker will transmit TCP packets from the attacker machine to the other attacker machine in the network. The attacking hosts will generate legitimate but useless TCP traffic over the simulated network to occupy the communication channel, thereby reducing network availability. The "attackHost0" from figure 28 and figure 29 will use TcpSessionApp to send TCP packets to the "attackHost1". "AttackHost1" will use TcpEchoApp to answer the TCP packets. The TCP frames will be transmitted in an interval between 0,1 and 1 millisecond, and the packet size will be between 500 and 1000 bytes. The attacking host will start sending the TCP packets at 400 seconds which will indicate the start of the attack. The attack will last to the 600 second of the simulation.

5.5.3 Scenario B

Unlike scenario A, this scenario will use UdpBasicApp module to send UDP packets with 600 bytes to the "attackHost1". The UDP packets will be transmitted in an interval between 0,1 and 1 millisecond. The "attackHost1" will use UdpEchoApp to respond. The attack will start at 400 seconds and stop at 600 seconds. The attack is suppose to flood the access point, switches and router with packets.

5.5.4 Attack scenario in smart grid

In the attack scenarios on the smart grid one attacking host is connected to the router between primary substation and secondary substation in transmission. Another attacking host is connected to the router between primary substation and secondary substation in distribution as shown in figure 29. There will be simulated traffic transmitted between "attackHost0" and "attackHost1". By doing this, it will be possible to study if the traffic from the other nodes in the network is affected by the attacking traffic.

5.5.5 Attack scenario in smart home

In the attack scenarios on smart home one attacking host is connected to the router inside the home network. The other attacking host will be connected to the router from the outside of the home network. These hosts will send traffic between each other. This will make it possible to identify if the traffic between the other nodes in the network is affected by the attacking traffic.

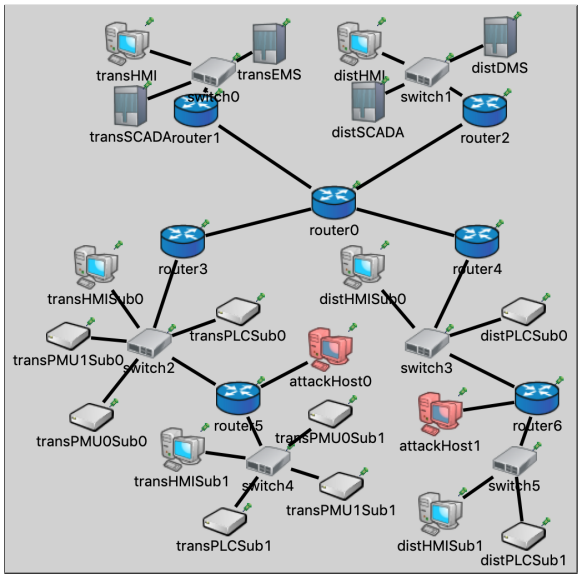


Figure 28: Smart grid attack scenario.

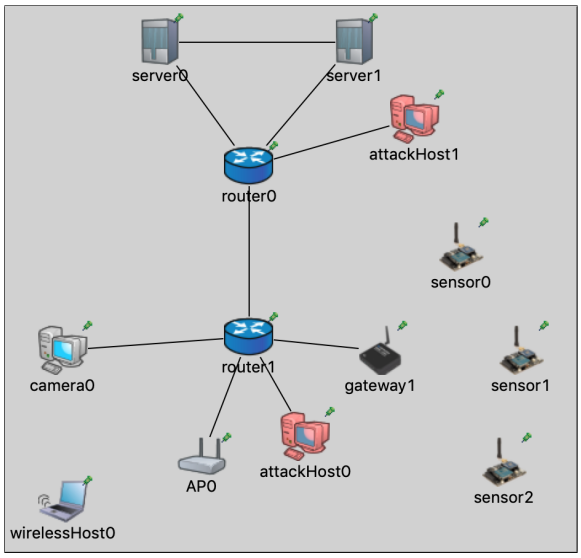


Figure 29: Smart home attack scenario.

6 Result

The thesis has implemented performance attack on two networks in a OMNeT++ simulator. OMNeT++ is used to analyse the performance of the networks before, during and after the attack. This chapter will look at the simulation results of attack scenario A and B on the smart grid and smart home automation system.

6.1 Smart grid attack scenario A

Simulation results for attack scenario A are shown in figure 30, 31, 32, 33 and table 6. Table 6 gives the numbers for latency and jitter for the different nodes before, during and after the attack. Figure 30 shows a chart of the end-to-end delay for the PLCs in the distribution section and figure 31 shows the PLCs in the transmission section. The x-axis interval between 400 and 600 visualize the impact of the attack scenario. The average latency and jitter for the PLCs in both sections are stable throughout the whole simulation. There is not any significant difference before, during and after the attack. Figure 32 and figure 33 shows a chart of the end-to-end delay of the PMUs. For the PMUs there are no difference in the latency before, during and after the attack. For the PMU in the primary substation the average latency is stable around 14,065ms for the whole simulation. The PMU in the secondary substation is also stable through the whole simulation with a latency of 20,086ms. There are some increases in the average jitter. Both the PMUs in the primary and secondary substation has an average jitter between 0,001 and 0,002ms before and after the attack. Under the attack the jitter increases for both of the PMUs. The PMU in the primary substation increases to 0,006ms and the PMU in the secondary substation increases to 0,011ms. The packet loss for both the PMUs increases from 0% before the attack to 0,02% during the attack.

	Latency (ms)			Jitter (ms)		
Attack	Before	During	After	Before	During	After
Transmission:						
PLC (sub 1)	31,925	31,817	32,010	6,529	6,379	6,638
PLC (sub 2)	51,884	51,659	51,791	11,958	11,952	11,847
PMU (sub 1)	14,065	14,065	14,065	0,001	0,006	0,001
PMU (sub 2)	20,086	20,087	20,086	0,001	0,011	0,002
Distribution:						
PLC (sub 1)	31,910	31,818	31,907	6,505	6,394	6,460
PLC (sub 2)	51,749	51,848	51,638	11,910	11,959	11,838

Table 6: Result smart grid attack scenario A on PLC and PMU.

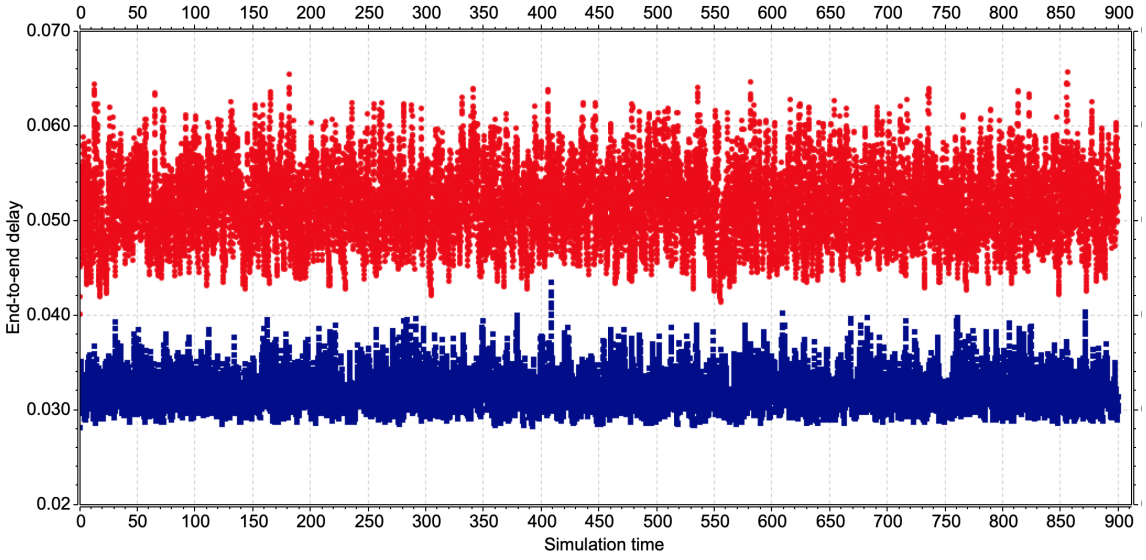


Figure 30: Smart grid attack scenario A moving average result for PLCs in the distribution section. Blue represent PLC in primary substation and red represent PLC in secondary substation.

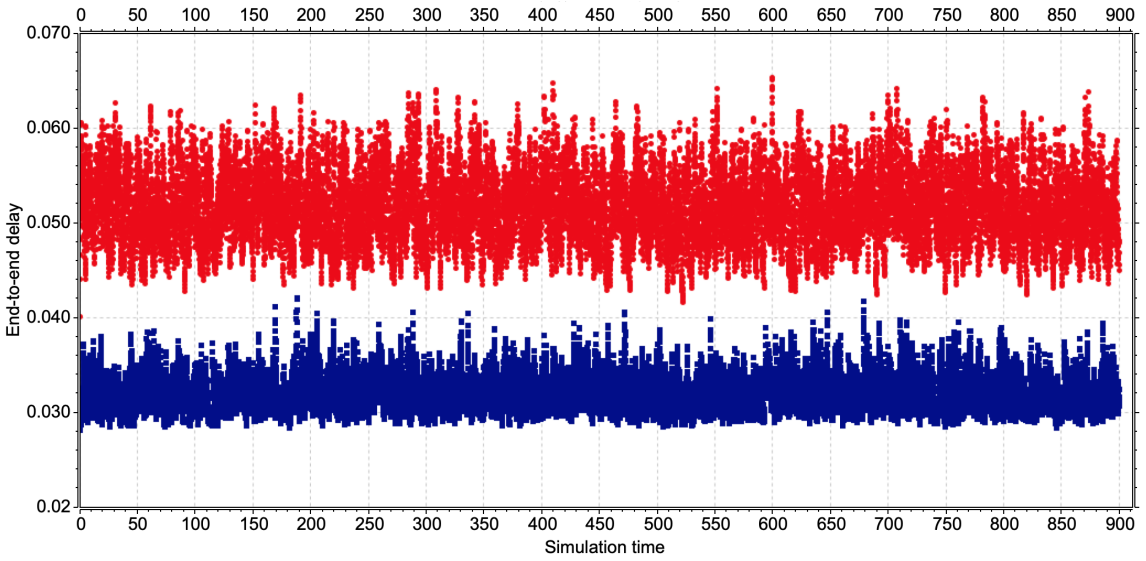


Figure 31: Smart grid attack scenario A moving average result for PLCs in the transmission section. Blue represent PLC in primary substation and red represent PLC in secondary substation.

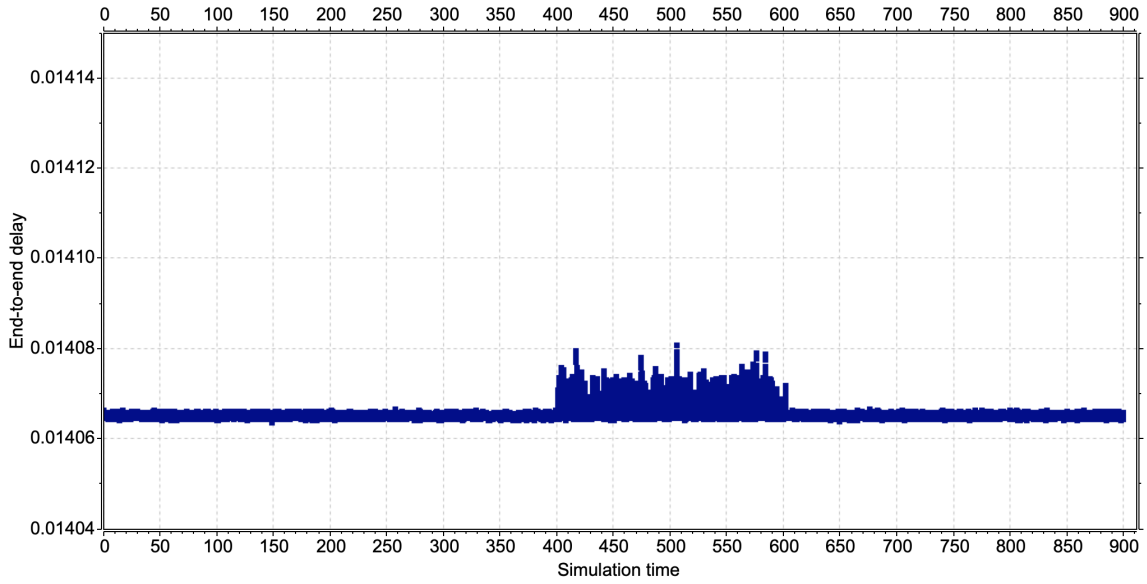


Figure 32: Smart grid attack scenario A moving average result for PMU in primary substation in the transmission section.

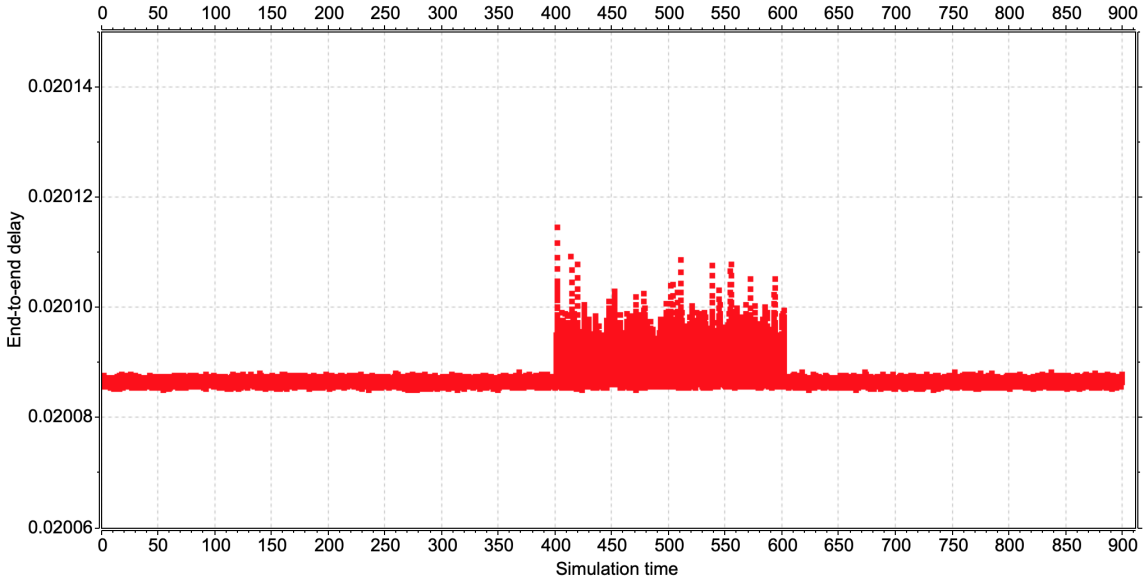


Figure 33: Smart grid attack scenario A moving average result for PMU in secondary substation in the transmission section.

6.2 Smart grid attack scenario B

Simulation results for attack scenario B are shown in figure 34, 35, 36, 37 and table 7. Table 7 gives the numbers for latency and jitter for the different nodes before, during and after the attack. Figure 34 shows a chart of the end-to-end delay for the PLCs in the distribution section and figure 35 is of the PLCs in the transmission section. The average latency and jitter for the PLC in both sections are stable throughout the whole simulation. There is not any significant difference before, during and after the attack. Figure 36 and figure 37 shows a chart of the end-to-end delay of the PMUs. For the PMUs there is some increases in the latency and jitter during the attack. For the PMU in the primary substation the average latency increases from 14,065ms to 14,073ms before it goes back to normal after the attack. The PMU in the secondary substation increases from 20,086ms to 20,103ms during the attack and goes back to normal when the attack ends. Both the PMUs in the primary and secondary substation has an average jitter at 0,001ms before and after the attack. Under the attack the jitter increases for both of the PMUs. The PMU in the primary substation increases to 0,021ms and the PMU in the secondary substation increases to 0,035ms. The packet loss for the PMU in the primary substation is 0% throughout the simulation, while the packet loss for the PMU in the secondary substation increases from 0% to 0,01% during the attack.

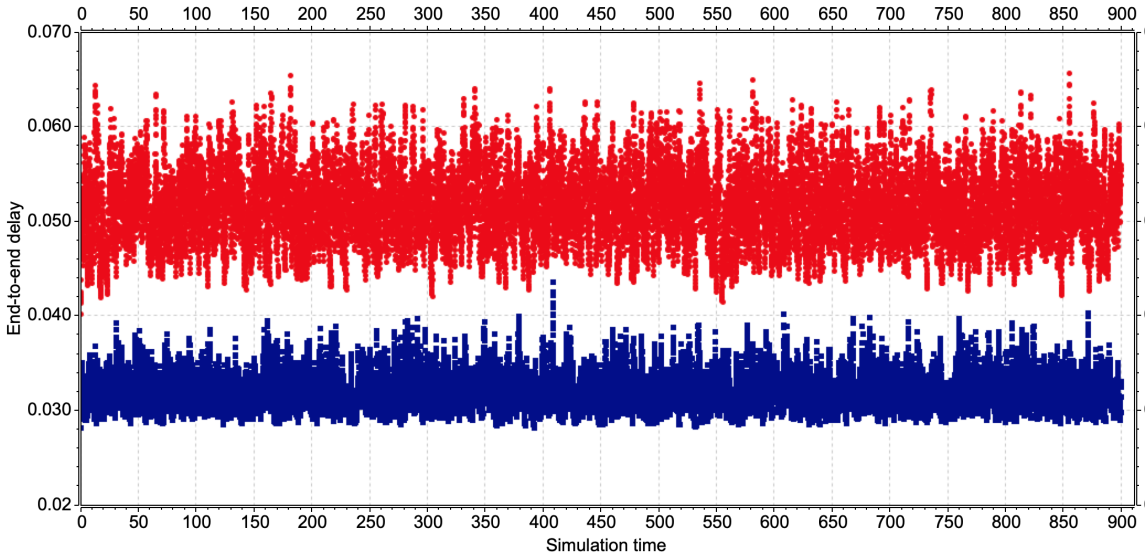


Figure 34: Smart grid attack scenario B moving average result for PLCs in the distribution section. Blue represent PLC in primary substation and red represent PLC in secondary substation.

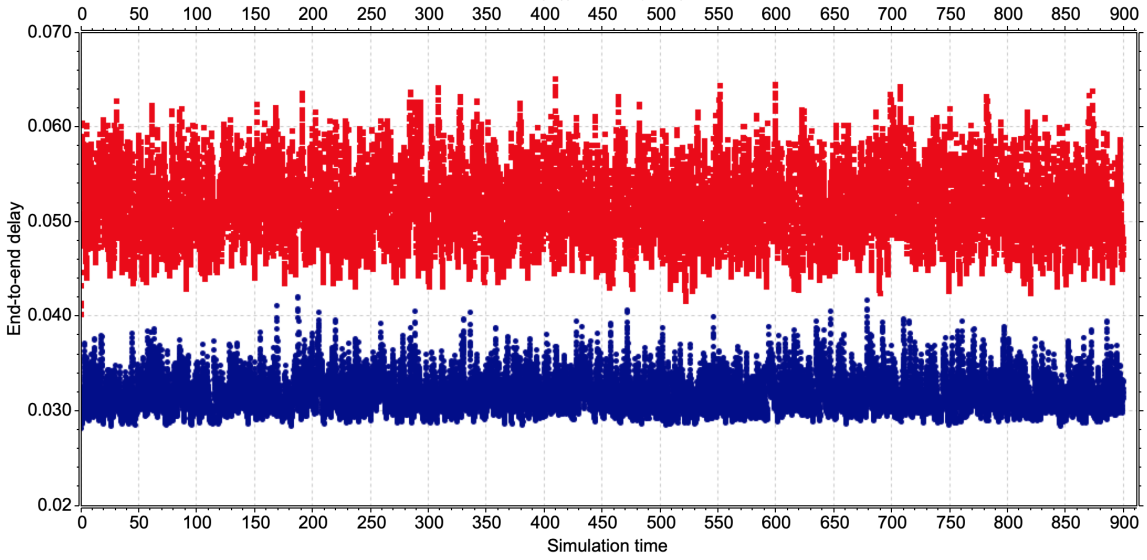


Figure 35: Smart grid attack scenario B moving average result for PLCs in the transmission section. Blue represent PLC in primary substation and red represent PLC in secondary substation.

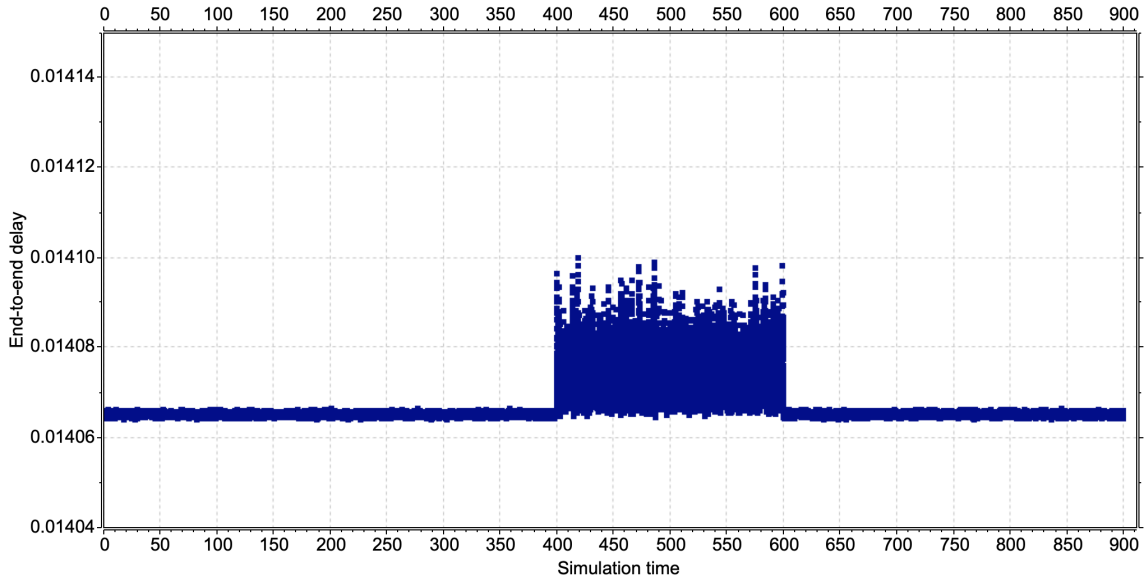


Figure 36: Smart grid attack scenario B moving average result for PMU in primary substation in the transmission section.

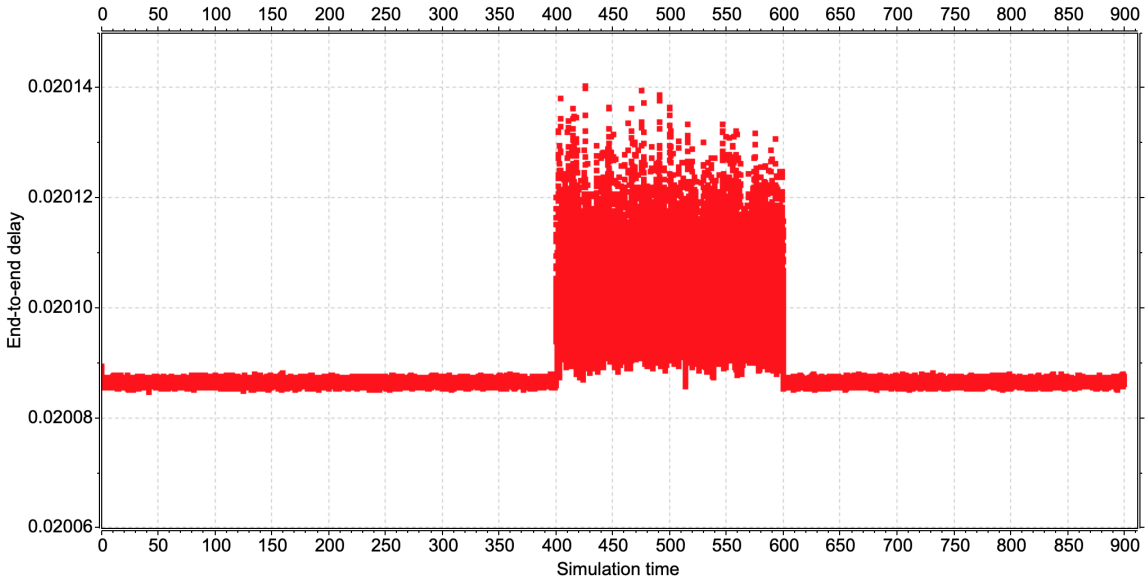


Figure 37: Smart grid attack scenario B moving average result for PMU in secondary substation in the transmission section.

	Latency (ms)			Jitter (ms)		
Attack	Before	During	After	Before	During	After
Transmission:						
PLC (sub 1)	31,885	31,845	31,977	6,477	6,392	6,513
PLC (sub 2)	51,779	51,738	51,186	11,935	11,974	11,848
PMU (sub 1)	14,065	14,073	14,065	0,001	0,021	0,001
PMU (sub 2)	20,086	20,103	20,086	0,001	0,035	0,001
Distribution:						
PLC (sub 1)	31,940	31,848	31,876	6,510	6,408	6,542
PLC (sub 2)	51,904	51,912	51,785	11,989	11,970	11,914

Table 7: Result smart grid attack scenario B on PLC and PMU.

6.3 Smart home attack scenario A

Simulation results for attack scenario A on the smart home automation network are shown in figure 38 and table 8. Both the figure and the table have the average end-to-end delay involved in sending messages from source to destination. This is one of the main parameters for message transfer. Figure 38 shows the average end-to-end delay performance for camera and gateway. Before the attack the average end-to-end delay for the camera's UDP packets to travel to the server was 2,372ms. During the attack this transfer increases to 2,382ms and after the attack it goes back to 2,372ms, as shown in table 8. For the average end-to-end delay for the gateway, it is difficult to see any different in the latency before, during and after the attack in figure 38. But in table 8 there is an increase from 1,420ms to 1,463ms average latency during the attack before the average latency goes back to 1,424ms.

Jitter should be of minimum value for the communication flow between source and destination for an efficient communication. As table 8 shows the jitter between camera and server is 0,015ms before the attack. During the attack this increases to 0,107ms and goes back to 0,016 after the attack. The jitter between gateway and server increases from 0,463ms to 0,483ms during the attack. After the attack the jitter goes down to 0,456.

The packet loss for the UDP packets between the camera and the server is absent before, during and after the attack. The packet loss between gateway and the server goes from 0,53% before the attack to 0,72% during the attack and then to 1,8% after the attack.

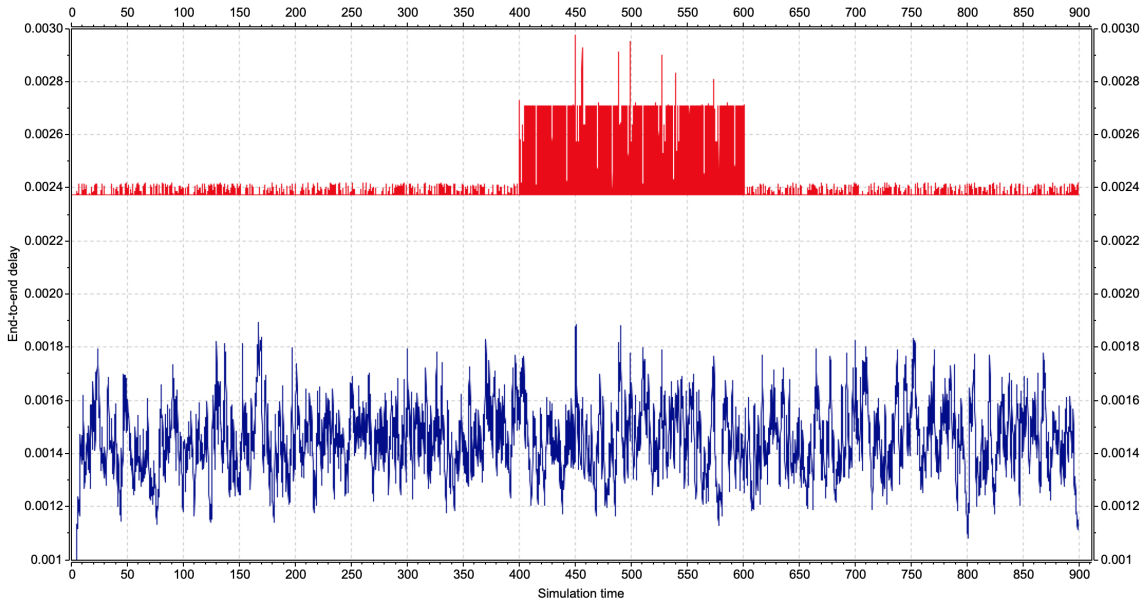


Figure 38: Smart home attack scenario A result - Moving average. Red represent end-to-end delay between camera and server. Blue represents end-to-end delay between gateway and server.

	Latency (ms)			Jitter (ms)		
Attack	Before	During	After	Before	During	After
Camera	2,372	2,382	2,372	0,015	0,107	0,016
Gateway	1,420	1,463	1,424	0,463	0,483	0,456

Table 8: Result from smart home attack scenario A.

6.4 Smart home attack scenario B

Simulation results for attack scenario B on the smart home automation system are shown in figure 39 and table 9. Both the figure and the table have the average end-to-end delay involved in sending messages from source to destination. This is one of the main parameters for message transfer. Figure 39 shows the average end-to-end delay performance for camera and gateway. Before the attack the average end-to-end delay for the camera's UDP packets to travel to the server was 2,372ms. During the attack this increases to 2,424ms and after the attack it goes back to 2,372ms as shown in table 9. For the average end-to-end delay for the gateway, it is possible to see a slight difference in the latency before, during and after the attack in figure 39. There is an increase from 1,444ms to 1,486ms average latency during the attack before the average latency goes back to 1,431ms.

As table 9 shows the jitter between the camera and the server is 0,013ms before the attack. During the attack this value increases to 0,123ms and goes back to 0,014 after the attack. The jitter between the gateway and the server increases from 0,462ms to 0,486ms during the attack. After the attack the jitter goes down to 0,464.

The packet loss for the UDP packets between the camera and the server is absent before, during and after the attack. The packet loss between the gateway and the server goes from 0,24% before the attack to 0,4% during the attack and then down to 0,03% after the attack.

	Latency (ms)			Jitter (ms)		
Attack	Before	During	After	Before	During	After
Camera	2,372	2,424	2,372	0,013	0,123	0,014
Gateway	1,444	1,486	1,431	0,462	0,486	0,464

Table 9: Result smart home attack scenario B.

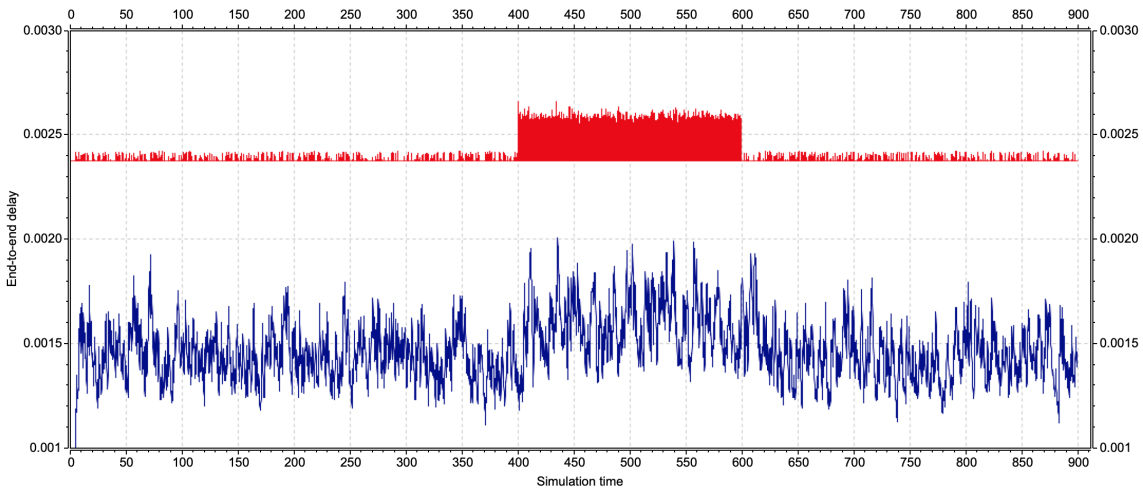


Figure 39: Smart home attack scenario B result - Moving average. Red represent end-to-end delay between camera and server. Blue represents end-to-end delay between gateway and server.

7 Conclusion

7.1 Discussion

While enjoying the latest intelligent technologies in smart grid for efficient and reliable power delivery, these technologies also face some critical security issues raised by both the original structural vulnerability of traditional power systems as well as its integration with communication networks. This thesis has focused on real-time performance characteristics of the smart grid topology created under delay attacks. The discussion in this work is drawn from the result from the PLCs and the PMUs end-to-end delay, jitter and packet loss, in the results from chapter 6. The attack scenario A is a TCP flood attack that generate legitimate but useless TCP traffic over the simulated network created. The simulated topology is based on the fundamental architectural characteristics and communication protocols in the smart grid sector. The attack showed a slight increase in the jitter and packet loss for the PMUs during the attack. The UDP flood attack in attack scenario B showed a slightly bigger increase in the average end-to-end delay and jitter during the attack, while the PLCs was unaffected by both of the attack scenarios.

For the smart home automation system, the result was drawn from the surveillance camera and gateway's end-to-end delay, jitter and packet loss. Both the attack scenarios affected the surveillance camera and the gateway, with an increase in the end-to-end delay and jitter during the attacks. The attacks had a greater impact on the average end-to-end delay and jitter for the camera's UDP packets then the gateway's TCP packets. The packet loss for the surveillance camera was unaffected, while the packet loss for the gateway increased during the attacks.

OMNeT++ uses a deterministic algorithm to generate random numbers, and initializes it to the same seed. The attack scenarios on the two simulated network was performed twice with different number of seed values, where the result was almost identical. The experiment could be performed with other number of seeds for potential variation and get a more reliable result.

Both the smart grid and smart home simulated networks was more affected by the UDP flood attack in attack scenario B. The flood attacks can result in an inability to access a device or the resources it offers. Some information sent from sensors is only valid and useful within a short amount of time. If the sampled value exceeds the short time frame, then the information does not serve its purpose any more. This can in worst-case scenario in the smart grid sectors, cause damage to the grid and blackouts. The attacks on the smart grid and smart home system caused just a temporal delay. The impact of the attack scenarios was minor and do not affect the overall state for both of the network systems simulated.

To achieve a greater impact on the smart grid, it would be preferred to conduct the attack during peak hours. This is a few hours per year, when contingences such as generator outages, failures of transmission lines or excessive demand condition, occur. To achieve less impact, it would be impor-

tant to research and implement countermeasures against these types of attacks. Countermeasures should secure against the adversarial threats, without affecting the performance characteristics of the system with too strong security controls.

7.2 Conclusion

The dynamic properties of cyber-physical systems make traditional penetration testing approaches harder to implement. The objective of this thesis was an analysis of reference scenarios and control systems architectures found in the smart grid and smart home automation system. The information gathered helped to get a better understanding of what a "normal operational condition" of the two systems are, as well as identify the fundamental architectural characteristics and communication protocols. This information was used to the creation of network topologies for a smart grid and a smart home automation system. These topological models were translated into network simulation environments using OMNeT++ and INET framework. Mock control and information flows have been designed to capture the master/slave hierarchies in the two topologies. Two network attacks, particularly targeting real-time performance characteristics such as packet dropping, message delays and jitter for periodic messages in the simulation framework has been created.

Finally, the conclusions of this thesis were based on two attack scenarios both performed on the smart grid and smart home infrastructure. The performance attack has been simulated on a realistic smart grid and smart home topology. It is concluded by the simulation result, which are presented in chapter 6, that the attacks on smart grid and smart home just caused a temporal delay. The impact of the attacks was minor issues and do not affect the overall state for both of the network systems simulated.

7.3 Possible extensions

Based on the results of the study, there are several recommendations for future research. First, the models developed in chapter 5 provide an approximation of the behavior of the dynamic elements in the smart grid and smart home topologies. The topologies developed could be extended to include more nodes which will present both a higher degree of structural knowledge as well as simulating more data traffic flow through the networks. Also, communication protocols should be improved in the simulated smart grid topology to get a result that can, to a greater extent, reflect a smart grid system in the real world.

Additionally, simulate defense strategies with limited strength and resources can be implemented to respond to different types and stages of attacks on performance characteristics.

Further research about different attack scenarios targeting real-time performance characteristics should also be carried out. For example, ARP flooding attack where the network is flooded with ARP replies, to make the system unable to resolve IP and MAC addresses.

List of abbreviations

ADR Automated Demand Response

AES Advanced Encryption Standard

AMI Advanced Metering Infrastructure

CCMP Counter Mode Cipher Block Chaining Message Authentication Code Protocol

CCU Central Control Unit

CPS Cyber-Physical System

CSMA/CA Carrier Sense, Multiple Access with Collision Detection

DMS Distribution Management System

DNP Distributed Network Protocol

DoS Denial of Service

EMS Energy Management System

HMI Human Machine Interface

IED Intelligent Electronic Device

IP Internet Protocol

ISM Industrial, Scientific and Medical

LAN Local Area Network

MDMS Meter Data Management System

PDC Phasor Data Concentrator

PLC Programmable Logic Controller

PMU Phasor Measurement Unit

RCU Remote Control Unit

RTO Regional Transmission Operator

RTU Remote Terminal Unit

SCADA Supervisory Control and Data Acquisition

SPDC Super Phasor Data Concentrator

TCP Transmission Control Protocol

TKIP Temporal Key Integrity Protocol

UDP User Datagram Protocol

WAN Wide Area Network

WPA Wi-Fi Protected Access

WPA2 Wi-Fi Protected Access II

Bibliography

[1] Coordination group on smart energy grids cyber security and privacy. CEN-CENELEC-ETSI Coordination Group on Smart Energy Grids (CG-SEG), 2016.

[2] Bryson, J. & Gallagher, P. D. 2012. Nist framework and roadmap for smart grid interoperability standards, release 2.0. *National Institute of Standards and Technology (NIST), NIST Special Publication 1108R2*.

[3] E. M. Carlini, G. M. Giannuzzi, P. M. P. S. A. V. & Villacci, D. 2016. A decentralized and proactive architecture based on the cyber physical system paradigm for smart transmission grids modelling, monitoring and control. *CrossMark, Technol Econ Smart Grid Sustain Energy*.

[4] B. Barman, A. K. Ram, J. J. B. M. & Pall, S. 2016. Development of a system model for home automation. *Journal of the Association of Engineers, India*, 86(3 and 4).

[5] D. Meyer, J. Haase, M. E. & Klauer, B. 2016. A threat-model for building and home automation. *IEEE 14th International Conference on Infustrial Informatics (INDIN)*.

[6] Knapp, E. & Langill, J. T. 2014. *Industrial Network Security Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems (2nd ed.)*. Syngress/Elsevier.

[7] E. J. Byres, M. F. & Miller, D. 2004. The use of attack trees in assessing vulnerabilities in scada systems. *Proc. Int. Infrastruct. Survivability Workshop*.

[8] Alcaraz, C. & Zeadally, S. 2015. Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection (IJCIP), Elsevier Science*, 8, 5366.

[9] Li, F. & Tang, Y. 2018. False data injection attack for cyber-physical systems with resource constraint. *IEEE TRANSACTIONS ON CYBERNETICS*.

[10] Hou, F. & Sun, J. 2017. Fasle data injection attacks in cyber-physical systems based on inaccurate model. *IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*.

[11] B. Zhu, A. J. & Sastry, S. 2011. A taxonomy of cyber attacks on scada systems. *Int. Conf. Internet Things 4th Int. Conf. Cyber Phys. Soc. Comput., Dalian, China*, 380–388.

[12] S. East, J. Butts, M. P. & Shenoi, S. 2009. A taxonomy of attacks on the dnp3 protocol. *Critical Infrastructure Protection III, IFIP AICT 311*, 67–81.

[13] B. Kang, P. Maynard, K. M. S. S. F. A. C. S. F. K. & Strasser, T. 2015. Investigating cyber-physical attacks against iec 61850 photovoltaic inverter installations. *IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA)*.

[14] A. Humayed, J. Lin, F. L. & Luo, B. 2017. Cyber-physical systems security—a survey. *IEEE INTERNET OF THINGS JOURNAL, vol. 4, no. 6*, 4(6).

[15] G. Francia, D. T. & Brookshire, T. 2012. Wireless vulnerability of scada systems. *ACM Southeast Regional Conf., Tuscaloosa, AL, USA*, 331–332.

[16] Z. Lu, X. Lu, W. W. & Wang, C. 2010. Review and evaluation of security threats on the communication networks in the smart grid. *The 2010 Military Communications Conference, MILCOM, San Jose, CA, USA*, 1830–1835.

[17] Z. Lu, W. W. & Wang, C. 2011. From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic. *IEEE INFOCOM, Shanghai, China*, 1871–1879.

[18] Y. Liu, P. N. & Reiter, M. K. 2011. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security*, 14(1).

[19] Barriga, J. J. & Yoo, S. G. 2018. Security over smart home automation systems: A survey. *International Conference of Research Applied to Defense and Security, MICRADS 2018: Developments and Advances in Defense and Security*, 87–96.

[20] K. Papadopoulos, T. Zahariadis, N. L. & Voliotis, S. 2008. Sensor networks security issues in augmented home environment. *2008 IEEE International Symposium on Consumer Electronics, pp. 1–4.*, 1–4.

[21] K. Islam, W. S. & Wang, X. 2012. Security and privacy considerations for wireless sensor networks in smart home environments. *Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design*.

[22] Can, O. & Sahingoz, O. K. 2015. A survey of intrusion detection systems in wireless sensor networks. *In Proceedings of the 2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO)*, 1–6.

[23] Bellardo, J. & Savage, S. 2003. 802.11 denial of service attacks: Real vulnerabilities and practical solutions. *Proceedings of the 12th USENIX Security Symposium*, 15–28.

[24] Sudit, M. E. K. M. 2007. Cyber attack modeling and simulation for network security analysis. *WSC '07 Proceedings of the 39th conference on Winter simulation: 40 years! The best is yet to come*, 1180–1188.

[25] Ashibani, Y. & Mohmound, Q. H. 2017. Cyber physical systems security: Analysis, challenges and solutions. *Computer and Security*, 68, 81–97.

[26] J. Lee, B. B. & Kao, H. 2015. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters*, 3, 18–23.

[27] Borlase, S. 2013. *Smart Grids: Infrastructure, Technology, and Solutions*. CRC Press.

[28] Sand, K. 2012. https://www.ntnu.edu/ie/smartgrids/what-is. https://www.ntnu.edu/ie/smartgrids/what-is. Accessed: 2019-05-21.

[29] SmartGrid.gov. 2011. What is the smart grid? https://www.smartgrid.gov/the_smart_grid/smart_grid.html. Accessed: 2019-05-01.

[30] W. Wang, Y. X. & Khanna, M. 2011. A survey on the communication architectures in smart grid. *Computer Networks*, 55, 3604–3629.

[31] Bolton, W. 2015. *Programmable Logic Controllers, Sixth Edition*. Newnes.

[32] S Wallace, X. Zhao, D. N. & Lu, K. T. 2016. *Big Data, Principles and Paradigms, chap. 17, Big Data Analytics on a Smart Grid: Mining PMU Data for Event and Anomaly Detection*. Morgan Kaufmann.

[33] Ball, F. & Basu, K. 2016. Performance evaluation of time-critical smart grid applications. *Proceedings of the Eleventh International Network Conference*, 13–15.

[34] j. M. Colbert, E. & Kott, A. 2015. *Cyber-security of SCADA and Other Industrial Control Systems*. Newnes.

[35] Gunti, V. 2015. What is scada/ems/gms and scada/dms? https://www.linkedin.com/pulse/what-scadaemsgms-scadadms-gunti-vijay/. Accessed: 2019-05-12.

[36] Mattioli, R. & Moulinos, K. 2015. *Communication network interdependencies in smart grids*. Enisa.

[37] Rouse, M. 2018. Smart home or building (home automation or domotics). https://internetofthingsagenda.techtarget.com/definition/smart-home-or-building. Accessed: 2019-05-22.

[38] M. R. Alam, M. B. I. R. & Ali, M. A. M. 2012. A review of smart homes—past, present, and future. *IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS*, 42(6), 1190–1203.

[39] imm.dtu.dk. 2018. Taxonomy of smart houses. http://www.imm.dtu.dk/~cdje/SmartHouseWebSite/taxonomy.html. Accessed: 2019-05-23.

[40] K. Ghirardello, C. M. & Kearney, P. 2018. Cyber security of smart homes: Development of a reference architecture for attack surface analysis. *Living in the Internet of Things: Cybersecurity of the IoT*.

[41] Chong, K. Y. 2012. Sensors in intelligent green buildings. *Electronics and Telecommunications Research Seminar Series*, 53–56.

[42] Mackiewicz, R. E. 2006. Overview of iec 61850 and benefits. *In proceeding of the IEE PES Power Systems Conference and Exposition*, 623–630.

[43] OMICRON. 2013. Sample values in iec 61850 environments. https://www.omicronenergy.com/en/applications/power-utility-communication/sampled-values-in-iec-61850-environments/#contact-menu-open. Accessed: 2019-05-01.

[44] K. McLaughlin, I. Friedberg, B. K. P. M. S. S. & McWilliams, G. 2015. Smart grid security: Innovative solutions for a modernized grid, chap. secure communications in smart grid: networking and protocols. *Elseview Inc.*, 113–148.

[45] P. Overholt, K. Uhlen, B. M. & Valentina, O. 2016. Synchrophasor applications for wide area monitoring and control. *International Energy Agency*.

[46] Martin, K. E. et al. 2014. An overview of the ieee standard c37.118.2—synchrophasor data transfer for power systems. *IEEE TRANSACTIONS ON SMART GRID*, 5(4), 1980–1984.

[47] Rastogi, T. & Sharma, R. R. 2014. Home automation system design: the basics. *Embedded*. URL: https://www.embedded.com/design/connectivity/4431025/Home-automation-system-design--the-basics.

[48] Stallings, W. 2013. *Network Security Essentials: Applications and Standards, 5th ed.* Pearson, London, NY, USA.

[49] Fall, K. R. & Stevens, W. R. 2011. *TCP/IP Illustrated: The Protocols, vol. 1*. AddisonWesley.

[50] Primer. 2014. *Wi-Fi: Overview of the 802.11 Physical Layer and Transmitter Measurements*. Tektronix.

[51] Brenner, P. 1996. *A Technical Tutorial on the IEEE 802.11 Protocol*. BreezeCOM.

[52] Microchip. 2019. Tcp vs. udp. https://microchipdeveloper.com/tcpip:tcp-vs-udp. Accessed: 2019-05-14.

[53] Odom, W. 2013. *Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide, Academic ed.* Cisco Press, 800 East 96th Street, Indianapolis, IN 46240.

[54] Rouse, M. 2014. Tcp (transmission control protocol). https://searchnetworking.techtarget.com/definition/TCP. Accessed: 2019-05-14.

[55] Farahani, S. 2008. *ZigBee Wireless Networks and Transceivers*. Elsevier.

[56] Williams, D. 2017. A battle of iot protocols. https://www.allaboutcircuits.com/news/a-battle-of-iot-protocols-zigbee-vs-thread/. Accessed: 2019-05-06.

[57] Ergen, S. C. 2004. *ZigBee/IEEE 802.15.4 Summary*. U.C. Barkeley.

[58] Blom, J. 2013. Bluetooth basics. https://learn.sparkfun.com/tutorials/bluetooth-basics/all. Accessed: 2019-05-12.

[59] Communications requirements of smart grid technologies. Dep. of Energy, United States of America, 2010.

[60] Kansal, P. & Bose, A. 2012. Bandwidth and latency requirements for smart transmission grid applications. *IEEE TRANSACTIONS ON SMART GRID*, 3(3), 1344–1352.

[61] N. Kayastha, D. Niyato, E. H. & Han, Z. 2014. Smart grid sensor data collection, communication,and networking: a tutorial. *WIRELESS COMMUNICATIONS AND MOBILE COMPUTING*, 1055–1087.

[62] M. H. Yaghmaee, Z. Yousefi, M. Z. & Alishahi, S. 2013. Quality of service guarantee in smart grid infrastructure communication using traffic classification. *22nd International Conference on Electricity Distribution*.

[63] Technology white paper, alcatel/lucent. Smart Choices for the Smart Grid. Retrieved from the web, 2011.

[64] W. E. Chai, N. Wang, K. V. K. & Kamel, G. 2015. An information-centric communication infrastructure for real-time state estimation of active distribution networks. *Smart Grid, IEEE Transactions on*, 6(4), 2134–2146.

[65] S. C.W. Lu, Q. W. & Seah, W. K. 2012. Quality of service provisioning for smart meter networks using stream control transport protocol. *IEEE communication magazine*, 3.

[66] Cisco. 2010. Network readiness assessment for ip video surveillance. https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Video/IPVS/IPVS_Network_Assessment.html. Accessed: 2019-02-26.

[67] ATIS. 2019. Iot characteristics matrix. *IEEE - Documents*.

[68] inet.omnetpp.org. 2018. Httpserver.ned. https://github.com/inet-framework/inet/blob/v4.1.0/src/inet/applications/ethernet/EtherAppServer.ned. Accessed: 2019-05-25.

[69] inet.omnetpp.org. 2017. Ipv4 network configurator tutorial released. https://inet.omnetpp.org/2017-09-15-ipv4configurator-tutorial-released.html. Accessed: 2019-05-25.

[70] inet.omnetpp.org. 2018. Differentiated services. https://inet.omnetpp.org/docs/showcases/general/diffserv/doc/index.html. Accessed: 2019-05-25.

[71] inet.omnetpp.org. 2018. Httpserver.ned. https://github.com/inet-framework/inet/blob/v4.1.0/src/inet/applications/httptools/server/HttpServer.ned. Accessed: 2019-05-25.

[72] M. Jaradat, Moath. Jarrah, A. B. Y. J. & Al-Ayyoub, M. 2015. The internet of energy: Smart sensor networks and big data management for smart grid. *Procedia Computer Science 56*, 592–597.

[73] Overman, T. M. & Sackman, R. W. 2010. High assurance smart grid: Smart grid control systems communications architecture. *First IEEE International Conference on Smart Grid Communications*, 19–24.

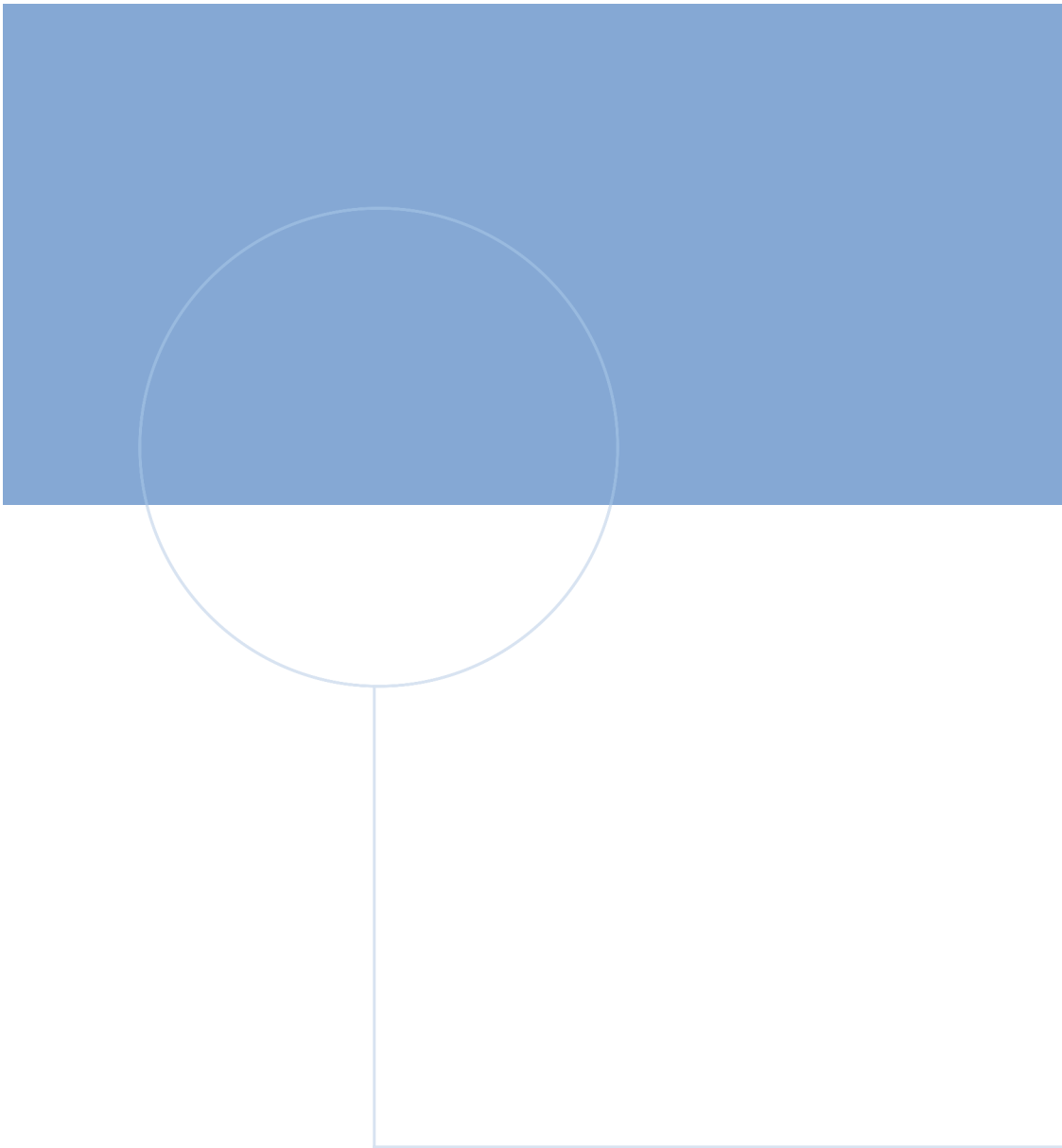
[74] B. Bumiller, L. L. & Hrasnica, H. 2010. Power line communication networks for large-scale control and automation systems. *IEEE Communications Magazine*, 48, 106–113.

[75] Techopedia. 2014. Master/slave. https://www.techopedia.com/definition/2235/masterslave. Accessed: 2019-05-17.

[76] J. A. Breed, A. B. & Hill, G. 2015. Method and apparatus for automation and alarm architecture. *Patent no. US 10084638*.

[77] M. Chenine, I. A. Khatib, J. I. V. M. & Nordström, L. 2010. Pmu traffic shaping in ip-based wide area communication. *5th International Conference on Critical Infrastructure (CRIS)*.

[78] Nguyen, H. L. & Nguyen, U. T. 2012. A study of different types of attacks in mobile ad hoc networks. *25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*.



NTNU
Norwegian University of
Science and Technology