Demand Response under cyber-attacks

Master thesis submitted to Delft University of Technology

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

in Engineering and Policy Analysis

Faculty of Technology, Policy and Management

by

Eleni Tzanakou

Student number: 4417895

To be defended in public on June 27, 2016

Graduation committee

Chair	: Prof. dr. ir. P.M. Herder, TU Delft
First Supervisor	: Dr. A. H. Teixeira, TU Delft
Second Supervisor	: Prof dr. J. A. Annema, TU Delft

An electronic version of this thesis is available in this link.

ACKNOWLEDGEMENTS

This thesis was the final step of my journey in the Engineering and Policy Analysis Programme, at TU Delft. Firstly, I would like to express my gratitude to the members of my thesis committee. I would like to thank the chair of my committee Prof. Paulien Herder, who greatly supported me through this process by providing me with valuable comments and suggestions. I really appreciate your patience when I was under stress and I feel grateful meeting you in my academic life.

A special thanks goes also to my third supervisor Dr. Jan Annema who had the willingness to be involved in every stage of this thesis and provided me with critical advices and comments from a different perspective. I feel you have helped me to grow professionally and broaden my horizon with regard to my thesis topic, thank you!

Thirdly, I would like to thank Dr. André Miguel Herdeiro Teixeira. I feel words cannot express how grateful I am for your encouragement and support. I am thankful that I met you in my life. You have taught me how to surpass obstacles with a smile and continued to believe in me when I lost faith in my own abilities. I will never forget you for that. I learnt many lessons from you both academic and for life.

Further, I would like to express my gratitude and appreciation to my senior professor in Greece for his time and efforts to support me in a specific step of this research.

This acknowledgement would not be complete without thanking Ms. Marja Brand for her support and her advices. You have always found a way to cheer me up when I was down, I would like to take the opportunity to let you know how much that means to me.

My life partner, Louka, for his patience in the difficult times, his endless love and support. My love, thank you for being in my life and believe in me, encourage me and always make me feel strong. This achievement belongs to you for the nights that you spend sitting close to me. My life would not be the same if you were not beside me.

My Dad, Dimo, who spends his whole life for his children and he taught me that education is the key for a happier life. My Mum, Despoina, for being present and trying to strengthen my self-confidence in each step of my life. My brother, Thodori, for his visits to Delft and the nice time that we spent together.

Last but not least, I want to thank all my new friends, Dimo, Grace, Sokratis and Philipp, whom I met here and with whom we created new memories. Also to those that I left in Greece, Sophie and Dionysis, I will meet them soon.

Eleni Tzanakou

Table of Content

Table of Figures

SUMMARY

Nowadays, the main goal of Energy World Council (2016) is to provide an affordable and stable energy system for the highest benefit of all people. These goals could be achieved by using the Information and Communication Technology (ICT). The continuous digitalization of energy sector with the implementation of ICT technologies in Smart Grid and also the use of smart devices such as smart meter, which are interconnected by Internet, result to both advantages and disadvantages. By using the new technologies the functional efficiency of the Smart Grid is increased but at the same time leads to a more vulnerable system and makes the Smart Grid a potential target for cyber-attacks. In fact, cyber-attacks are becoming one of the most serious threats in critical infrastructures. More than 80% of energy companies dealt with a growth in the incidents of successful cyber-attacks in 2015 (Herring, 2016). These facts show the importance of investigating the impacts caused by cyber-attacks on the system, and the need for a systematic way to assess it. Here it is essential to highlight that investigating the impacts in design phase of the system, could result in a more secure system against cyber-attacks.

In order to gain insights into the degree of influence of cyber-attacks regarding the energy prices and the power demand, the research objective of this thesis is to shed light on the impact of two types of cyber-attacks, targeting the signals along the communication link, on the normal behavior of the system and their indirect influence on the behavior of consumers and utilities, when a price based Demand Response (DR) program is used. This research is important in order to deal with the increasing growth of cyber-attack incidents in smart grid. The approach that is followed to investigate the research problem consists of several parts.

The research methodology is as follows. At the beginning, Smart Grid as a system and the DR programs that are implemented on it are described in details. Later, as critical infrastructure, Smart Grid's security objectives that should be retained secure and not violated from cyber-attacks are elaborated to see the most crucial that should be taken into account in this thesis. Based on the gained knowledge of this part, a classification of the attacks based on the most important objectives takes place. The results show that availability is one of the main objectives, as it is vital for the consumers and utilities to have available up-to-date information without delays. At the same time, it is essential to ensure the integrity of data regarding the energy consumption and the prices that are transferred through the system. Next, by combining the impact assessment model published by Federal Information Processing Standards (2004) and the failures scenarios of NESCOR (2015), the possible impact of cyber-attacks is defined in a more conceptual and qualitative way.

In the next part, agent-based simulation is used to model the communication between utility and consumers regarding the Demand Response program (Real Time Pricing mechanism (RTP) in particular) as well as the intrusion of an attacker into the communication. The inputs of the model include standard energy demand patterns per household type, attack type, duration of attack, number of consumers and number of affected consumers. In order to simulate the RTP mechanism into the system, a distributed algorithm, that finds the optimal energy consumption for the consumers, the optimal price values that the utility server communicates and the optimal generating capacity for the utility server, is used. Default consumer profiles are generated based

on synthetic profiles and the annual energy demand by household type. Attacks are modeled based on attack type, duration and time of occurrence, disrupting the stable state of the RTP mechanism. The emergent behavior from the hourly interaction between utility and consumers and also the interference of the attacks serve as an illustration of the implications of cyber-attacks on the DR program.

Finally, the insights from the literature but also the findings from a set of well-designed experiments are combined in order to understand the implications of cyber-attacks in the priced based program of DR. Results from the thesis conclude that a man-in-the-middle (MITM) attack can have severe impact on the price signal. Consumers receive false price signals from the utility and their decisions are based on wrong information. This leads to an increase of energy consumption for the affected consumers during the peak hour as well as the decrease of energy consumption for non-affected consumers that react to the higher prices. Additionally, a Denial of Service (DoS) attacks results to no transmitted price on the system. Even though, there is no apparent solution when no price signals are available, the model is constructed based on the mitigation solution where the consumers are able to use the previous received price and schedule their demand based on that. This choice is taken in order to retain a value that is closer to the subsequent not transmitted signals. Because the price is updated in hourly basis the attack has low impact if it has small duration or it does not take place during high peak hour.

Moreover, during the development of the model, rational decision-making process is followed for behavior of the consumers, which means that they make choices that maximize their benefits and minimize any cost for them. Thus, any other incentives for the consumers are not taken into account in this research. One main suggestion for further research could be to extend our model in order to give to consumers more incentives except from the cost, which can influence their energy consumption, such as the use of eco-friendly appliances, which will contribute not only to the reduction of their bills but also, to protection of the environment. This could be implemented by adding additional component in the model (i.e. smart appliances) which will influence the total amount of demand and the load will be better defined. Finally, the contribution of this thesis could be useful for designing mechanisms on how to protect the system from the data manipulation (man-in the middle attack) and the availability of DR resources (DoS attack) in communication network.

1 INTRODUCTION

In the first part of this chapter, the research problem in the subject area Smart Grid cyber security is introduced. The research gap is presented, based on a thorough literature review. In the second, part of the introduction, research objective, research questions and methodology are formulated.

1.1 Smart Grid Cyber security – Research problem

A Smart Grid comprises of an automated, decentralized network characterized by two-way flows of electricity and information. The system is aimed at optimizing the balance of supply and demand in real-time by the use of advanced technology capable of measuring, controlling, monitoring and delivering (electrical) energy. Even though Smart Grids are an improvement compared to the traditional electric grid, it is also a more vulnerable system(Wang & Lu, 2013). Cyber-security threats pose a significant and growing challenge, because Smart Grids depend fundamentally on Information and Communication Technology (ICT) infrastructures, (Sgouras, Birda, & Labridis, 2014). In Smart Grids, several vulnerabilities exist, which could lead to undesired situations up to complete system failures. These vulnerabilities include but are not limited to:

(1) Access to sensitive personal and business information collected from smart meters and other smart gird devices (Clements & Kirkham, 2010; Pearson, 2011)
(2) Hazardous cyber-attacks on critical system components through entry points of artificial intelligent components of Smart Grids (Pearson, 2011),
(3) Exploitation of vulnerabilities of communications among components of control system for data spoofing (manipulation) (Clements & Kirkham, 2010),
(4) Internet Protocol (IP) spoofing on internet-enabled devices and the use of Denial of Service (DoS) attacks, where the objective is to overload target with massive volume of traffic to take them down (Ghansah, 2009),
(5) Cyber-attacks that physically damage critical infrastructure (Clements & Kirkham, 2010).

It is of outmost importance to tackle these security issues and secure the reliability, availability and integrity of Smart Grids, since it is a critical infrastructure and a possible failure in the system may have negative effects for the society.

1.1.1 Security concerns

Since the communication between components of Smart Grids is based on ICT (**Figure 1**), Smart Grids are inevitably vulnerable to cyber threats. A Demand Response (DR) system under attack is illustrated in **Figure 2**. An adversary agent performs a Denial-of-Service (DoS) attack on the server, making it unavailable to further request processing. It is also possible for the adversary to attack the communications between meters and server. These attacks impact the energy prices and demand load of the system, since the server is incapable of updating properly the customers with the changes of the energy price. **Figure 3** indicates the hypothesized influence of an attack on load curves in a high peak period of a day. Since the meters are not aware of any price updates, users do not receive information to reduce their energy demand during high peak periods, and the load may shift towards that point.

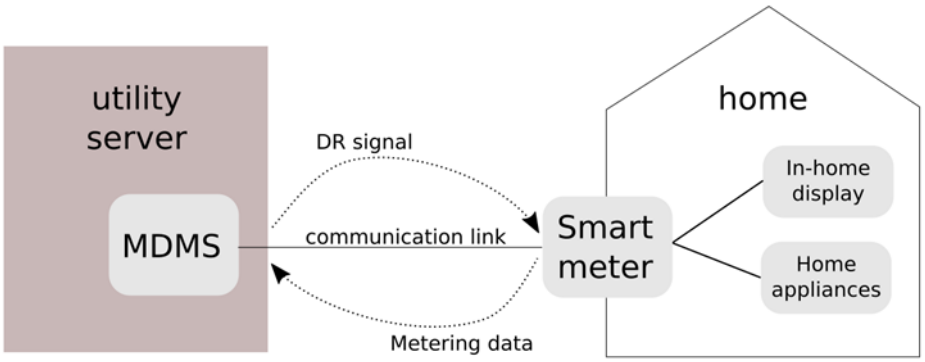

Figure 1 *Information flow in the smart grid. Smart meters send metering data to MDMS and receive DR signals (Bhatt et al., 2014).*

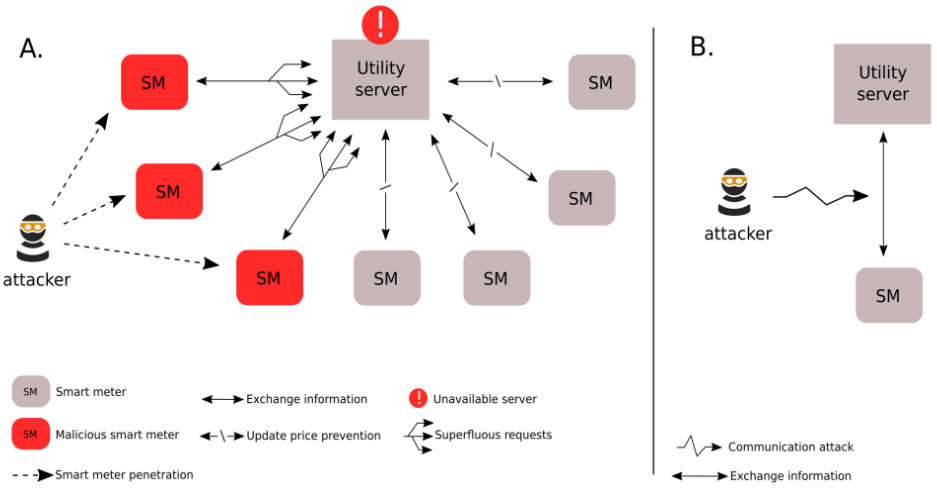

Figure 2 *Illustration of Demand response system under attack.* ***A.*** *DoS attack on the server. Multiple smart meters are affected by the attacker and send superfluous requests to the server resulting in its unavailability.* ***B.*** *Attack in the communication link between server and smart meter. This may lead to the manipulation of the transferred data.*

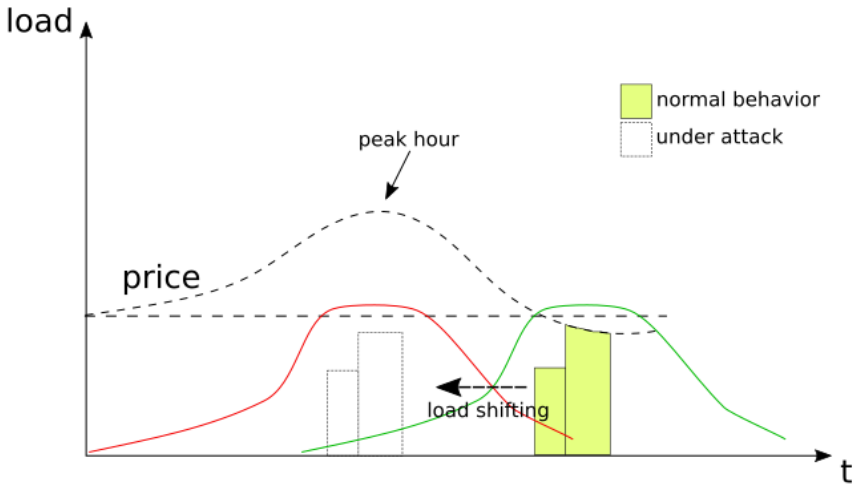

Figure 3 *A load curve shift when the DR is under attack (own illustration)*

The focus of this thesis is on the information that the customer receives about the energy prices, for cases in which dynamic pricing programs are in place. Because the pricing information is transferred electronically and many participants have access to this information the integrity of the pricing signal should be maintained and protected from illegal manipulation of adversaries (Wang & Lu, 2013). Further, DR functions should assure information integrity and availability (California Energy Commission, 2014; Wang & Lu, 2013) since attacks can also result in manipulation of the information with various implications for both customers and utilities, and for the outcome of DR (Wang & Lu, 2013).

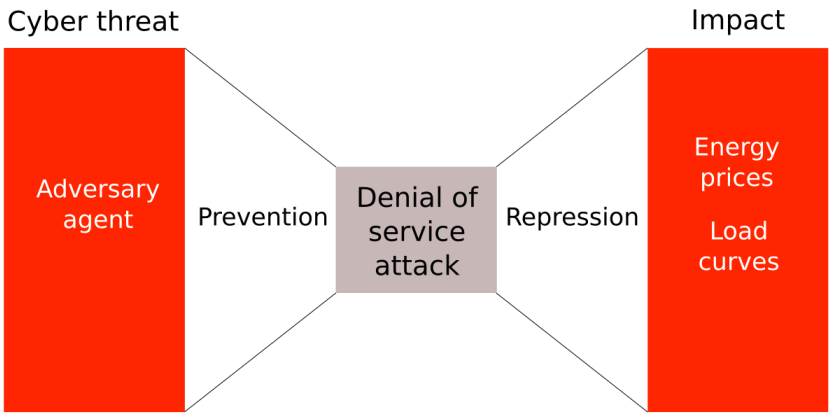

Figure 4 *Bow-tie diagram for a potential Denial of service (DoS) attack.*

Therefore, it is essential to investigate how cyber threats can reflect on Demand Response functionality and change its outcomes. Figure 4 shows a bow-tie diagram. Hazardous events, e.g. DoS attacks, which are triggered by adversary agents, can modify and affect the energy prices and load curves. The Smart Grid should be capable to prevent an attack by using specific control measures. Moreover, if an attack happens, the system should quickly recover in order to minimize its impact.

1.1.2 Research gap

Plenty of studies have focused on the basic behavior of the consumers and utilities in the DR. Douw et al. (2016) constructed an Agent Based Model (ABM) to examine how different price scenarios influence consumers' behavior. More specifically, the authors modeled both individuals' and social behavior to investigate the incentives that lead to better electricity consumption choices. In a master of science thesis, (Mahalingam, 2013) investigated how the different DR price-based policies could maximize the benefits for the consumers and the system in the context of the day-ahead electricity markets, specifically in the Netherlands. These studies found that the activation of DR pricing-based mechanisms affect the basic behavior of consumers and utilities in a good manner (Mahalingam, 2013). Most of the literature focused only on how the end-users/consumers could benefit by the DR pricing programs combining the technical network (electricity model) and the social network (behavioral model of "friends") (Worm, Langley, & Becker, 2015). However, none of these approaches has taken into consideration how an adversarial agent will affect and may change the outcomes of DR. Therefore, there is a need to extend existing models with an adversary agent in order to investigate what could happen if an attacker modified the pricing signals transmitted to a set of smart meters, and to investigate how this attack would affect the DR energy prices and the power demand. This research gap is made explicit below.

Research gap: Even though the available literature to some extent analyzed the DR pricing mechanisms as an important factor that influences consumers' energy consumption, it does not give any insights on how different types of cyber-attacks can influence indirectly the consumers' behavior and the price signals sent to the non-compromised devices.

1.2 Research definition

In the following section, the identified research gap is translated into a clear and specific research design. First, the research objective is described. Second, the main research question and sub-questions are proposed to accomplish this research objective. Third, the research methods are specified. Finally, the scientific and practical contribution of this research is made explicit, and the structure of this document is laid out.

1.2.1 Research Object and Scope

Given the information described above, the main research objective of this project is to investigate how and in what scale different types of cyber-attacks reflect on the outcomes of DR regarding the energy prices and the power demand and how the consumers' and utilities' behaviors are influenced.

Because existing research addressing this particular aim is rather limited, the scope of this research is *exploratory*. First, a baseline scenario without attack is analyzed, then several scenarios of the system under attack are investigated and the impact of cyber-attacks on the DR is assessed by comparing the model outcomes.

1.2.2 Research question

The main research question for this research was formulated as follows:

"What are the implications of integrity and availability cyber-attacks to price signal on DR programs and subsequently how does this affect the power demand in the Smart Grid?"

To answer this research question, the following three sub-questions are formulated and each of them involves several research steps.

1. *"What is the effect of different types of cyber-attacks in the received price signal of the Real Time pricing (RTP) program?"*
   DOS attacks:
   The effect of a DoS attack on the price signal is indirect. The target of a DoS attack is the server, which becomes unavailable during the attack. This unavailability leads to disruption of the resource access and violation of the timing requirements of critical message exchange. An attack during off-peak hours may result in delay of information exchange between consumers and server (mild impact). However, during peak hours a DoS attack may result into corruption of the system (severe impact), since the main objective of DR system on peak hours is to ensure the reliability of Smart Grid operation by signaling higher prices to consumers, in order to reduce their electricity consumption. If the consumers are not informed about the price changes during a critical time, then the system may exceed its limit and be corrupted.

   Man in the middle attack:
   One of the aims of this type of attack is to modify critical information. More specifically, the attacker gains access to information being exchanged and then manipulate pricing information transferred from the server to the consumers.

2. *"What is the impact of cyber attacks on consumers' energy consumption during peak hours when using the RTP program?"*
   During peak hours, the energy consumption is higher than other periods of the day. So, the consumers benefit by using DR programs and specifically RTP. By receiving a new price several times throughout the day (e.g. every hour) they are able to alter their consumption. This may affect the reduction of the energy consumption in peak hours. In case of cyber attack incident, as above-mentioned the consumers are not correctly informed about the new prices to change their energy consumption to off-peak hours. This may lead to higher electricity bills and extra costs.

3. *"How do different magnitudes of an integrity attack affect the received price and the power demand?"*
   Man-in-the-middle attack may affect a fraction of households in the Smart Grid. Different scales of such attacks may have different effect on the price signal as well as the energy consumption not only for the affected households but also for the non-affected directly by the attack.

1.2.3 Research methodology

In this research two main methods are applied in order to answer the research question and the sub questions and to gain insights to fill the research gap. The research methods that used to answer the aforementioned

research question and its sub-questions are explained in this section. The Figure 5 presents a flowchart of this research. Then, table 1 depicts the research methods used for answering each research sub-question.

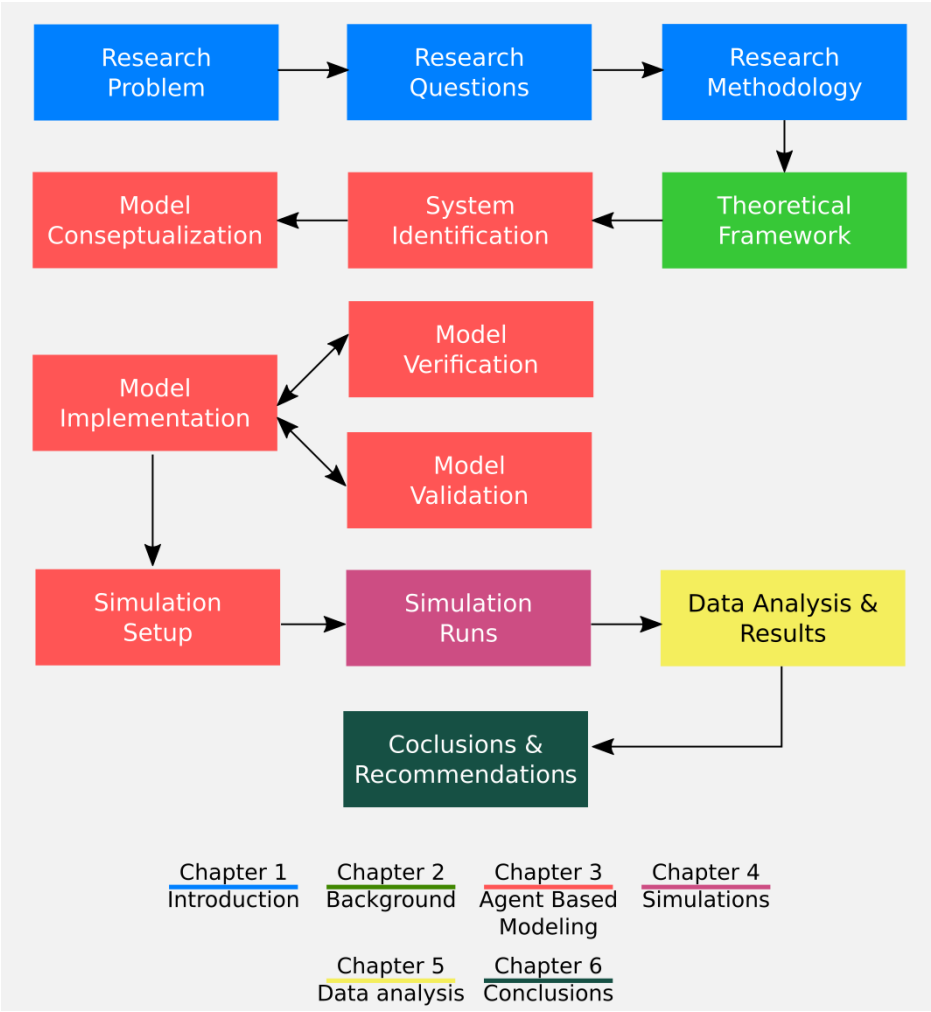

Figure 5 *Flowchart of thesis' structure*

First, two systematic literature reviews were conducted in this study that were aligned with the scope of the research. The first review was aimed to improve the researcher's understanding of the problem situation and to enable the selection of the method to develop the model. After that, the second review formed the basis for selecting the specific types of cyber-attacks to be used in the model and studying how the DR programs may be affected by the attack on theoretical level. The literature for both reviews was retrieved by means of systematic searches of keywords in the engine Scopus and Google Scholar, such as Smart Grid, demand response, cyber security, cyber attacks, communication technologies, etc..

The second method that was used in order to answer the research question of this thesis was the development of an Agent Based Model (ABM). A definition for the ABM is the following: "*Situate an initial population of autonomous heterogeneous agents in a relevant spatial environment; allow them to interact according to simple local rules, and thereby generate – or 'grow' – the macroscopic regularity from the bottom up.*" (Epstein & Seely, 2006). This method of computational modeling was chosen to explore different system behavior and scenarios in an iterative process. The main limitation regarding the simulation model is that because most of the data regarding DR programs and

the potential cyber-attacks and their consequences are private. So, we made some assumptions, which did not influence the validity of the simulation model.

Why Agent Based model?

Seven aspects that make ABM unique according to Lättilä, Hilletofth, & Lin (2010):

1. It studies individual agents and therefore, system heterogeneity
2. Its unit of analysis are agents' rules
3. Its central mechanism is emergent behavior
4. Its main components are agents, rules and interactions
5. System structure can change during the simulation run
6. It aims for exploratory analysis
7. AB models can handle both discrete and continuous time, the latter at the cost of high demand for computational capacity

Sub-questions	Literature review	Simulation model
What is the effect of different kinds of cyber-attacks in the received price signal of the RTP program?	✔	✔
What is the impact of cyber attacks on consumers' energy consumption during peak hours when using the RTP program?		✔
How different scales of an integrity attack affect the received price and the power demand?		✔

Table 1 *List of the research sub-questions that are answered using one or more research methods. Apparently, ticks indicate which method answers the questions.*

1.2.4 Scientific and practical contribution

The scientific contribution of this thesis is that we explore and analyze the behavior of DR program of Smart Grid infrastructure under certain conditions. More specifically, we analyze the impact of cyber-attack on DR. We focus on the communication of price signals and energy consumption in DR programs. Several cyber-attack scenarios on DR take place in order to analyze their impact on the outcome of DR and the other entities of the system. For the analysis of the behavior of the several entities, we design an Agent Based Model (ABM). This model is based on a baseline scenario with normal operating conditions. Adversary agents are carefully designed that disrupt the system. The innovative design of this factor is beneficial for the proper development of the future infrastructures. It indicates the impact of potential cyber-attacks and it helps to prioritize the security aspects more accurately.

In practice, attacks have caused a series of problems such as economic losses, loss of load, even blackouts in electricity grid (Bhatt, Shah, & Jani, 2014). The design and the development of the communication unit of Smart Grid infrastructure are based on existing networking protocols. Inevitably, cyber-attacks come into the play. The proposed simulation model provides an effective and efficient tool to gain insights about the impact of these cyber-attacks in the DR system. It can be extended and applied in different conditions for other types of attacks or other price mechanisms in DR.

1.3 Thesis structure

This thesis is structured as follows: **Chapter 1**, introduction, describes the domain area and specific research problem. Further, the research questions that will be addressed are formulated and the methodology that was adopted to answer the research question is depicted. The remaining parts of this thesis are organized as follows. **Chapter 2** further elaborated on the DR approach, with a brief introduction of the main concept and the various types of DR options that are relevant. In addition, the concept of cyber security of Smart Grids and its objectives are explained in greater detail in and the different types of cyber-attacks and security issues described. In **Chapter 3,** we provide a detailed system description, which serves as the basis of the computational model, as well as the main aspects of the agent based model and the process of modeling the problem is descripted. In **Chapter 4**, the results of the analysis from the different modeling experiments and the impacts of these results are examined. Finally, in **Chapter 5** conclusions and recommendations for decision-makers are given based on the results and findings from the analysis. Last, in **Chapter 6** suggestions for future research are set out.

2 THEORETICAL FRAMEWORK

In this chapter, the concept of the Smart Grid and its characteristics are introduced. After that, the Demand Side Management (DSM) and its connection with the Demand Response (DR) are explained. Further, DR programs in the context of the Smart Grid are explained and price-based programs are described.

2.1 Smart Grid

At this point the current electricity grid no longer meets the requirements of the growing demand for energy, and lacks of effective integration of renewable sources (Mwasilu, Justo, Kim, Do, & Jung, 2014). At the same time, the need for increasing network control and communication requirements created the need for a more 'intelligent' redesign of the electrical network of the 21st century (Gungor et al., 2013). To face these new challenges, the concept of the Smart Grid has been developed.

The Smart Grid is considered a fundamental infrastructure for humankind and modern society with the potential to replace the current electricity grid (Flick & Morehouse, 2011). It consists of a more robust, efficient and flexible modernization of the existing power system, and has been defined as "*an electricity network which includes various features of operational and energy measures consisting of smart appliances, smart meters, renewable energy resources, and energy efficiency resources*" (Federal Energy Regulatory Commission, 2008).

Technically speaking, a Smart Grid is a complex system. It allows multi-directional power flow and exchange of information (Gungor, Lu, & Hancke, 2010). It uses communication and information technologies (ICT) to support monitoring and decision making software tools that enable the optimal transmission and distribution of electric power from utility to consumers (Wang & Lu, 2013). It depends on ICT-enabled devices (e.g. smart meter) and ICT infrastructures (e.g. Advanced Metering Infrastructure) since its components need to communicate between each other and with the utility (Wang & Lu, 2013).

Figure 6 (next page) illustrates a basic conceptual model of the Smart Grid. This figure exemplifies how technologies of communication and information will play a central role in all the different stages from production to consumption (giving the opportunity to the consumer to participate in production as prosumer), ensuring sustainability and quality services, distributed electricity production, processing information locally, storing the produced energy and smart measuring of consumption.

In the design of Smart Grids, the following objectives needs to be taken into consideration (U.S. Department of Commerce, 2010):

1. Reliability and quality of service (through the adoption of a distributed electricity model).
2. Use of the existing infrastructure in a conservative way and introduction of renewable resources in order to reduce the environmental pollution and at the same time to meet the power demand.
3. Flexible design that allows the system to self-healing in case of a serious damage.
4. Active involvement of consumers in a try to save energy (through demand response programs and dynamic billing, in which the price of the kWh depending on the specific time of a day)

5. Ability to more accurate forecasting of demand by received data from smart meters

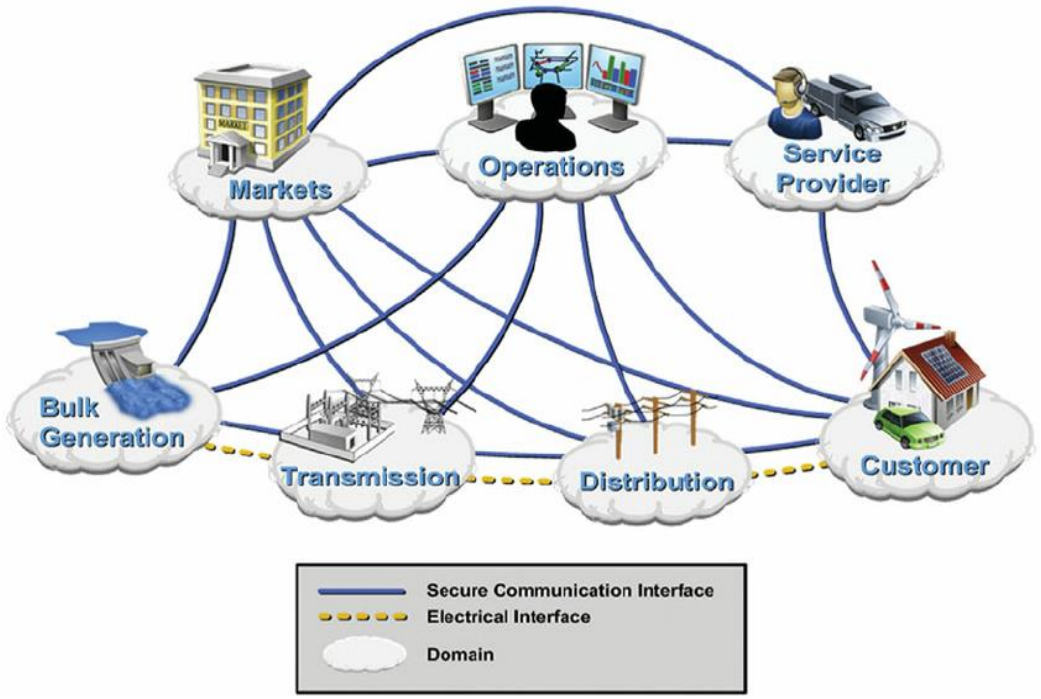

Figure 6: *NIST conceptual model for SG (Fang, Misra, Xue, & Yang, 2012)*

2.1.1 Characteristics of Smart Grid

The Smart Grid introduces a completely new, communication network between energy suppliers and consumers. With automated decision making the balance in the grid between demand and supply is constantly maintained. This allows the collection and analysis of data at each level in real time and helps in production and demand balance. The various applications of Smart Grid communication technology and their services are summarized in the table 2 below (Bhatt et al., 2014)

Smart Grid applications	Key Services
Advanced metering infrastructure (AMI)	Interval measurement Load control Pre-payment Tariff flexibility Communication and data security
Home automation network (HAN)	Local/remote control of devices Overall consumer load management Energy efficiency
Demand response (DR)	Load adjustment Dynamic pricing
Supervisory control and data acquisition (SCADA)	Automated control of transmission and distribution

system	Substation automation

Table 2 *Smart Grid applications and their key services (Bhatt et al., 2014)*

2.1.2 Smart meters

The smart meter is a main component of the Smart Grid. It is a device that records consumption periodically and communicates that information back to the utility for monitoring and billing. An essential application of smart meters that is beneficial for the consumers and the utility companies is the real time pricing. Smart meters are able to measure and monitor the electricity consumption and to address the data on both consumers and utilities by providing statistical data in different programmed time periods. This information is more precise than the data of manual meter reading.

Through the use of smart meters, utility companies could offer lower prices of electricity during off-peak hours, and incentivize users to adjust their energy consumption on peak hours correspondingly. This, in turn, would provide utility companies with the opportunity to plan a more sophisticated energy production, since smart meters provide a digital representation of the fluctuations in demand (Kalogridis, Efthymiou, Denic, Lewis, & Cepeda, 2010).

By this time, many countries have successfully implemented smart meters. In France, more than 90% of the electricity consumers have smart meters installed. Utility companies are obligated by the German government to provide consumers with time-of-use prices, since 2011. In Norway, users that consume above 100,000 units are required to deploy smart meters with hourly recording. In the UK, it has been decided to deploy smart meters in households until 2020. Till 2014, almost half of the US residential consumers had installed smart meters. Nowadays, more than 50 million smart meters have been deployed (Deconinck, Delvaux, De Craemer, Qui, & Belmans, 2017).

2.1.3 Advanced Metering Infrastructure (AMI)

Advanced Metering Infrastructure (AMI) provides a flexible, secure and more automated network infrastructure. It consists of two-way communications with smart meters, consumers, data collection bases and management systems. AMI gives the opportunity to consumers to reduce their energy consumption and pay lower electricity bills and to the utilities to operate a more robust electricity system. More specifically, the two-way communication channels allow interval data flow from smart meters to Meter Data Management Systems (MDMSs) about dynamic pricing and demand response programs (see next subsection). MDMSs store and manage smart meters' data aiming at providing useful information for billing and analysis (Cleveland, 2008; Wang & Lu, 2013).

2.2 Demand Response

Demand Side Management (DSM) is a mechanism that includes the planned and implemented activities that aim to balance demand with supply by influencing consumers to change consumption (Gelazanskas & Gamage, 2014; Gellings, 1985). There are two DSM schemes (Palensky & Dietrich, 2011); Demand Response (DR) and Energy Response (ER) as depicted in Figure 6. In this project, we focus on DR programs. According to the Federal Energy Regulatory Commission (2008), Demand Response is "*an action taken to reduce electricity demand in response to price, monetary incentives, or utility directives so as to maintain reliable electric services or avoid high electricity prices.*"

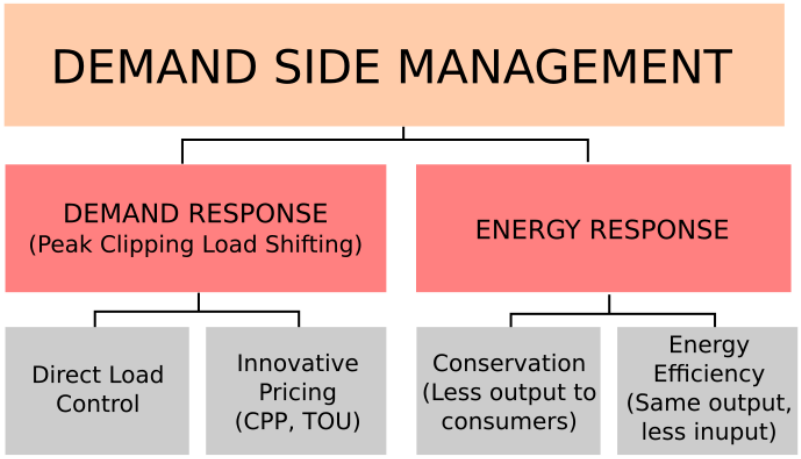

Figure 7 *Demand Side Management schemes.*

The Figure 7 shows the various ways that each consumer can adjust his electricity consumption applying the demand management measures (Mahalingam, 2013). The impact on load shape is described in the following lines. The horizontal axis represents the time during a day (0.00-23.59), whereas the level of demand is given on the vertical axis.

Peak Clipping: refers to the reduction of the electricity consumption during the peak hours. As a result, when the load declines, the demand follows the same behavior in peak hours.

Valley Filling: The load increases during off-peak periods to eliminate the large differences between on-peak and off-peak hours, which in turn improves the system load factor, i.e. the ratio between peak and minimum loads.

Load Shifting: combines the advantages of the peak clipping and the valley shifting by shifting the existing load from peak to off-peak periods, which means from high energy price periods to low ones. Also, the customer may postpone some high demand activities during the peak hours and gain economic benefits by buying cheaper electricity.

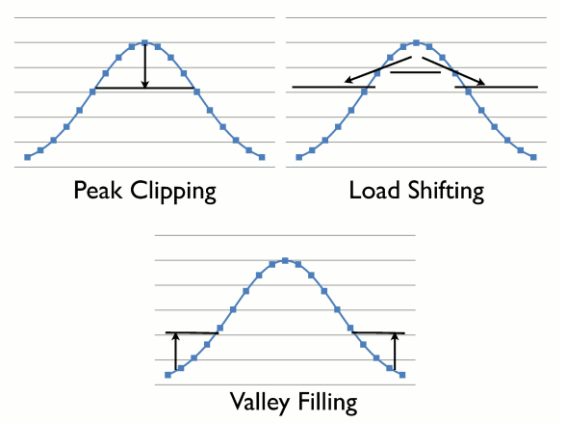

Figure 8 *Load shape impact of Demand response (Gellings, 1985)*

More specifically, DR programs and tariffs contribute to the reduction of the energy use during the peak hours as well as on specific high energy price events (i.e. congestion and market conditions that increase the energy costs) (California Energy Commission, 2014), which leads to lower costs and electricity loads. DR is about keeping the same amount of the total consumption, but shifting it to another specific time. Its main purpose is to properly inform consumers about the energy price in order for them to be able to react on events regarding the change of electricity price and to gain more economic benefits (Gelazanskas & Gamage, 2014).

2.2.1 DR programs

The applied DR programs are divided in two main categories, the price-based DR and the incentive-based DR (Albadi & El-Saadany, 2007; Wissner, 2011), each of them has its own subcategories (Figure 9). The price-based DR refers to changes that consumers make regarding modifications on the price of electricity, which include real time pricing, critical peak pricing and time of use pricing (Albadi & El-Saadany, 2007). If the billing divergence between periods of use is significant, consumers may compromise with the existing pricing system but also may change radically the way they use electricity in order to decrease the cost. This can be achieved by taking advantage of the off-peak periods and/or consuming less during the on-peak periods (Gelazanskas & Gamage, 2014). All the changes on electricity usage level made by the consumers are completely voluntary.

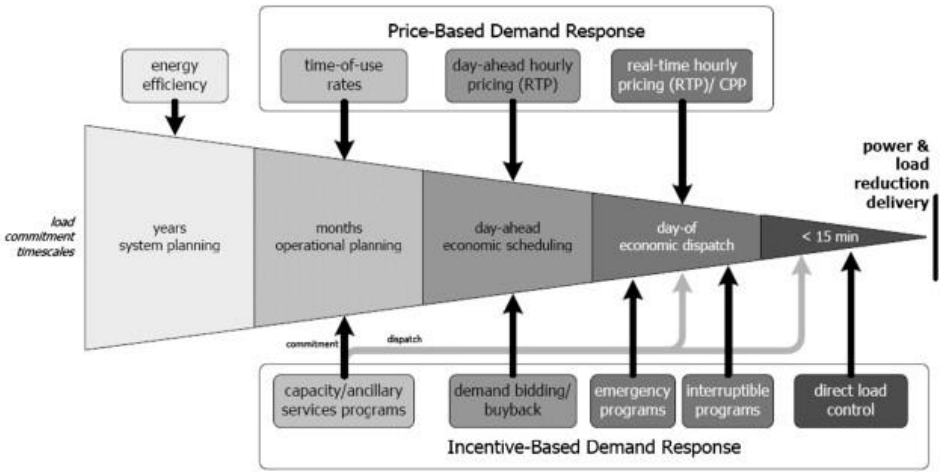

Figure 9 *Programs of demand response in the electricity system by time scale (Wissner, 2011).*

Price-based programs

- Time-of-use (TOU): It is based on fixed prices on different seasonal or daily intervals. These intervals could be days in year, days in week, and months in year and hours in a day. Generally, the costs for electricity consumption are high on high electricity demand intervals whereas on lower electricity demand intervals the costs are lower. This condition motivates consumers to shift their loads to lower demand intervals in order to benefit from the lower prices.

- Critical Peak Prices (CPP): It is a relatively newer version of TOU pricing in which the prices for peak hours replaced with much higher. A CPP event is signaled under specified trigger conditions, such as unexpected situations in the network, compromising system reliability and extremely high electricity costs.

- Real Time Pricing (RTP): RTP program reflects better the market price of electricity. It is a flexible pricing program in which the price of electricity fluctuates in small intervals (typically every hour) influencing the wholesale price of electricity. The price that the customer is required to pay is the market clearing prices with some extra fees depending on the market that customer belongs to (intra-day or the day-ahead markets). Customers are not informed about the real time prices in advance and they should respond immediately in the price signals that received about the price changes day or hour after. As a result, in this program the customers are not protected by the price fluctuations.

- Critical peak rebate (CPR): Consumers are rewarded according to the reduction of the electricity consumption in high demand periods. This is a new program, which is in essence the inverse of the CPP method.

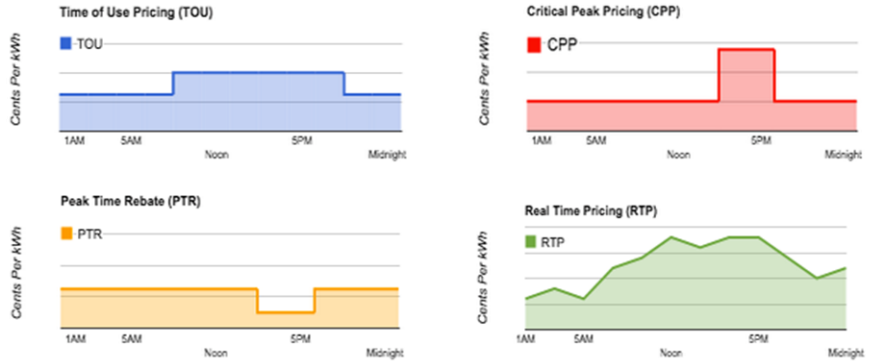

Figure 10 *Price-based DR programs*

Incentive-based DR programs provide financial incentives to consumers, in order to help with their load reduction. Load reduction may be necessary in cases, where the system's stability is in danger or pricing is very high. Some DR programs include penalties for customers that participate, but fail to comply with their contracts with the company.

Even though, Smart Grid applications facilitate the improvement of Smart Grid in terms of reliability, efficiency, and security, it may lead to new vulnerabilities and security issues (Hull, Khurana, Markham, & Staggs, 2012; Wang & Lu, 2013). The concepts of cyber security and main security objectives in Smart Grids are explained further in the next chapter.

2.3 Cyber security of Smart Grids

The integration of new technologies in the Smart Grid and their rapid spread, particularly those related to the Internet, might introduce new threats to the security of the Smart Grid (Chambers & Gravely, 2012). The advanced technologies offer significant advantages and opportunities, but at the same time increase significantly the problems related to the protection and availability of information into the system. Cyber-attacks may take advantage of accessibility via communication network, trying to gain remote access and compromise or control various electronic devices or vital components of the Smart Grid (Hull et al., 2012).

Cyber security objectives

The existence of security in every form of network is crucial since it may carry personal or confidential data. The security objectives, that Smart Grids should fulfill, in order to safeguard against threats vary. With the aim to keep Smart Grid in a secure manner it is important to understand the security objectives. Following there are three fundamental and most well document security objectives and two secondary objectives. For the aim of this thesis, we will focus in availability and integrity (Hull et al., 2012)

Fundamental Objective 1: Confidentiality

Data confidentiality is the property that ensures that only authorized users have access to sensitive information. In other words, unauthenticated users are prevented to access confidential information. In a Smart Grid infrastructure, data confidentiality refers to privacy of customer information, critical enterprises information, and electric market data. One usual method to achieve confidentiality is encryption. However, in some cases data aggregation coupled with differential privacy suit better regarding data confidentiality.

Fundamental Objective 2: Integrity

Data integrity is the property that ensures that there is no unauthorized modification to data and information. The recipient of a package should be sure that no third person is able to alter the packet data without being detected. Integrity for Smart Grids applies to information such as sensor values and control commands. A lack of integrity leads to disinformation which may cause security problems and may disrupt the operation of the Smart Grid.

Fundamental Objective 3: Availability

Availability of data is the property that ensures that services and information offered through the network are constantly available to authorized users. For Smart Grids, this relates to all cyber components of the grid, for instance SCADA systems. A loss of availability may result in both security problems and economics losses. In Smart Grid, the real-time systems have an expected maximum delay of some msec. These systems constantly monitor the electricity network and a breakdown in the communications can cause power loss.

Secondary Objective 1: Authorization

Authorization is a property that ensures the rights of each user in the Smart Grid and defines that any user will not be able to have access to levels beyond its own rights. A loss of authorization may result in both security and privacy problems. Therefore, only authorized users should use the computer system or peripheral devices and only in accordance with a predetermined way.

Secondary Objective 2: Authentication

Authentication is a property that certificates that a user in the system is actually the one that claims to be and that a message that the system sent by this, indeed sent it by this and no one else.

The previous security objectives should play an important role when a cyber-security framework is designed, because in its step should provide ways to ensure their existence.

Cyber security management frameworks

There are many frameworks (e.g. ISO31000, ISO27005, NIST cyber security framework etc.) to study and improve cyber security. In the paper "Cyber-Physical System Security for the Electric Power Grid" the risk methodology of Figure 10 is proposed. This methodology aims to show explicitly the connection between the control functions of the physical power system and the cyber infrastructures (e.g. communication links etc.) and to recognize the physical impact of cyber-attacks.

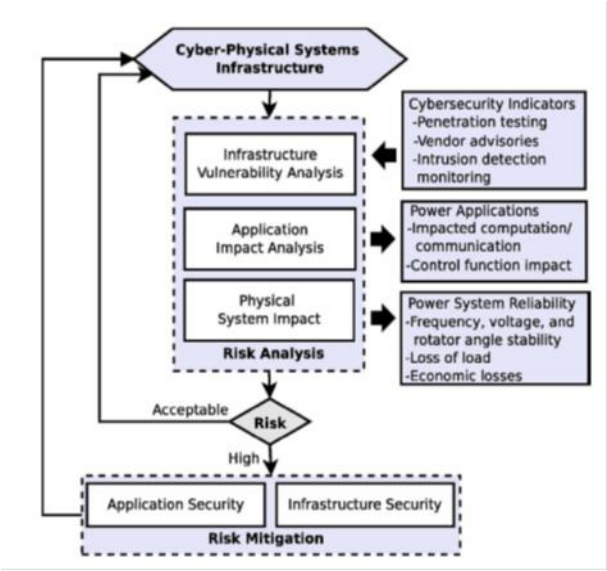

Figure 11 *Risk assessment methodology (Sridhar, Hahn, & Govindarasu, 2012)*

According to the authors (Sridhar et al., 2012), the risk reduction measures can be divided into two main parts, risk analysis and risk mitigation. For the aim of this thesis, we will focus on the first part. At first, each risk is defined by the probability of an event to occur multiplied by the resulting impact. This probability is applied in the infrastructure vulnerability analysis step, which addresses the ability of the cyber infrastructures to reduce the attacker's penetration into the control functions of the physical power system. The next step is the application impact analysis. In this step, the possible impacts of attacks, which are caused by the exploitation of the previous vulnerabilities, are examined and the affected control functions and/or communication links are determined (Sridhar et al., 2012). After receiving the appropriate information about the impact of the attacks, the physical system impact step takes place to evaluate and quantify the impact, such as loss of load, economic losses etc., in the power system through simulation methods, more specifically this thesis focuses on the impact assessment.

The main idea of this thesis is based on the following statement of the authors. An attacker is able to take advantage of the existing vulnerabilities along the communication links and launch attacks to the control signal along the links, by either jamming the transferred data (e.g., integrity attacks), or introducing a delay or denial in the communication (e.g., denial of service (DoS), timing attacks)(Sridhar et al., 2012). It is essential to examine and investigate impacts of such attacks on the system as they could undesirably affect its availability and integrity, as two of the main security objectives (Chambers & Gravely, 2012).

2.4 Attack classification based on the fundamental security objectives

As a critical infrastructure, the Smart Grid is expected to be an attractive target for malicious attacks. A Smart Grid is characterized by an increasing number of security issues mostly caused by cyber attackers via the communication network. The ultimate goal of these attacks is to cause calamitous damage to power supplies and individual devices and widespread blackouts, which is strictly prohibited in Smart Grid (Sgouras et al., 2014).

Started in 2004, Hacker's Profiling Project (HPP) (Chiesa, 2010) is an attempt to identify the hacker's profiling. Although, the term "hacker" does not necessarily indicate harmful behavior (e.g. hackers protecting data and testing security on a system), in this report "hacker" and "attacker" are used interchangeably for the sake of simplicity because the majority of hackers have deleterious behavior. The ultimate goal of HPP is to analyze the phenomenon of hacking. They want to understand the different motivations and incentives of hackers and to observe real criminal actions. They also apply their profiling approaches to the collected data and learn and distribute useful knowledge regarding hacking and cyber attacks to the public. In table 3, the detailed categorization for the different types of hackers as described by the initiators of this project is depicted.

	Description	**Lonely or Group member**	**Target**	**Motivations**
Wannabe Lamer	9-18 Years Old "wannabe a hacker but are not able to"	Group	Final Users	For Fashion
Script Kiddie	10-18 Years Old, Script Kid	Group	PMI with unknown vulnerabilities	To discharge anger and attract attention
Cracker	17-30 Years Old, The destroyer	Lonely	Private corporations	To show power and attract attention
Ethical Hacker	15-50 Years Old, hacker per excellence	Lonely (in a group for fun/research)	Big Firms, complex systems, whereever there is a challenge	For curiosity to learn improve the world
Quiet, paranoid, Skilled Hacker	16-40 Years Old, tacturnm paranoid and specialized hacker	Lonely	According to necessity	For curiosity to learn, for egoism or specific motivations.
Cyber Warrior	18-50 Years Old The mercenary	Lonely	Symbolic corporations & organizations, final user	For Profit
Industrail Spy	22-45 Years Old, The Industrial Spy	Lonely	Business companies, multinational	For Profit

			corporations	
Government Agent	25-45 Years Old, The Government Agent (CIA, Mossad, FBI etc)	Lonely or in a group	Governments, terrorist suspects, strategic companies, individuals	As a Job (espionage/ counterespionage/ activity monitoring)
Military Hacker	25-45 Years Old, Enlisted to fight "with a computer"	Lonely or Group Member	Governments, Strategic Companies	As a job or for a cause (action to control / damage systems)

Table 3 *Classification of hackers* (Chiesa, 2010)

The previous table is an extensive list of hackers/attackers. It is apparent that attacks on an infrastructure like Smart Grid may be caused by capable attackers. Thus, their incentives are more serious and strong (e.g. profit). Flick & Morehouse (2011) identified a more generic classification regarding the attacker's incentives particularly for the Smart Grid:

Personal gain: Some attackers try to exploit the capabilities of the Smart Grid technologies for personal monetary gain. For example, an attacker can use different methods, such as a malware, which is "*a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system (OS) or of otherwise annoying or disrupting the victim*" to gain control of the consumer's smart meter and to modify the data stored and disrupt the consumer's access to power. Then they ask a significant amount of money from the consumer to repair the damage.

Terrorism: There are many reasons and motives that lead to a terrorist attack. With the attack, terrorists can affect dramatically many people (by causing for example constant blackouts) and thereby shift the attention of the government and various public organizations on them.

Revenge: A former employee of a factory, who has been dismissed from his job, could be a representative example. He wants to take revenge from his employer. With the attack he can gain access to the smart meter of the factory and can interrupt the power supply for a period of time.

Types of Cyber Attacks

Because it is very difficult to take into account all the potential attacks due to the high complexity of the Smart Grid as a system, the types of cyber-attacks based on the previous security objectives are classified as follows (Wang & Lu, 2013):

- Attacks aiming at availability cause delays and jammed communication in the Smart Grid.
- Attacks aiming at integrity modify or disrupt the data exchange between the components of the Smart Grid.
- Attacks aiming at confidentiality have a purpose to gain illegally information from network resources of Smart Grid.

Basic types of attacks

Denial-of-Service (DoS) is the attack where the attacker (Bob) denies at the source (Alice) to have access in the destination (Mary) (Figure 12) (Queiroz, Mahmood, & Tari, 2011). A simple DoS attack tries to consume

resources to deny access by legitimate users. The DDoS (Distributed DoS) attack aims to destroy resource capacity, such as bandwidth, or to deny access to authorized users. This technique uses a network of attack agents (bots) to accumulate a simultaneous attack of messages on the specific target. The combination of DoS with other attack makes the attacker able to gain unauthorized access to a system, to transmitted data, or even to the network. It is difficult to keep wireless networks in the AMI environment secure and their components are vulnerable to an attack (Wang & Lu, 2013).

Man-in-the-middle-attack is when Bob masquerades as Mary (Figure 11), so he receives all messages from Alice. Bob can change the messages and forward them modified to Mary (Queiroz et al., 2011). The attacker disrupts a legitimate communication between two parties. The attacker controls the flow of information in communication links and may distract or distort the information sent by one of the original participants. The attacker pretends to be one of the two participants and thus receives messages from the communication between them. Then, he is able to change their content and to send false messages to the receiver. For example, if the receiver is an operator in the control center of an electricity supply company, then the attacker can send him false data. This could force him to take specific actions when is not needed or make him think that everything is running smoothly on the network in order to avoid take action when action is required (NESCOR, 2015; Wang & Lu, 2013).

Spoofing is the attack where Bob impersonates Alice so he can create and send messages to Mary. In this type of attack the attacker pretends to be someone else in order to gain access to a system to limit the resources or gain access to sensitive information. This type of attack can take various forms. At the level of the electricity network, the data from sensors and smart meters are transmitted to the control center for further processing. If the attacker launches an attack on one device and simultaneously alters the data collected from it, then the operator will perceive a smooth network operation and so the attack would be unnoticed (Wang & Lu, 2013).

Eavesdropping is the attack where Bob receives all messages sent by Alice to Mary, although Alice and Mary are not aware of it (Queiroz et al., 2011). The attack can be launched with the use of specific tools. These tools collect packages transferring through a network and depending on their quality, analyze the collected data. The main difference between "Eavesdropping" and "Man in the middle" attack is that in the first case, the receiver receives all messages sent by the sender without being modified in their content, i.e. attacker simply eavesdrops the conversation between them without them knowing it. On the contrary, in "Man in the middle" attack, the attacker pretends to be receiver and receives all messages sent from the sender and falsifies them in the way he wants (Wang & Lu, 2013).

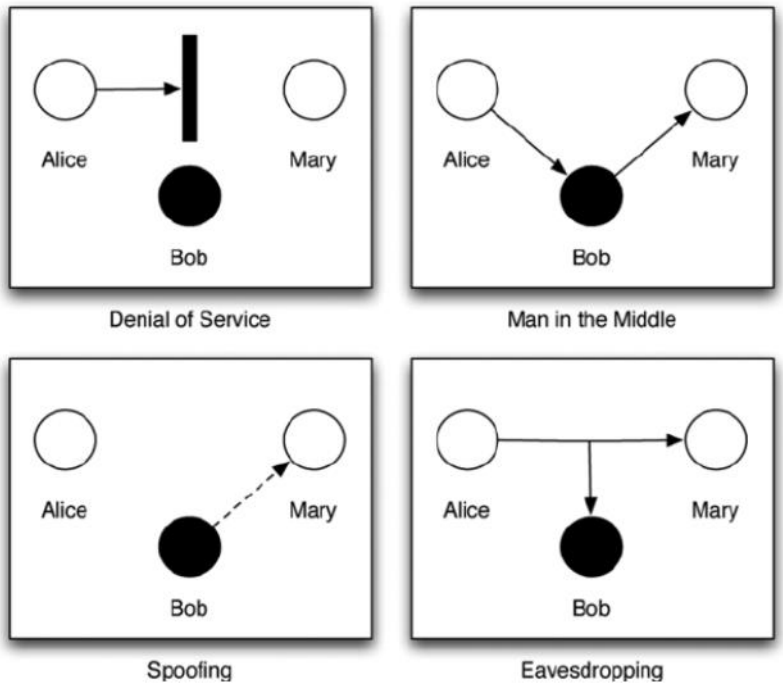

Figure 12 *Basic types of attacks* (Queiroz et al., 2011)

Security Issues – Different Scenarios

The aim of this subsection is to examine two scenarios that might take place in certain components of a Smart Grid, more specifically in Demand Response. Through this process an evaluation of the most representative risks that threaten these components and their communication takes place. In each scenario the certain impact that could be caused in a DR system and their potential level risk are defined. The assessment of the risks is based on the impact assessment model published by the Federal Information Processing Standards (FIPS) of the National Institute of Standards and Technology (NIST), (2004). The degree of impact will be assessed as low, moderate and high.

The possible impact is assessed as low when the violation of the security objectives causes limited harmful effects such as:

1. Insignificant economic losses
2. Limited damages to system's components
3. Limited negative consequences for the involved stakeholders that interact with the system
4. Reduction in the ability of a system to operate to an extent and the duration that still can perform its basic functions; but there is a visible reduction in efficiency of its functions.

The probable impact is evaluated as moderate if the violation of the security objectives results in serious effects like:

1. Significant economic losses
2. Significant damages to system's components

3. Significant and serious consequences for the involved stakeholders that interact with the system which cannot cause loss of life or serious life threats
4. Significant reduction in the ability of the system to operate an extent and duration that still can perform its basic functions; but there is an important reduction in the efficiency of its functions.

The degree of impact is characterized as high, when the violation in the security objectives has severe and catastrophic effects such as:

1. Severe and extensive economic losses
2. Extensive and severe damages to system's components
3. Severe and catastrophic consequences for the involved stakeholders that interact with the system, which could cause loss of life or serious life threats
4. Severe reduction or total loss in the ability of a system to operate to an extent and duration that it cannot perform even its basic functions

Availability is one of the main objectives as it is important for the consumers to have network access. Also, it is essential to ensure the data integrity and confidentiality because the sensitive information that transferred through the system. Therefore, cyber security for Smart Grid systems plays in important role and it has turn into necessary for utility companies to realize the most recent threats and to conduct detailed assessment concerning their systems.

According to the NESCOR Failures scenarios (2015), the following scenarios are descripted and their potential risk is addressed based on the previous impact assessment model:

Scenario 1: *Messages are Modified or Spoofed on DRAS Communications Link*
An attacker gains access to the communications link between the demand response automation server (DRAS) and the customer DR system modifies on-going communications, inserts modified or wrong messages, or launches a DoS or a replay attack. The DRAS and the customer system could take an unauthorized message or a wrong message. Such a message may cause unfavorable behaviors of these systems.
Impact: Low to Moderate
A false message may deliver modified information indicating cheaper prices to consumers, which encourages them to increase power consumption during on-peak periods. This may lead to power loss and the utility may have economic losses.

Scenario 2: *Blocked DR Messages Result in Increased Prices or Blackouts*
An agent blocks communications between a demand response server (DRAS) and a customer (i.e. smart meters). This could be succeeded by flooding the communications link with other messages, or by altering the information in communications link. These activities could prevent legitimate DR messages from being received and transmitted. This can occur at the wired or the wireless part of the communications link.
Impact: Moderate to High

Blocked DR signals may result in higher prices for electricity for the utility, which results on financial losses for them and gains for parties selling electricity back to the utility company. Also, blocked signals may result in increased energy charges for the consumers.

The previous scenarios aim to provide insights to the utility companies to conduct a detailed assessment for their systems and also to increase cyber security awareness throughout the different stages of the DR procedures (NESCOR, 2015).

On the other hand, the assessment of the impact based on descriptive scenarios is mainly subjective. Thus, in this thesis we attempt to develop an accurate model based approach to assess the impact of cyber-attacks into the DR system in a realistic and systematic way. This model based method has also more benefits compared to the descriptive scenarios because through a model we can run repeatability experiments and gain more information and valid results with less human effort.

3 AGENT BASED MODEL (ABM)

In this chapter, we elaborate in the modeling process. The necessary information that is used for the model implementation is provided. Also, the main idea and the methods that are used in the model are described.

3.1 System model - a detailed description

The model of the system that we focus (Figure 13) is based on several studies regarding the real time pricing (RTP) mechanism of DR (Samadi, Mohsenian-Rad, Schober, Wong, & Jatskevich, 2010; Samadi, Mohsenian-Rad, Schober, & Wong, 2012). The system consists of a central utility server and a set of subscribers (i.e. households). For each household it is assumed that there is an energy consumption controller (ECC) unit, which controls the user's power consumption, embedded in smart meter. These smart meters are connected to the utility server through communication links. The intended period for the system operation is divided into T time slots.

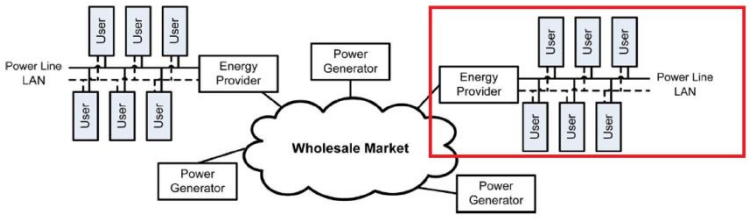

Figure 13 System model as indicated in (Samadi et al., 2012).

Households

Households are the consumers (or end-users) of the Smart Grid and they are assumed to have smart meters installed. We model three representative household depending on the number of members. Different household types have different annual demand (Nibud, 2017). Even though, the list of household types is more extensive, types that have similar annual demand are grouped and the average annual demand is used instead. This value is used to calculate the basic demand profile (see next section) for each household for each period. Also, each type has a proportion of occupancy in the Smart Grid (CBS, 2015). This proportion is used as probability, when we initiate the system and randomly generate households.

Table 3 indicates the household types with their corresponding values. As expected, households with single person need the least amount of energy usage, whereas households with more four and more persons require the most. Also, the proportion of the second type (two to three persons) is the larger in the modeled Smart Grid.

Household type	Annual demand (kW/h)	Proportion on Smart Grid
1 person	2000	0.37
2-3 persons	3250	0.44
4 and more persons	4500	0.19

Table 4 *Household types*

Let N be the set of households. For each time slot $k \in K$, M_n^k and m_n^k, denote the maximum and minimum power level of the n-th household, respectively. The maximum power level may represent the total consumption of household assuming that all appliances are on, whereas the minimum power level may represent the load from appliances which always need to be on during the day. E_n denotes the total minimum energy requirement for a household n. In order to provide the required energy for each user, it is required that:

$$\sum_{k \in K} x_n^k \geq E_n$$

where x_n^k is the demand of household n for time slot k. So, the feasible energy consumption controlling for a household n is defined as:

$$x_n = \left\{ x_n : \sum_{k \in K} x_n^k \geq E_n,\ m_n^k \leq x_n^k \leq M_n^k ,\forall\, k \in K \right\}$$

The central idea is that the entities are independent decision makers pursuing their own satisfaction. The energy demand of each household may vary based on different parameters. The different responses of different households to various price scenarios can be modeled by using utility functions from microeconomics. Utility function represents the level of satisfaction obtained as a function of its total power consumption. For a household n, $U(x, \omega)$ denotes the utility function where x is the energy consumption and ω is a parameter which varies among the households representing the value of electricity for each household. Quadratic utility functions corresponding to linear decreasing marginal benefit are considered for this model:

$$U(x, \omega) = \begin{cases} \omega x - \dfrac{a}{2} x^2, if\ 0 \leq x \leq \dfrac{\omega}{\alpha} \\ \dfrac{\omega^2}{2a}, if\ x > \dfrac{\omega}{a} \end{cases}$$

where α is a pre-determined parameter. This utility function is based on the assumption that fulfills the following properties:

- Utility functions are non-decreasing, i.e. users are always interested to consume more power if possible until they reach their maximum energy level.
- The utility functions are concave and the level of satisfaction for households can gradually get saturated.
- Households are ranked based on their utilities. In this formulation, it is assumed that for a fixed consumption level x, a larger ω implies a larger U (x, ω).
- The general expectation that no power consumption brings no benefit is assumed.

A household that consumes x kWh electricity during a designated number of hours at a rate of P dollars per kWh is charged Px dollars per hour. Hence, the welfare of each user can simply be represented as

$$W(x, \omega) = U(x, \omega) - Px,$$

where W(x, ω) is the household's welfare function, U(x, ω) is the utility function, Px is the cost for the energy consumption x. For each price, the household adjusts the consumption in order to maximize its welfare. Thus, the following function describes the demand update for each household at each time step k:

$$x_i^k(P^k) = \underset{m_i^k \le x_i^k \le M_i^k}{\operatorname{argmax}} \left\{U\left(x_i^k, \omega\right) - P^k x_i^k\right\}$$

where $x_i^k(P^k)$ is the consumption for the imposed price P^k.

Demand load profiles

In order to produce demand profiles for a household we use synthetic load profiles. We have collected synthetic load profiles generated for the years 2015-2017 (APCS, 2017). These profiles are unitized over the year of use; the aggregation of all values for a year is 1 (or close to 1). In these data, each value represents the Profile Coefficient for a quarter of an hour (the Settlement period). Profile Coefficient is an estimate of the fraction of yearly consumption within the Settlement period. Thus, using the annual demand for each different household type, we can calculate the demand allocation for a Settlement period (15', an hour or a day, etc.). Because we do not use appliances to adjust the demand based on the price changes we set minimum and maximum demand. So, based on the demand profiles from the given data, we generate minimum and maximum load profiles. They represent the 70% and 110% of load profiles respectively. These profiles are important as they are the necessary boundaries for the calculation of the welfare for the consumers in simulations.

Utility server

For the utility server, its pursuit is to minimize its energy costs. Alternatively, its attempt is to maximize the available capacity at which the cost is minimal. A cost function $C_k(L_k)$ denotes the cost of providing L_k units of energy offered by the utility server in each time slot $k \in K$. The following quadratic cost functions are used in the model:

$$C_k(L_k) = a_k L_k^2 + b_k L_k + c_k,$$

where $a_k > 0$ and $b_k, c_k \geq 0$ are pre-determined parameters.

The following function describes the Capacity update for the utility server:

$$L_k(P_k) = \underset{L_k^{min} \le L_k \le L_k^{max}}{\operatorname{argmax}} \{P_k L_k - C_k(L_k)\}$$

where L_k is the available capacity, P_k is the imposed price and L_k^{min}, L_k^{max} are the capacity boundaries for time step k.

Real Time Price Mechanism

For real time price schema, the method derived from this study (Samadi et al., 2010) is used. It is based on the dual decomposition approach of the optimization problem they formulate in their work. The price is recalculated every constant time steps and it is based on the available energy capacity of the utility server and the overall demand of the households. The following function describes the real time price update:

$$P_{t+1} = \left[P_t + \gamma\left(\sum_{i \in N} x_i^k P_t - L_k(P_t)\right)\right]^+$$

where γ is the step size.

3.2 Description of modeling steps

This section describes the research methodology that was followed and the ten steps that are used in the modeling process of the agent based model are described (Dam, Nikolic, & Lukszo, 2013). This model helps us to find the appropriate answers to the research questions of this thesis.

The aim of this technique is to gain valid insights with regards to the implications of cyber-attacks on the DR program. Even though, essential information is retrieved from the literature, with the implementation of ABM a more in-depth analysis is aimed to verify the initial hypothesis quantitatively. The outcomes of the model include numerical deviations of the aggregate demand that occur due to the cyber-attacks and through the two way communication of price and demand signal between utility server and households. The amount of flexibility of the value of RTP program is based on the responses of the individual households to the price signals. The aggregate demand is the total energy demand of all the households in the system reacting to the price signals. The households behave independently as a result of several rules and properties. New energy prices are calculated based on dynamic rules affected by the peak period, the current energy costs and capacity for the server and the aggregate demand of the system. The interactions between the server and households and the penetration of attacker evolve the overall behavior of the system. Therefore, a bottom-up approach, in which all the interactions between the server and the households (i.e. aggregate demand) could be well represented by an agent-based model.

Step 1 – Problem formulation and actor identification

Currently, there are insufficient insights regarding the impact of cyber-attacks in DR programs. These insights could contribute to the development of a more secure Smart Grid, which will retain its security objectives as a critical infrastructure system. It is already highlighted the benefits of DR programs but there are no insights on how cyber-attacks affect and may change the outcomes of DR.

The key actors of the model are the consumers of electricity in the form of individual households. They have been chosen according to their household's annual demand, with the help of retrieved data from the Nibud database (Nibud, 2017). They are classified in three main household types. Also, the utility is considered as an active player in the model since the implementation of real time pricing policy translates to desirable consumption patterns. Moreover, attackers, who launch a cyber-attack in the communication link between

utilities and consumers, act between the consumers (active agents) and the utilities. Also, they are passive players in the model and are not clearly represented, but they are very important in the real-life world.

In our model, the network consists of different actors and is visualized in a comprehensive way as following:

Figure 14 *Actors representation of the model*

The Figure 14 depicts the actors that are connected with the communication link through which the information is transferred. The link connects the **utility** with the **households**. In each different type of household a smart meter is implemented. Finally, the **attacker** is connected to the communication link and launches the attacks into the network.

The modeler' role is to build a precise model, which will introduce and examine the problem of cyber-attacks in pricing based mechanism of DR. It is important to highlight that all assumptions made with respect to the real word situation without changing the correctness of the insights that are gained from the model.

Step 2 – System identification and decomposition

In this step of the modeling process, we identify the environment and the system with the individual components and their characteristics and variables. Figure 15 indicates the system, its components with their interactions and the physical boundaries among the entities. The system comprises of a single utility server, an aggregator that collects the demand from the network, a regulator that regulates the levels of demand on the network by applying a certain price program (RTP, etc), and a set of households that have smart meters. These entities are connected through a two way communication link forming the network. The attacker is an additional entity that connects on the network. Since we focus on the transition of the price-demand signal, we take out other physical connections, such as the electric grid. The communication between the entities includes price and demand signals. Normally, the regulator decides the DR price schema in order to achieve social welfare and reliable electricity network, and the aggregator collects the demand from each household and calculates the consumers aggregated demand for the following day. In this model, because the price depends on the function cost of the server and the aggregate domestic demand and no market mechanism is used, aggregator and regulator can be represented as passive entities and their functions (i.e. aggregate demand, use of price schema) are operations of the server. Even though in real life cases these two entities are essential and have active role and cannot be excluded from the system.

The price signal is sent every instant of time (every hour for example) from the regulator to the households. Households, calculate the current demand based on price values with the aim to maximize their welfare. The demand signal is sent from the households to the aggregator every instant of time (every 15 minutes for example), which in turn sends the aggregated demand to the utility server. Based on current information on the network (overall demand, price) the utility server calculates the energy capacity with the aim to minimize the cost for the system and sends the optimal value to the regulator, which recalculates the price in order to regulate the demand on the network.

Attacker's role is to disrupt this information flow. One of the possible attacks is the man-in-the-middle attack. Attacker causes jamming on the price signal and sends false signal in order to trick the consumers. This interruption occurs in high-peak hours, in which the system is more prone to energy issues and failures. However, system blackouts or destructions are not considered possible in the model because there is always enough electricity in the network for the consumption. So, the data disruption leads in increasing energy demand from households, even if the utility server is incapable to offer it.

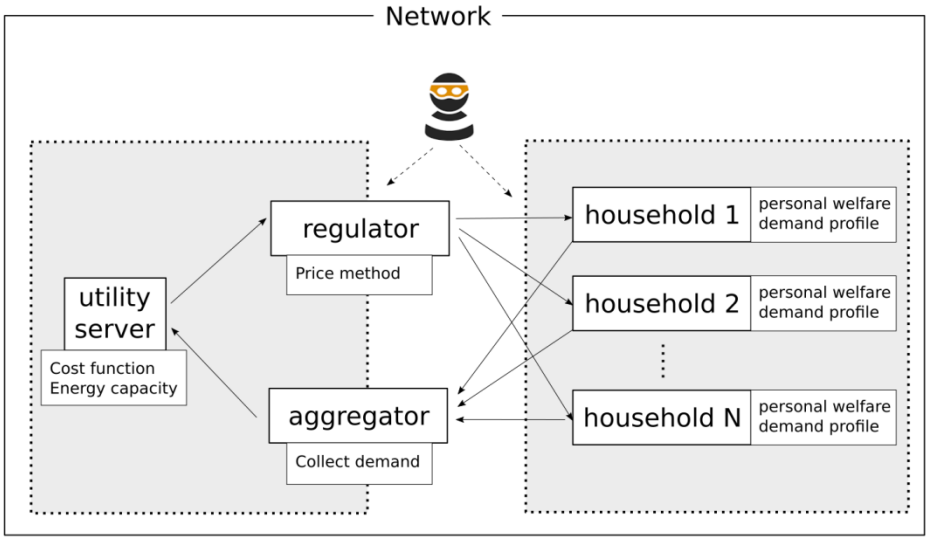

Figure 15 *Information flow in model*

Step 3 – Concept formalization

In this step, the identified concepts for the model are converted into computer readable format by means of defining the context and removing any ambiguity in the computational context. A method that facilitates the concept formalization is the class diagram structure. The several agents of the system are 'objectified', meaning that agents with their characteristics, behaviors and actions, and their in between interactions are converted into objects (or classes) with their respective variables and methods. Figure 13 shows the class diagram for the system.

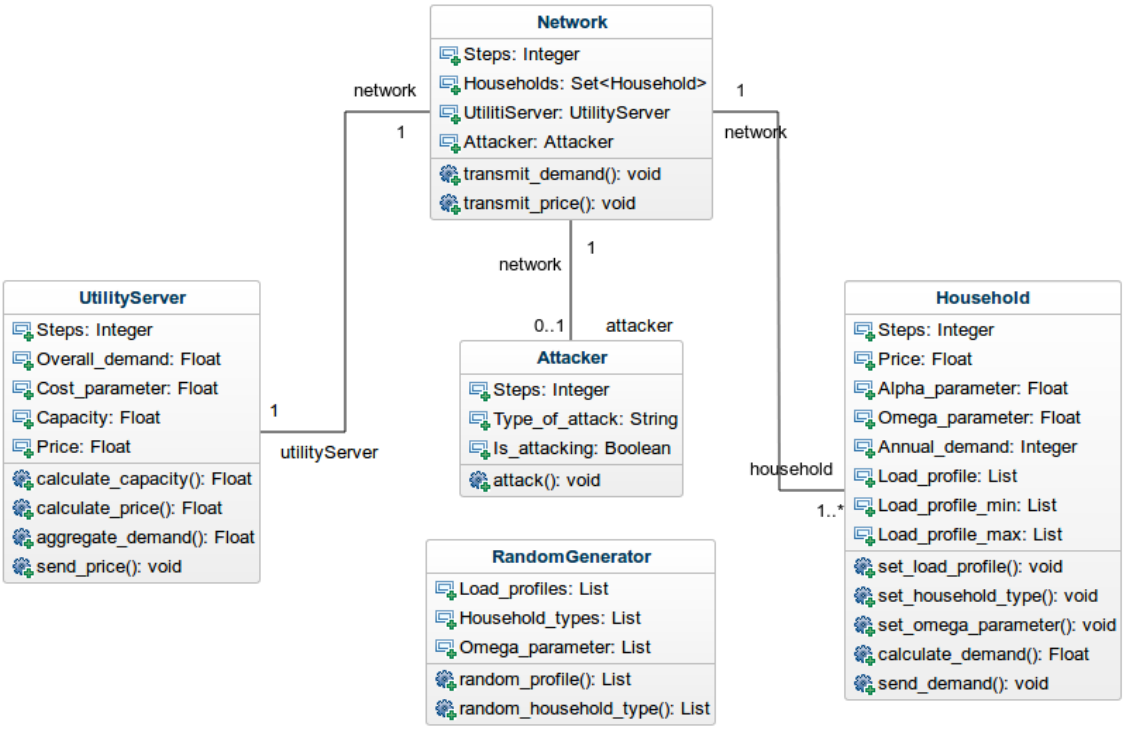

Figure 16 *Class diagram of the system*

To simplify the software structure, the aggregator and regulator agents have been merged with the utility server. So, the UtilityServer class comprises the compound of agents Utility server, aggregator and regulator. The attributes of this class are:

- the steps (or ticks) of the system,
- the overall_demand, which is the aggregate demand of the system (aggregator's attribute) at each step,
- the capacity, which is the capacity (server's attribute) of the system at each step,
- the price, which is the recalculated price (regulator's attribute) at each step
- the cost_parameter, which is the parameter for the cost function. This parameter varies for different steps in the period. It has different value for off-peak, med-peak and high-peak time instances.

The methods (or operations) of this class are associated with the behaviors of its entities:

- calculate_capacity(): This method calculates the capacity of the system at each step. The capacity value is the optimal value (argmax) for the minimization of the cost of the system for the current time instant. It depends on the current price, the overall demand of the system and the peak (off, med, high → different paramater value).
- calculate_price(): This method recalculates the price of the energy for a time instance. It is enable for the RTP program and it calculates the new real price of the energy given the capacity, the overall demand and the previous price on the system.

- aggregate_demand(): This method sums the demand of all households for a time instance.
- send_price(): This method activates the network to transmit the price signal (i.e. the new price) to the households.

Household class refer to the households of the network. So, in the attributes and methods of that class there are also elements for the smart meters. The attributes of this class are:

- the steps (or ticks) of the system,
- the electricity price, as it is received from the network for a time instance,
- the annual_demand; this attribute is associated with the type of household, different household type has different annual demand,
- the load_profile, this attribute is randomly chosen at the beginning of a new day and it is used to generate the boundaries of the demand profile for the household,
- the load_profile_min, which is the minimum demand profile for the household,
- the load_profile_max, which is the maximum demand profile for the household,
- parameters alpha and omega, these two parameters are used to calculate the maximum welfare for the user at each time step.

The methods for the behavior as well as some initial steps for the objects are:

- set_load_profile(): this is used at the initial step of the simulation, and before every new day; it generates a daily load profile for a household.
- set_household_type(): this method randomly chooses a household type and the attribute annual_demand is initialized.
- set_omega_parameter(): this method randomly sets a value of omega parameter from a pool of integers.
- calculate_demand(): this method returns the demand that maximizes the welfare for a household.
- send_demand(): This method activates the network to transmit the demand signal (i.e. the household's demand) to the utility server.

The Attacker class represents the potential threat of the system. The attributes of this class are:

- the steps (or ticks) of the system,
- the type_of_attack, which annotates the type of the attack at the current simulation,
- the is_attacking, a boolean attribute that indicates whether the attacker is attacking at the current time instance.

The attack() method shows the behavior of the Attacker agent. When the attacker attacks this method is called and the system is affected accordingly.

The Network Class groups the other classes. It is the communication link for the entities. This class is an additional class that facilitates the simplification of the formalization of the system. It contains a single UtilitiServer class, an Attacker and a set of Households. The only operations for this class are the data transmissions (transmit_demand() and transmit_price()), which model the communication between the entities. The association links between the classes indicates that the network consists of a single utility server, the potential attacker (may or may not be present), and a set of households.

The RandomGenerator class is an additional class that contains data and operations that help the generation of data for the households. Its attributes are lists of available data, such as load profiles, omega parameter and household types. With the method random_profile() it randomly generates a load profile based on the list of load profiles. With the method random_household_type() it randomly generates the type for each household; different type have different probabilities of occurrence.

Step 4 – Model formalization

Narrative of the model for a single day for a scenario with an integrity attack (man-in-the-middle). The main process operates for 96 ticks, so each tick represents 15 minutes of an hour in the day. Initially, the random values are set. These values are the household type and the demand profiles for the households. For each tick, the utility server first collects the demand from the households. Based on this overall demand calculates the optimal energy capacity. If it is time to set new price (every 4 (1 hour)), utility server calculates the new price based on the its capacity and the overall demand and communicates it to the households. In the case of integrity attack, the attacker intervenes into the price signal and changes its value. This results for households in receiving different price than the one sent by the server. Finally, the households calculate the new demand based on the false price. It should be noted that the baseline scenario, where no attack event occurs, has the same narrative excluding the attacker's tasks and events.

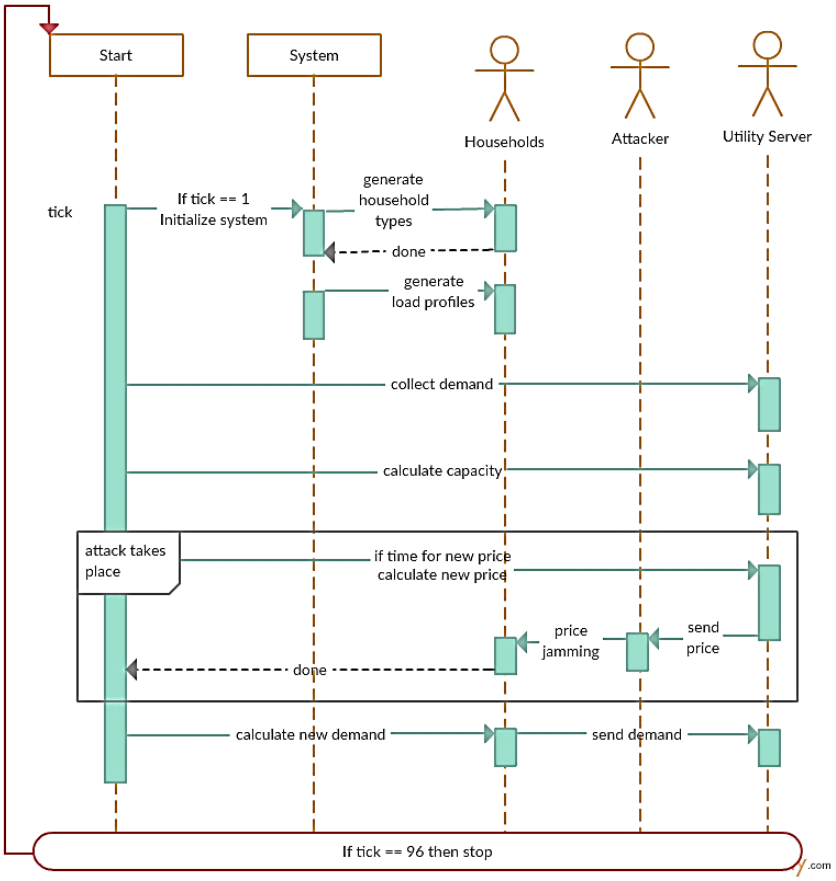

Figure 17 *UML sequence diagram*

The pseudo code that describes this narrative follows in Algorithm "Process of the day". As in the sequence diagram, the baseline scenario is realized when the attacker is not present.

Algorithm 1 Process of a day

```
Household = Object
households = Set[Household]
utilityServer = Object
attacker = Object
hours = List
while tick ≤ 96 do
    if tick == 1 then
        for each household in households do
            household.setDemandProfile()
            household.setHouseholdType()
        end for
    end if
    overallDemand = utilityServer.collectDemand(households)
    capacity = utilityServer.calculateCapacity()
    if tick in hours then
        price = utilityServer.calculatePrice(capacity, overallDemand)
    end if
    if attacker.isAttacking() then
        price = attacker.attack()
    end if
    for each household in households do
        household.calculateDemand(price)
    end for
end while
```

Step 5 – Software implementation

The model is implemented in Python 3(Perez, Granger, & Hunter, 2011) with the agent-based modeling tool Mesa (Kazil & Vērzemnieks, 2014). This tool is an alternative to other tools such as NetLogo (Wilensky, 1999) and Repast (North et al., 2013). The main difference is that it is written in the powerful language Python, which has a large community worldwide and allows for use of several libraries to analyze the results of the simulations. The initial idea was to use NetLogo, but it was quickly rejected, because it was less user-friendly as the implementation of the several agents was time-consuming. Also the documentation was poor and there are no additional tools to quickly analyze the results from the simulations; additional analysis tools like Excel or Matlab are necessary. On the contrary, Mesa is based on Python3, so the model is modular and fully programmable. Apart from the built-in core components the user can customize many features, using object oriented techniques. Also, built-in data structures such as *Pandas* and *Series* facilitate the analysis of the simulation results. Built-in python tools such as *Matplotlib* or *NumPy* are essential additions as they are powerful libraries for analysis and post-processing of the results. Finally, the nature of Object-oriented structure of the model makes it customizable and extensible for future work.

Step 6 – Model verification

The main goal of this step is to investigate if there are any structural mistakes in the code and to verify the technical correctness of the model, aiming not to draw conclusions from a mistakenly working model. The main 4 types of verification are the following:

1. Recording and tracking agent behavior

In this step, the agents were tested for input, state and output throughout the entire simulation cycle. Households acquire new demand profile every day randomly from the pool of collected profiles and different

annual demands are set based on given probability for different household types. The initialization of the parameter of ω, which indicates the household's level of satisfaction on energy consumption, was assessed in terms of the variety of resulting demands for the households. Also, the initialization of other parameters was specific for each operation and agent and the scale of parameters at every point in the program was monitored and tested for consistency and correctness.

2. Single agent testing

In this step, the agents were tested individually whether they respond to signals from the system or other agents of the system. The single agents test involves two parts (Dam et al., 2013):

1. Testing theoretical predictions and sanity, in which it was observed if agents behave as expected according to normal conditions.

2. Break the agent tests, in which agents took extreme values in order to discover the boundaries of normal behavior.

More specifically, the households were assessed whether they respond to the price signal changes by monitoring the demand and its fluctuations. Also, in the same manner, the response of the utility server to the overall demand and peaks of a day was assessed by checking the capacity update at every time step. Subsequently, the attacker behavior, through price modifications, is tested accordingly.

3. Interaction testing

In this step, the interactions between the agents are tested. The interactions between the agents consist of three types: price signal, demand signal and false price signal. Hence, the interaction tests are based on the response of each agent on these interactions. This took place by running the model with only one of each agent. The expected outputs for each interaction are assessed in terms of whether the corresponding values are proportional or inversely proportional. For example, the decrease of price value indicates the increase of demand for the households, whereas for utility server indicates the decrease of energy capacity. Likewise, the imposed price by the attacker indicates the proportional increase/decrease of the demand by the households.

4. Multi-agent testing

In this step, the overall behavior of the system is tested. This involves the interactions among all the agents and the behaviors of resulting patterns. Two tests are performed in this step of verification: A variability test in which the variability of various critical model outputs was assessed. Also, a timeline sanity test was performed with the aim to assess various outputs of the model at the default parameter setting, and tried to foresee any unexpected modeling behavior. The aggregated demand on the system is assessed whether it follows the default demand profiles from the literature. Several runs of the multi-agent test for the same set of parameters were performed to test the stability of the model and trace any unexpected errors. These tests were repeated for all possible scenarios (baseline scenario or with attacks) in order to check for bugs and verify the outputs from the system.

Step 7 – Experimentation

The research problem of this thesis is answered through various scenarios in an ABM. The main focus of this section is the design of the experiments. Each of these experiments aims to provide valid answers to the research questions. Three different experiments are designed for the simulation of the agent based model. Their results on the power demand and the price signal, concluded by the interaction of the agents with the system, are consequently used for data analysis.

General Experimentation setup

Due to the nature of the studied problem, the time intervals need to be chosen so that the given information from the experiments increases the accuracy of the analysis. Also, the synthetic profiles have reporting values every 15 minutes, which leads us to simulate each tick to account for 15 minutes of an hour. Hence, a single day is 96 ticks. In addition, the periodicity of the real time pricing is chosen to be k = 4 ticks (i.e. every hour) in order to represent the real existing cases (intra-day) where consumers are informed for the price updates every hour.

Intervals of peak hours are derived by the patterns of collected demands. Then the intervals are as following:

1. [0, 27], [92, 96] are in the off peak hours
2. [28, 35], [56, 71], [88, 91] are in the medium peak hours
3. [36, 55], [72, 87] are in the high peak hours

The number of households is chosen to be 500 for two reasons. First, large number of households is used in order to eliminate any possible deviation between the different demand patterns. Second, with the large number of households it is possible to distinguish the different outcomes when choosing the different values for the fraction of affected households (see below).

For households

- Each household is assigned the ω parameter randomly from interval [5, 15] with equal probability.
- Each household is assigned the household type randomly with different probabilities as previously described.
- For every day, each household is assigned a default load profile randomly generated as previously described. The demand load boundaries (min, max) for each tick are the 70% and 110% of the default demand load profile respectively.
- α parameter is the same for all households and equal to 0.5.

For utility server

- the parameter a_k of cost function is variable and depends on the daytime. For off-peak, med-peak and high-peak is 0.02, 0.1 and 0.2 respectively.

For the Real time pricing

- the step size γ for the pricing function is set to 0.15

Scenarios

Scenario 1: Baseline scenario: No attack occurs. Demand for all users with Real Time Pricing schema.

The system works properly. Price and demand signals are communicated to the agents of the system. Households correspond to price changes and modify their demand accordingly. Also, utility server reacts to overall demand of the system and adjusts the price of the energy according to its energy costs.

Scenario 2: Integrity attack scenario.
This scenario aims to determine the overall energy consumption in peak hours using the RTP program under the integrity attack. During a certain time of the day (high peak hours) an integrity attack is launched on the communication link of the price signal. High peak period is the most critical for the infrastructure throughout a day. Through this scenario, the effect of this cyber-attack and its implications on the power demand and the price signal is examined and compared to the baseline scenario. In addition, different cases with different fraction of affected households are considered (5%, 50%, 90%, and 100%). These fractions are used in order to assess the implications when the attack occurs on different scale of affected households. Low scale (5%), medium scale (50%) and large scale (90%, 100%) of affected households are used.

Scenario 3: DoS attack scenario.
This scenario is designed to study the impact of DoS attack on the system and the results are compared to the baseline scenario. This type of attack is different from the previous one, as it makes the utility server unavailable for a certain period of time. This attack scenario takes place in a smaller period of time and starts during the high peak hours. As a result, the overall energy consumption in peak hours using the RTP program under the availability attack varies significantly.

Step 8 – Data Analysis

For identifying the implications of two types of cyber-attacks in RTP mechanism of the DR program and on the demand power and price signals, an agent based model was implemented with the use of framework Mesa in Python3. Different experiments were designed and implemented in the developed model as described in the previous section. Several libraries of Python3 were used to extract and analyze the data from the model. The findings from the different designed experiments are presented and discussed in chapter 5.

Step 9 – Validation

While the step 6, the model verification emphases on verifying the outputs of the model, the step 9, the model validation, has as a goal to investigate if the model corresponds to the real world and behaves as it is expected to behave. There are four main different techniques to validate the model and to check if the results and insights from previous steps are reliable. These four techniques are the following:

1. Historic replay
2. Expert consultation (face validation)
3. Literature validation
4. Model replication

The developed model validated with the aim understands if the model behavior represents as much as possible, with the available "real" data, the real world behavior and if the interactions and the pricing mechanism characterized by correctness. Because there is no Smart Grid implementation with the demand response system applied on this model, it is impossible to validate the results of this model with a ground truth from real world. Also, the dynamic pricing mechanisms, such as the real time pricing, are not applied yet in the real world. Even though, some data may are available from pilot programs, these data all not open to the public, due to privacy protection of the sensitive information that are contain. So, for now without available data from the past, it is not able to use the historic data, as a validation method.

The model was validated with two different approaches. From the data analysis section, as we can see the results show that the model represents the reality as much as possible. Unfortunately, not all the outputs of the analysis were validated through literature validation, because some of the concepts that were examined in this thesis are state of art and there are not applicable yet in the real world.

In this case, expert consultation was used as a validation method. During the expert validation with the Professor D. Gritzalis from the section of ICT Security of the Laboratory of Information & Communication Systems Security, Dept. of Information and Communication Systems Engineering, School of Engineering, Greece. An interview was conducted through Skype with the expert and the main steps of the methodology, the results of the data analysis and the assumptions of the model were discussed. On the other hand, some thoughts about the face validity concern the subjectivity of this method. It is so because face validity based on one expert opinion, who will gain only an abstract overview of the main processes of this research and even if he is an expert in cyber security and critical infrastructures protection due to time limitations he only proposed that the model "looks accurate and corresponds to reality" rather than the stronger believe that the model "is correct and represents the reality".

Due to the highly demanded time and the large workforce that are needed for the model replication and due to the time limitations during the thesis it was impossible to perform the model replication as a validation technique. After the completion of the step of the model validation, the confidence was grown that the model appropriately satisfies the aim of the research.

Step 10 – Model Use

In this step of the thesis, the *usability, feasibility and adaptability* of the previous developed and simulating model is described.

Usability

The main reason of defining the usability of the model is to understand to whom this model would be useful and why. Smart Grid is a complex infrastructure and multiple actors participate in the network. Its security is considered essential and the impacts of potential cyber-attacks are not negligible. This model would be used for further research, either from researchers in ICT and Cyber security sections, who study the impact of cyber-attacks in the Smart Grid or researchers in Energy & Industry section, who study the vulnerabilities and the security of critical infrastructures. By using this model, one will be able to understand how different households

correspond in the real time pricing mechanisms and also to assess the results of an integrity and availability cyber-attack to the system. Also, nowadays, the Real time pricing mechanisms are only applicable in pilot programs. Hence, through this model, researchers or organizations could gain insights on the effectiveness of real implementation of these mechanisms by considering the impact of an attack and concluding whether is worth or not to implement it in real life or what necessary actions would need to be taken before the actual implementation.

Feasibility

In this section, an attempt to discuss the limitations and constraints of the model takes place. Consumers (Households) always tend to change their consumption throughout a day (24 hours). Even though, this is true with the use of smart metering system, modifications on the night are not corresponding to reality. Attacker's capability to penetrate the system is not modeled. So, it is not possible to assess the prevention of potential attacks on the Smart Grid. The model is based on the demand response program, excluding any other connection among the agents, such as electric grid. This prevents the model from detecting other issues and destructions an attack may cause on the electric grid. The communication links are simple connections among the agents. Other aspects, such as connection delays and packets transmission are not modeled. This prevents the author from assessing the attacks on the size of information transferred on the network and their effects in terms of system overloads. Synthetic demand profiles are used instead of real data or appliances' energy adjustments. Also, classification of households is limited in 3 types based on the annual consumption. The combination of the latter two assumptions narrows the space of possible outcomes for the demand load profiles of households in the model.

Adaptability

When this model was implemented, the adaptability was one of the main aspects taken into consideration. It was really important to make the model adaptable in different conditions with the least effort. The nature of object-oriented structure facilitates any attempt for agent extension. Appliances can be modeled as new Classes and replace the current demand load profiles for the households to expand the outcomes for the demand profiles for households. Also, the communication links can become more complex by adding methods and attributes on the Network Class in order to add additional assessments on attackers' penetration capability and Smart Grid's data flow size. The implementation of other price programs such as TOU can be done effortlessly. Also, the attacker's behavior can be more sophisticated by adding probabilistic behavior models as methods of the Attacker Class.

4 DATA ANALYSIS AND RESULTS

In this section the results from the different designed experiments are elaborated and explained in order to investigate the impact of the different types of cyber-attacks in their energy consumption and the transmitted and received price signals, when consumers activate RTP program of DR. Thus, the experiments, which were designed for the aim of this study, were applied in the developed model, as described in the previous section. As a result, the outputs of the model were analyzed in details in order to gain valuable insights that would provide sufficient answers to the research questions.

Median curves for the simulation runs

For the stability of the results we extract the median plot for each value under study. Each scenario runs in 30 replications and from the 30 replications the median plot is extracted. Figure 18 and Figure 19 depict the plots for the aggregate demand of 10 and 500 smart meters respectively in the system.

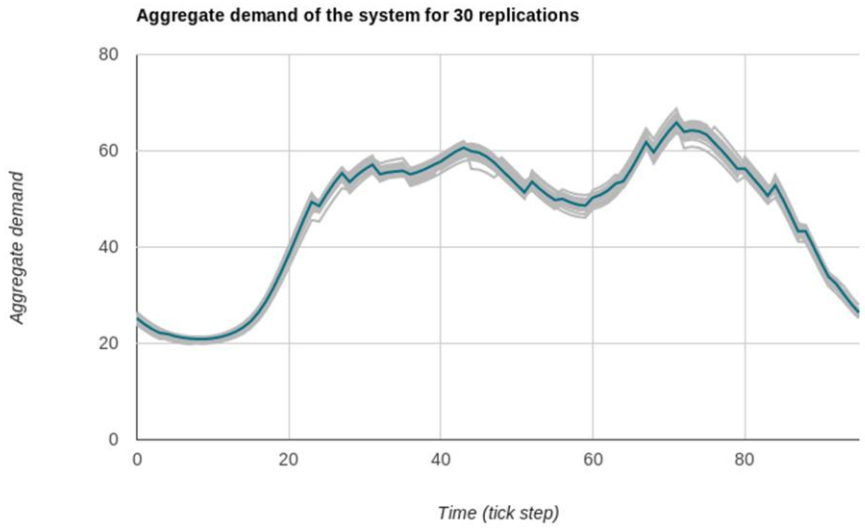

Figure 18 *The aggregate demand for 500 smart meters of 30 replications of the simulation. The grey area indicates the values covered by the 30 runs. The blue line is the median plot for these runs.*

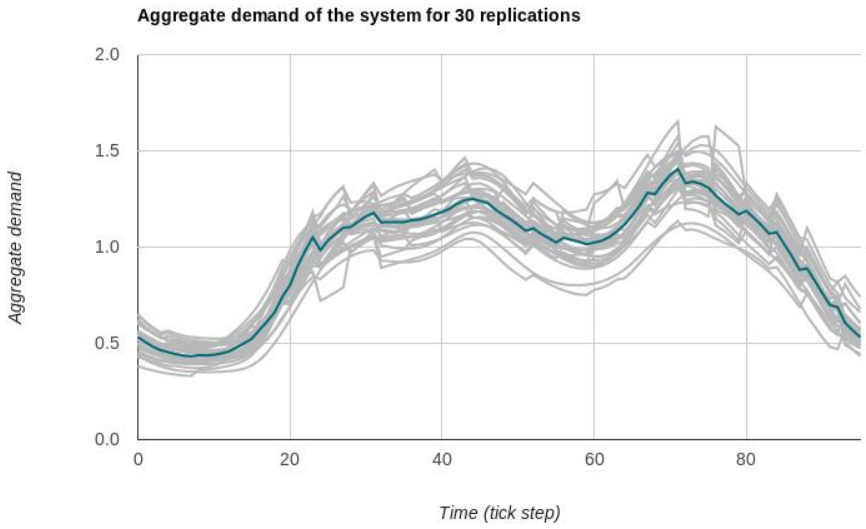

Figure 19 *The aggregate demand for 10 smart meters of 30 replications of the simulation. The grey lines indicate the values covered by the 30 runs. The blue line is the median plot for these runs.*

As expected, the curves for 10 smart meters are more variable compared to the corresponding curves of 500 smart meters. This is normal since the demand profiles generated for the 500 smart meters are more possible to overlap compared to the 10 smart meters leading to less variable curves. Finally, in both cases the median curve is a good representative of the sample. Therefore, for the following sections the median curves for the individual values are used.

Aggregate demand of household in the system

To investigate the outcome of the real-time price program we run the simulation for the model for the baseline scenario. We compare the aggregate demand that the households computed based on the price signal to the default aggregate demand generated by the respective synthetic profiles. The scenario runs within one day and in 30 replications. From the 30 replications the median plots are extracted.

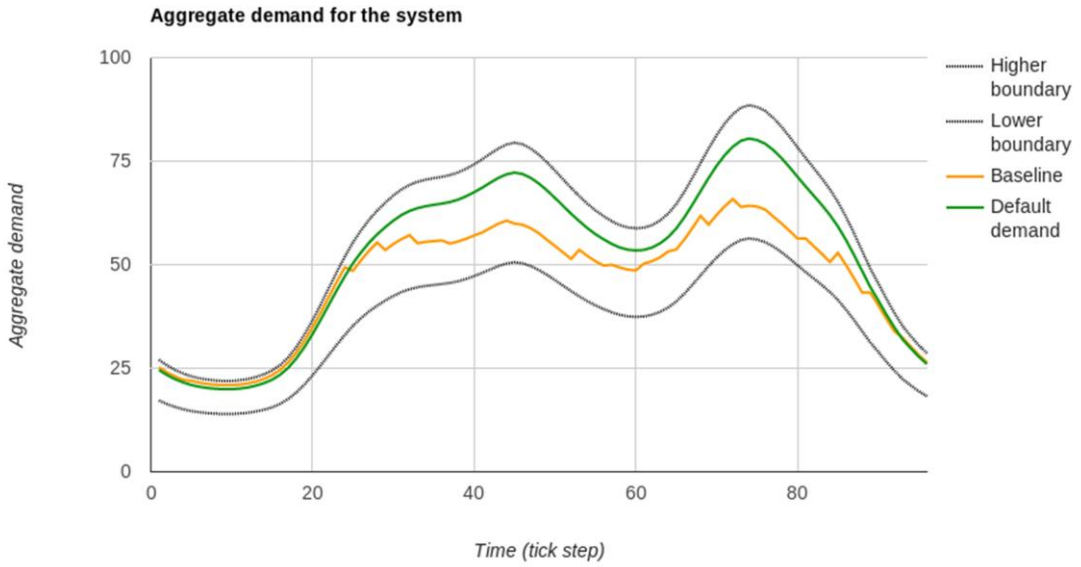

Figure 20 *Aggregate demand of the system plot for a day. The x-axis indicate the day in 96 time steps whereas the y-axis indicate the aggregate demand. The yellow line indicates the baseline scenario. The green line indicates the default aggregate demand as extracted from the synthetic profiles.*

Figure 20 shows the results of the aggregate demand for the normal behavior of the system. Compared to the default demand the aggregate demand of the system is lower in high peak hours and higher in the off peak hours. This shows that the households maximize their welfare with lower demand values where the price has its highest values throughout a day. In the same manner, the demand is increased insignificantly in the off peak hours, where the price is lower. Overall, the household react on real time price values by changing their demand in order to maximize their welfare. The aggregate demand in off peak hours differ insignificantly from the default profiles due to the fact that the cost of the energy for the server is low, and hence the values of the price are low. This leads households to maximize their welfare demanding the maximum possible energy.

4.1 Effect of man-in-the-middle attack on price and demand

To investigate the effect of man-in-the-middle attack on the price signal and the aggregate demand we run the simulation for the model for the baseline scenario as well as the scenario under attack. Each scenario runs within one day and in 30 replications. From the 30 replications the median curves is extracted. The attack takes place in mid-peak and high-peak hours. Two different cases of attack are considered with three different fractions of smart meters affected (100%, 50%, 5%): man-in-the-middle attack with halved price values (MITMh) and man-in-the-middle attack extreme case (MITMx). We measure for price transmitted by the server (TP), price received by the smart meters (RP) and aggregate demand of the system.

Table 5 summarizes the results for the different scenarios. Overall, the values of the different metrics correspond to the fraction of affected smart meters. When a fraction of 5% of smart meters is affected then the system is slightly affected. Except for the received price values for both cases, which is directly affected by the attacker, the other values change a little. However, when the fraction increases to 50% and 100%, the values change considerably. As expected, the worst case scenario is the extreme case with fraction of 100%, where the maximum aggregate demand, transmitted price and received price are the highest among all cases. It is worth noting that because of the demand boundaries for the aggregate demand, the system is always capable of offering the demanded energy and thus, there is a maximum boundary for the transmitted price as well. This is the reason why the differences between the extreme cases and the halved price cases are not great.

	average TP	Min TP	Max TP	average RP	Min RP	Max RP	Demand	Min Demand	Max Demand
Baseline	0.18	0.11	0.25	0.18	0.11	0.25	46.66	20.91	65.86
MITMh100%	0.22	0.11	0.31	0.13	0.08	0.24	53.04	21.04	80.32
MITMh 50%	0.19	0.11	0.28	0.12	0.08	0.19	49.67	20.88	71.92
MITMh 5%	0.18	0.11	0.26	0.11	0.08	0.16	47.07	20.96	66.98
MITMx 100%	0.24	0.11	0.34	0.05	0.0016	0.31	55.56	20.28	87.49
MITMx 50%	0.2	0.11	0.29	0.05	0.0016	0.2	50.46	21.04	74.4
MITMx 5%	0.18	0.11	0.26	0.04	0.0016	0.16	47.07	21.01	66.99

Table 5 *Results for the different scenarios*

The following figures indicate the aggregate demand of 500 households in a day for the different scenarios. Figure 21 indicates the aggregate demand when the man-in-the-middle attack with half price occurs, whereas Figure 22 shows the aggregate demand with the attack in the extreme case. The percentages are the fraction of affected smart meters for each scenario. The baseline scenario (yellow line) indicates the normal behavior of the system. The Min and Max demand boundaries are also depicted with dotted lines.

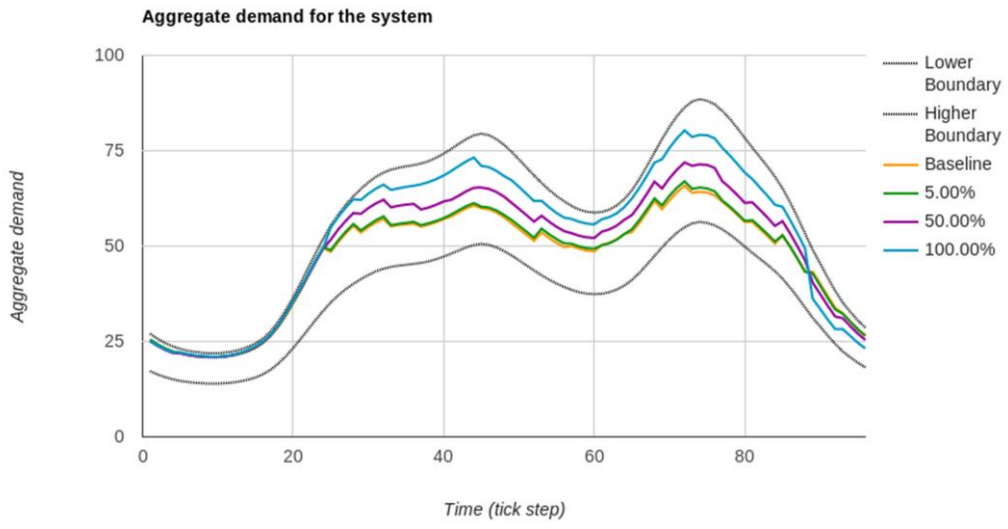

Figure 21 *The Aggregate demand of 500 households in a day. Scenarios with half price values on fractions of 5%, 50% and 100% of smart meters are depicted.*

Despite the fact that demand is analogous to the hours of the day, households reduce their consumption during high peak hours. This indicates that when the price is high the households maximize their welfare with lower demand values and vice versa. Subsequently, when the attacks occur and the households receive falsely lower prices they tend to increase their demand. As expected, on the attack scenario with the half price affecting the total smart meters of the system, the demand is significantly increased especially in high-peak hours where demand has higher boundaries (and thus, the households are more willing to demand for more energy). Also, the fraction of the affected smart meters affects the resulting demand curves. The 5% affected smart meters has negligible effect on the aggregate demand whereas the 50% increases it considerably. Generally, with the increase of the affected smart meters in the system the aggregate demand also increases.

For the extreme scenario, the demand reaches its maximum values as expected, as the price is nearly zero; the households maximize their welfare on the highest possible demand values. The fraction of the affected smart meters plays an important role here as well. As the number of affected smart meters increases the aggregate demand increases. Even though, this event is practically impossible, it is a good indicator for potential dangerous situations, where households tend to increase their demand, which may result in economic losses for them but also for equipment damages for the system.

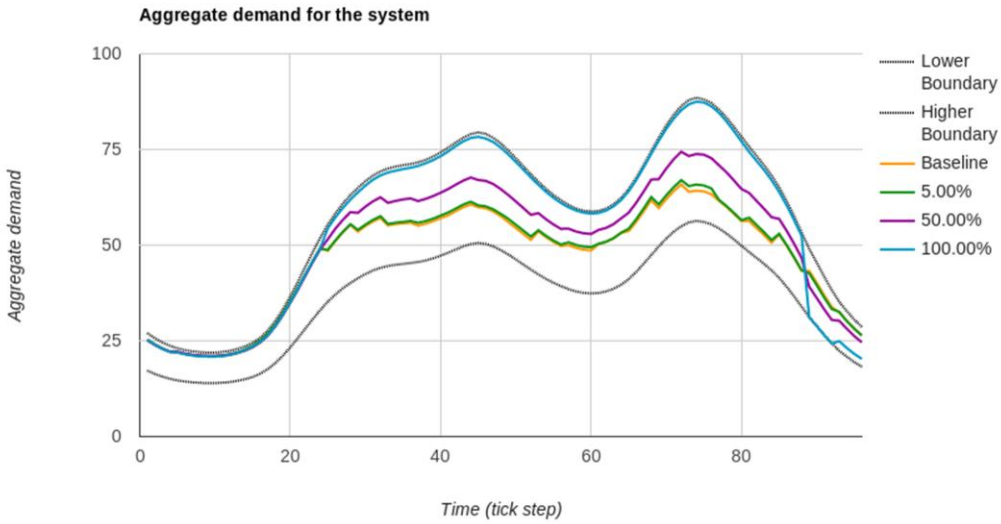

Figure 22 *Aggregate demand of 500 households in a day. Scenarios with extreme low price values on fractions of 5%, 50% and 100% of smart meters are depicted.*

The following figures indicate the real time pricing in a day for the different scenarios under man-in -the-middle attack. Each set of figures indicate the transmitted/received price when different fraction of smart meters is affected in both half price and extreme low price scenarios. The baseline scenario (blue line) indicates the normal behavior of the system. Apparently, the transmitted and received price for the baseline is the same.

The results show that the attack in these hours affect the price (Figures 23, 24, 25); the price is increased for the hours under attack. The effect is apparent during the attack, where the price reaches higher values compared to the baseline scenario. This may be partially affected by the households, which increase their consumption in

these hours as they receive false lower prices (yellow line). Overall, we observe that as the fraction of affected smart meters increases the effect on the price becomes greater. When the attack occurs on the 5% of smart meters the effect is negligible. However, for the larger fractions the effect is significantly higher. The highest values for the price are observed on the extreme attack scenario with fraction 100%. In addition, after the effect of the attack, when the smart meters receive the actual real time price from the server, the price starts dropping. This indicates that the households decrease their demand once they receive higher price values.

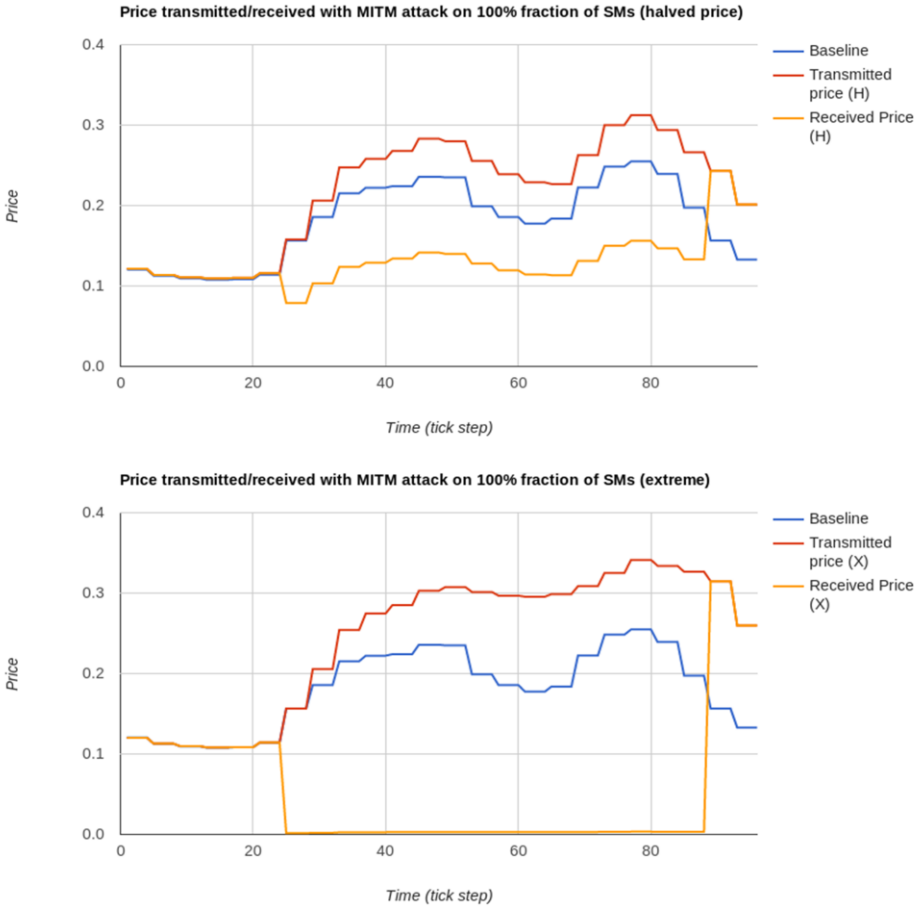

Figure 23 *Real time price that server sends and meters receive for a day under man in the middle attack on the total number of smart meters for both scenarios.*

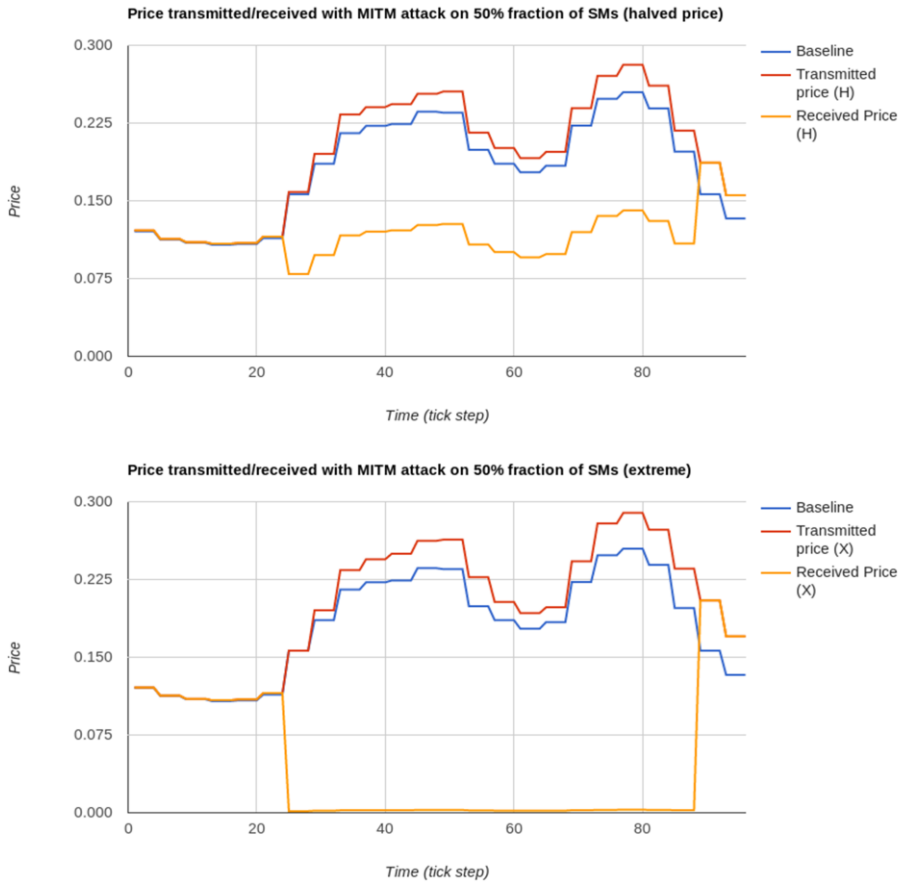

Figure 24: *Real time price that server sends and meters receive for a day under man in the middle attack on the fraction of 50% of smart meters for both scenarios.*

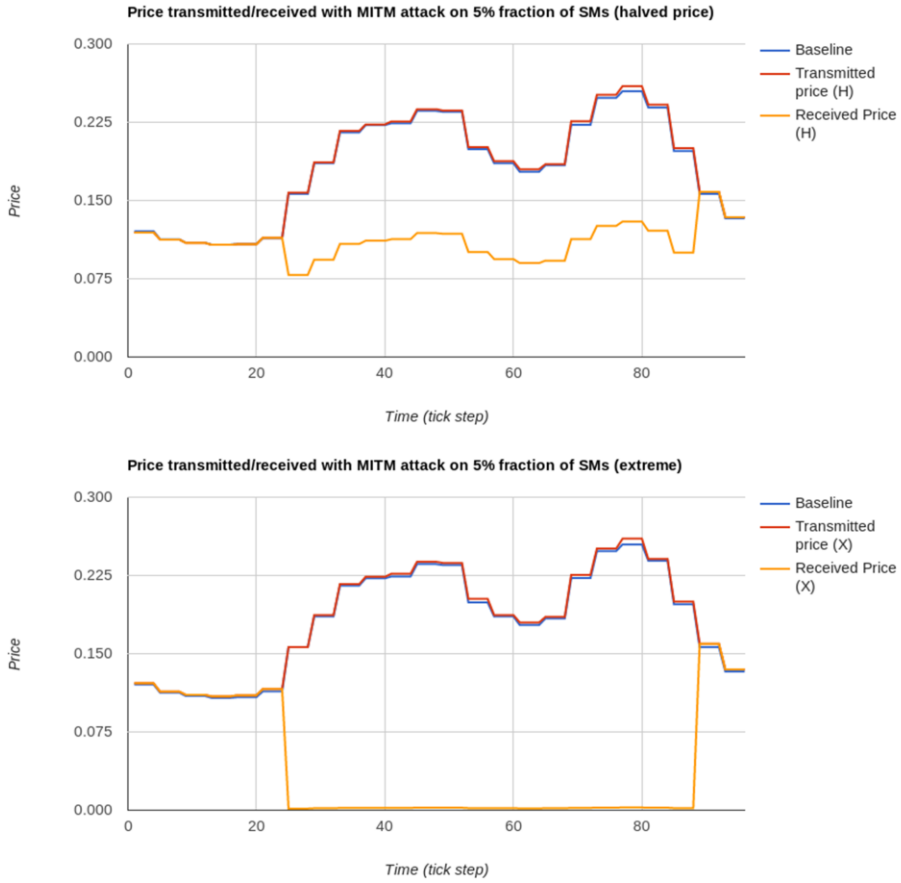

Figure 25 *Real time price that server sends and meters receive for a day under man in the middle attack on the fraction of 5% of smart meters for both scenarios.*

It is worth noting the fact that in the worst case scenario (extreme scenario on 100% smart meters) the values of the price while the system is under attack are moderate and fluctuate around certain -higher than the baseline scenario- price. The expected behavior would be the one depicted in Figure 27, in which the price is steadily increasing throughout the period of the attack. Our case can be explained by the fact that the server is always capable of providing the demanded energy. This means that the maximum demand (upper demand boundary) can be provided with a certain price by the server; the price plot in Figure 23. On the other hand, the behavior in Figure 27, where the price is continuously increasing, can be derived by a system in which the server cannot provide the demanded energy. In this case, the server has lower capacity than the aggregated demand. Thus, when the meters demand higher energy than the server is able to provide, then the price is constantly increasing.

We are able to replicate this behavior by lowering the maximum capacity of the server. We decrease the higher available capacity of the server by 1/5 of the maximum demand. The plots in Figure 26 confirm this behavior. When the aggregate demand is higher than the maximum capacity then the server increases the real time price in order to compensate the costs of operation. However, because the households continue to demand more energy the price keeps increasing (Figure 27).

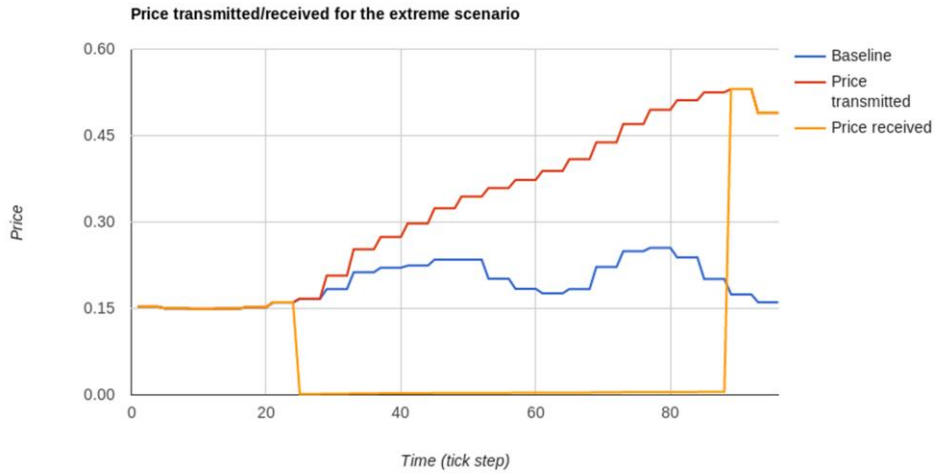

Figure 27: *Real time price that server sends and meters receive for a day under man in the middle attack extreme case, in which the server is incapable to serve the high demand of the system. This may results in high energy costs for the system and subsequently higher costs for the individual households.*

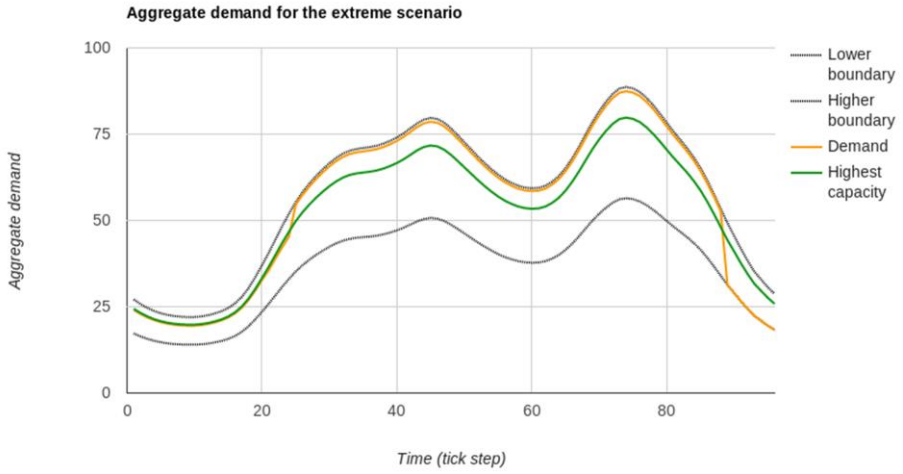

Figure 26: *Aggregate demand for the system under man-in-the-middle attack where the capacity of the*

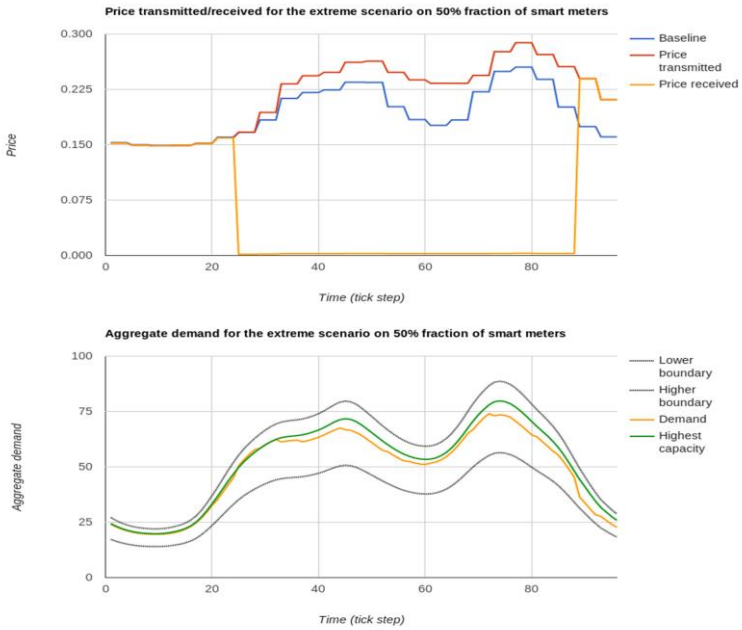

Figure 29 *Price signal and aggregate demand for the system under man-in-the-middle attack where the capacity of the server is lower than the aggregate demand. The fraction of the affected smart meters is 50%.*

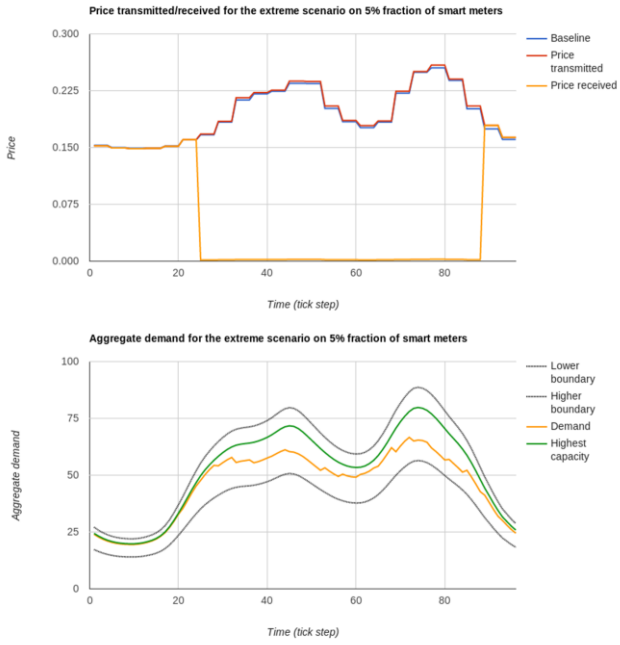

Figure 28: *Price signal and aggregate demand for the system under man-in-the-middle attack where the capacity of the server is lower than the aggregate demand. The fraction of the affected smart meters is 5%.*

We also tested this case with the attack in smaller fraction of smart meters. Figures 28, 29 indicate the results for demand and price for the system under man-in-the-middle attack on 50% and 5% of the smart meters respectively. The results show that because the aggregate demand is not higher than the maximum capacity of the server, the price, even if it is increased, it fluctuates around a certain price range and does not constantly increase.

4.2 Effect of DoS attack on price and demand

To investigate the effect of DoS attack on the price signal and the aggregate demand we run the simulation for the model for the baseline scenario as well as the scenario under attack. Each scenario runs within one day and in 30 replications. From the 30 replications the median curve is extracted. The attack takes place in different times within a day and lasts for 2 hours. During the attacks households continue to demand energy using the latest received price. The DoS attacks are launched in low peak and high peak hour.

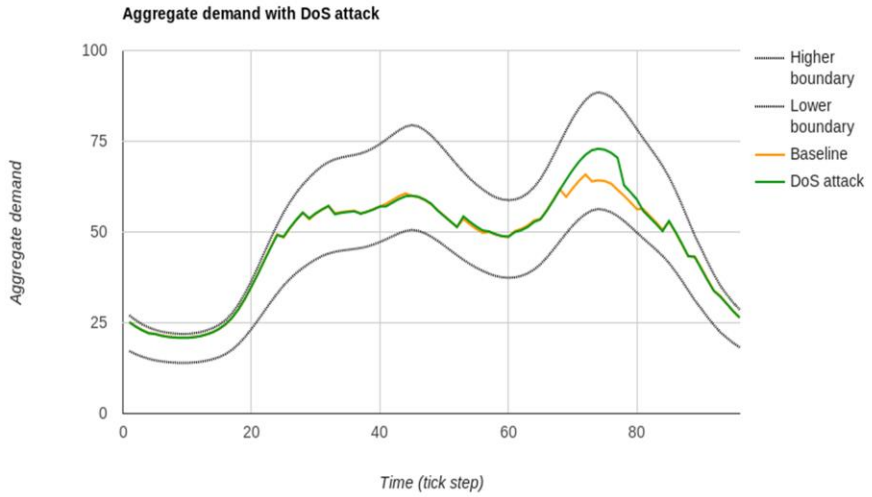

Figure 30: *Aggregate demand of the system plot for a day under DoS attack. The x-axis indicates the day in 96 time steps whereas the y-axis indicate the aggregate demand. The yellow line indicates the baseline scenario. The attack launches in high peak hour (green line).*

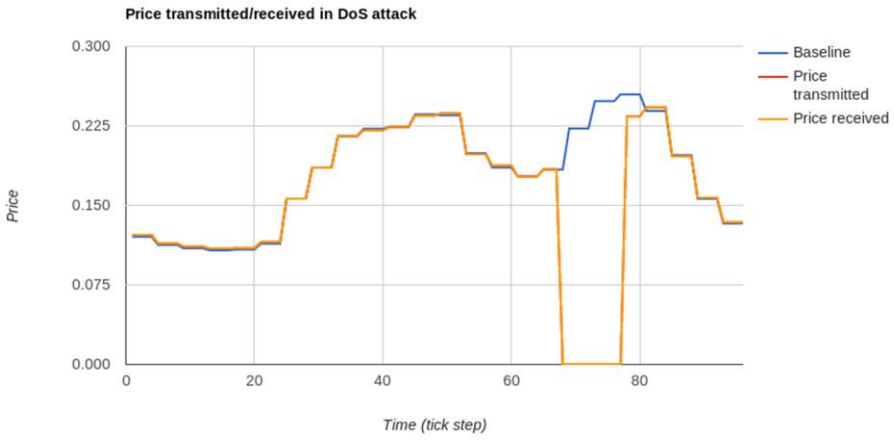

Figure 31: *Price signal throughout a day under a Dos attack on high peak hour.*

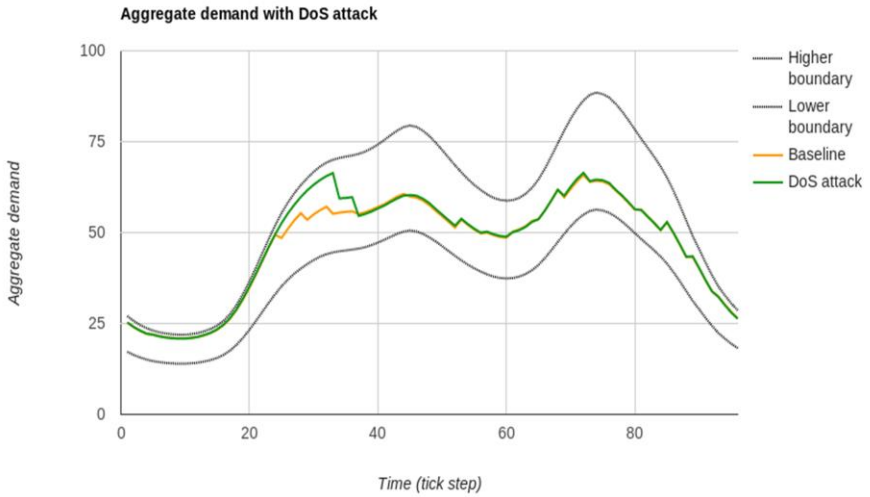

Figure 32: *Aggregate demand of the system plot for a day under DoS attack. The x-axis indicate the day in 96 time steps whereas the y-axis indicate the aggregate demand. The yellow line indicates the baseline scenario. The attack launches in low peak hour (green line).*

Overall, the results show that the attacks largely affect the system; during their occurrence the price signal is not transmitted/received (the transmitted and received prices have the same values) (Figures 31 and 33). Furthermore, the time for recovery of the system is the same for both attacks. The price signal immediately returns to its normal state and follows the baseline scenario. Also, during the attack the households increase their demand as the price they have received before the attack is constant (Figures 30 and 32). Hence, this state could have serious implications for the system, due to the increased aggregate demand. The immediate recovery of the server leads to the healthy state of the system, because it forces households to reduce their demand.

The assumption of using last received price may affect the outcome of these attacks. To check this, we consider additional scenarios where the DoS attack starts in several times of the day. More specifically, we run ten independent scenarios under DoS attack in different times, starting from hour 2 till hour 20 with step 2. The results show that aggregate demand varies with regards to current received price. In cases where the last received price is smaller than the price households are supposed to receive, then the demand increases, whereas when the price is higher, then the demand lowers (Appendix I). This behavior indicates that the DoS attack is partially affected by the time of the day and the subsequent values of price compared to the last received price.

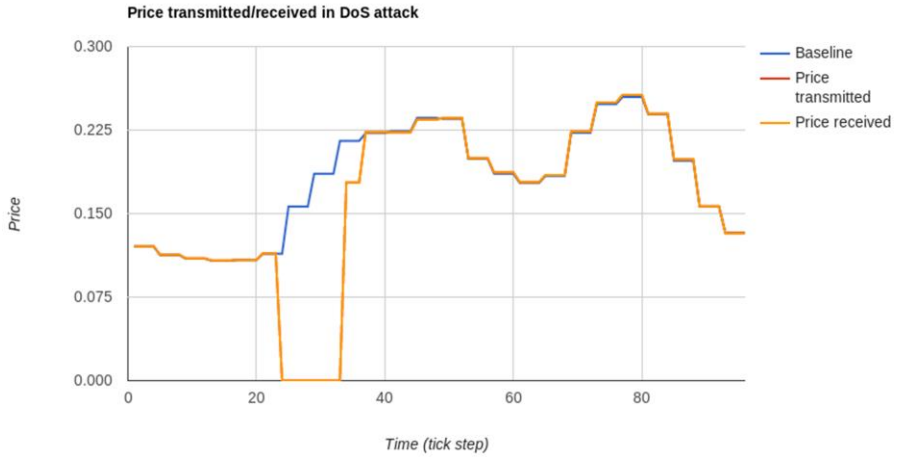

Figure 33 *Price signal throughout a day under a Dos attack on low peak hour.*

4.3 Scale of Man-in-the-middle attack

To investigate the effects of different scales of integrity attack on the price signal and the aggregate demand we run the simulation for the model for the scenario under attack. Each scenario runs within one day and in 30 replications and different fraction of affected households is used (5%, 50%, and 90%). From the 30 replications the median curves is extracted.

When a fraction of households are affected and receive the false price by the attacker the households that receive the proper price are affected implicitly. And this because the server calculates the price based on the aggregate demand of the system, indicating that the higher demand of the affected households increases the price transmitted to the other households. In Figure 34, the percentage of the deviation from the received price in the baseline scenario of the received price by non-affected users when the system is under attack is shown. The trend of the plots supports the former statement. Ultimately, the fraction of the affected households is a negative factor for the normal price the non-affected households receive.

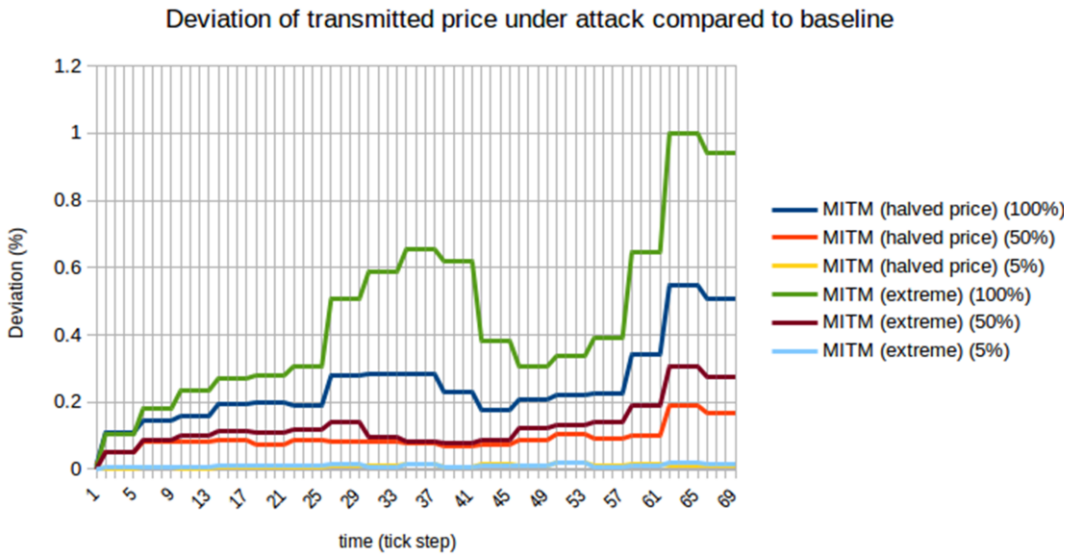

Figure 34 *The percentage of the deviation from the received price in the baseline scenario of the received price by non-affected users when the system is under attack.*

Depending on whether households are directly affected (receive false price) or not by the attack, they demand different values of energy. The affected households tend to increase their consumption because they receive reduced price by the attacker. In particular, Figure 35 shows the average deviation of the demand of an individual smart meter in high peak hours from the baseline scenario. The individual smart meters are taken from six different scenarios where the effect (half price, extreme) and the fraction (5%, 50%, 90%) of affected smart meters vary. For each scenario we calculate the average deviation for affected and not affected households. We exclude the scenarios with fraction of 100% because the results are not indicative. The results show that two factors influence the deviations: the number of affected households and the false price the attacker sends. With the increase of the fraction, the demand of not affected smart meters gradually drops. The not affected households are implicitly affected by the aggregate demand of the system, which increases proportional to the number of affected households. So, the server increases the real time price to succeed less aggregate demand, but only the not affected smart meters react on this. For the latter factor, the effect is more straightforward. Regardless of the fraction of the affected households, individual affected households increase their demand in accordance with the price they receive. Thus, lower prices result into higher demand values for the affected households. Consequently, these higher values of demand lead to lower demand values for the not affected households.

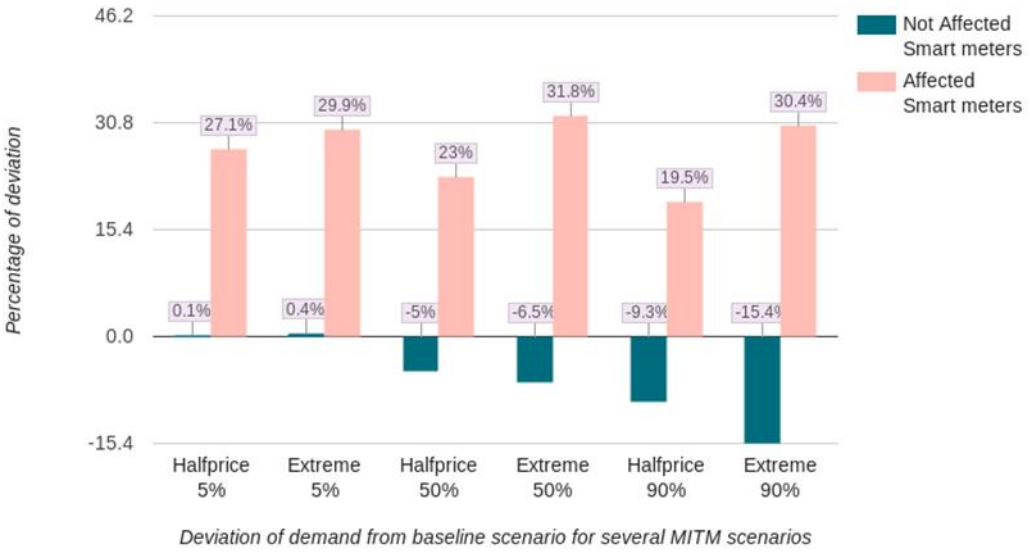

Figure 35 *Deviation of demand form baseline scenario for several MITM scenarios*

5 CONCLUSIONS AND RECOMMENTATIONS

In this chapter, the major conclusions and insights that were gained from the previous sections of this thesis are summarized. Therefore, in first sections the research question and sub-questions are answered and the contribution is defined. Hereafter, the derived conclusions of this thesis are used for formulating recommendations for decision-makers respectively for each key stakeholder of the system.

5.1 The fundamental goal: answering the research questions

Nowadays, Smart Grid promises to replace the existing traditional power grid with the integration of advanced communication technologies and providing a more effective and reliable next generation power grid. Due to the fact that most of these technologies are based on ICT tools and many automated electronic devices (such as smart meters) are inter-connected via communication networks throughout critical resources of Smart Grid, their integration makes the Smart Grid vulnerable to cyber-attacks. So, parts of the Smart Grid communication network, such as heterogeneous electronic devices and network architecture could be vulnerable points for attackers. Cyber-attacks can have an instantaneous impact on basic security objectives of such a critical infrastructure. Availability and integrity are two of the main security objectives and constitute the basis of information security. Thus, their disruption could result in serious consequences for the Smart Grid. Thus, by recognizing the necessity for a secure critical infrastructure that will provide efficient and secure information delivery throughout the Smart Grid a deeper research on Cyber security is needed. There is a demand of new researchers on cyber security, which is not fully deployment yet in Smart Grid and during the next years, can shed light in the research for Smart Grid security.

As stated before, Smart Grids are vulnerable to numerous physical and cyber-attack as a result of communication and computation vulnerabilities engaged in the grid. The growth of an efficient and secure Smart Grid requires a deeper understanding of possible impacts resulting from effective cyber-attacks. This thesis examined two different types of cyber-attacks on DR system of Smart Grid communication and metering infrastructures. More specifically, in this thesis we studied two types of cyber-attacks which target the integrity and the availability in Smart Grid by manipulating the data exchange between its main components. In the first case, the attacker alters the content of the data and the integrity is violated. In the second type of the examined cyber-attack, the attacker either blocks or delays the data delivery and the availability is violated. In order to address how cyber-attacks can influence the outcomes of DR, regarding the energy prices and the power demand a simulation model were constructed to test system behaviors under different conditions. The simulation results for the different scenarios provide insights in the implications of cyber-attacks on power demand and price signals when DR programs are used in Smart Grid.

The research work was conducted to answer the main research question, *"What are the implications of integrity and availability cyber-attacks to price signal on DR programs and subsequently how does this affect the power demand in the Smart Grid?"*.

1. *"What is the effect of different types of cyber-attacks in the received price signal of the Real Time pricing (RTP) program?"*

This research question was addressed, by the analysis of the simulation results. During DoS attack, the price is

not transmitted, therefore, it is zero for that period. However, this behavior does not affect the system entirely, because households continue to demand energy based on the last received price. On the other hand during the man-in-the-middle attack, the received price deviates from the transmitted price at attacker's will, thus the affected households effect's degree depends solely on the attacker's will and ability.

2. *"What is the impact of cyber-attacks on consumers' energy consumption during peak hours when using the RTP program?"*
This research question again is answered based on the simulations results of the model. From the nature of the Agent Based Model, and because each agent attempts to maximize their welfare at every simulation step, the balance among operation cost, real time price and demand during peak hours leads the demand and consequently the consumption of the households in lower values compared to a fixed price program (e.g. the generated synthetic profiles). This can be explained by the fact that in high peak hours the operation costs for the utility are higher, due to higher aggregate energy consumption in general. Thus, in real price program server is able to update the price based on its current state. Server sets this price in order to maximize its welfare (i.e. minimize costs) in the future steps. Consequently, households adjust their consumption in accordance to the real price and their needs in order to maximize their welfare. We observe an average 17% reduction of the consumption in high peak hours with the use of RTP compared to the default generated profiles. This indicates that, with the RTP program the health of the system can be sustained more efficiently.

The scenarios for the system under DoS attack show that users increase their energy demand. During the attack the demand increased by an average of 9.6%. This indicates that since the real time price is not transmitted during the attack, the households further on kept the energy demand based on previously received price. In the model, we assume that the DoS attack does not brought down the entire system. Even though the server for demand response is unavailable, the flow of energy do not stop (i.e. energy grid is not directly affected) and households continue to demand energy. Thus, a potential DoS attack may affect the consumption and households demand for more energy. On the other hand, the scenarios for the system under MITM attack indicate that households are highly affected by the attack. Depending on false received price value households increase their energy demand accordingly, resulting in higher costs for them.

3. *"How do different magnitudes of an integrity attack affect the received price and the power demand?"*
When a fraction of households are affected and receive the false price by the attacker, households that receive the proper price are affected implicitly. This because the server calculates the price based on the aggregate demand of the system, indicating that the higher demand of the affected households increases the price transmitted to the other households. The higher the fraction of the affected households is the higher the effect on the received price is. Depending on whether they are directly affected (receive false price) or not by the attack, households demand different values of energy. The affected households tend to increase their consumption because they receive reduced price signals by the attacker. Subsequently, these higher values of demand lead to lower demand values for the not affected smart meters.

Ultimately, from the insights gained from the previous sub-questions, we are able to answer the main research question of the thesis. The conducted research indicates that integrity and availability cyber-attacks have great

impact on the price and demand signals when an RTP program is used. We observed that under the integrity attack the price changes at attacker's will, and apart from the directly affected households, a number of households is affected indirectly. The false price signals lead the affected households to demand more energy, which in turn affect the behavior of the whole system leading to undesired situations, i.e. increasing energy price and fluctuations of energy demand. Nevertheless, the magnitude of the attack is an essential factor since the larger the number of affected households, the larger the implication on the system. We observed an average demand increase of 25% for the affected households. The demand for the non-affected households reduced from 5% to 15% depending on the magnitude of the attack, which affects the price, varying in range 12% and 36% increase, except for the attack on the smallest fraction (5%), where the influence on the total price was negligible. In the case of availability attack, the system is less affected compared to the integrity attack. This may partially be influenced by the mitigation schema we decided to use; households use the last received price in order to calculate their demand during the attack. With this mitigation schema and because the duration of the attack is shorter compared to integrity attack, the system is affected only in specific hours of the day; during high peak hours and more importantly in the transitions between the peaks. This is crucial because households would demand more energy in high peak hours while they use the lower price they received in the med-peak hour before the attack occurs. Even though, this attack is short we observed an increase demand up to 15% for a specific time where the last received price differed nearly 30% from the hypothetical price for that moment.

5.2 Discussion of results

In this thesis project, we explored the implications of potential cyber-attacks on Smart Grid; a critical infrastructure. More specifically, we focus on the impact of attacks on the RTP program and the communication between utility server and households; the price and the demand signals. Even though the available literature to some extent analyzed the DR pricing mechanisms as an important factor that influences consumers' energy consumption, it does not give any insights on how different types of cyber-attacks can influence the outcomes of DR and indirectly the consumers' behavior. So, we sought to cover this gap.

To do so, we implemented an ABM to simulate the Smart Grid and the potential attacks. For modeling the cyber-attack scenarios on the DR program, an agent-based modeling approach was chosen deliberately. This approach readily allowed to account for the heterogeneity of the components of the system. The Smart Grid components were modeled as individual agents with their autonomous decision patterns. The interaction of agents with one another evolves the overall behavior of the system. Since, the objective of the model was to study consequences of cyber-attacks on smart grid, the attacker's capabilities to penetrate the system was not explicitly modeled. This allowed to simplify the model and make it more focused on the for the study relevant system aspects. The Real Time Pricing (RTP) program is chosen as a part of price based DR program, since its periodicity of the signals among the different components of the system facilitates the existence of a potential cyber threat in the system that could largely affect the system. RTP is implemented based on a distributed algorithm that finds the optimal energy consumption for the households, the optimal price values that the utility server communicates and the optimal generating capacity for the utility server. So, in a normal situation, where households demand desired energy and server is capable to provide energy, the system is stable. To disrupt this stability, cyber-attacks come

into play. During the simulations, the communication of price signal is affected by DoS and man-in-the-middle attacks.

We found that the attacks largely affect the system. More specifically, during the DoS attack, the price is not transmitted; therefore, it is zero for that period. This behavior does not affect the system entirely. On contrary to study by Asri Satin et al. (2015) where they assume that the system is brought down during the attack, here we assume that electricity grid and communication network are separate systems. So, the households continue to demand energy based on the last received price. In our simulations, this results into increasing energy demand by the households on specific hours during the day; for example, during the transitions between the different peaks in particular, we observe an increase up to 15%. In other hours we also observe demand reduction due to the price difference between last received and the hypothetical price for the same time. Other assumptions, for example the use of a fixed price mechanism, may lead to different behaviors. During the man-in-the-middle attack, the received price deviates from the transmitted price at attacker's will, thus the effect degree on the affected households depends solely on the attacker's will and ability, although we do not model attacker's capability of penetrating the system. It is worth noting that even when only a fraction of households is affected, the households that receive the proper price are affected implicitly. This is because, in the simulations, the server calculates the price based on the aggregate demand of the system, indicating that the increased demand of the affected households increases the price transmitted to the non-affected households. Considering the demand, the man-in-the-middle attack effect depends on whether households are directly affected or not by the attack. The affected households tend to increase their consumption because they receive reduced price signals by the attacker. On the other hand, the non-affected smart meters are implicitly affected and tend to reduce their consumption, since they receive increased energy prices.

The scale of the man-in-the-middle attack, in terms of number of affected households, is a factor that affects the outcomes of the simulations. The results indicate that the higher the fraction of the affected households is, the higher the effect on the price and the demand is. With the increase of the fraction, the demand of non-affected households drops. The non-affected households are implicitly affected by the aggregate demand of the system, which increases proportional to the number of affected households. So, the utility server increases the real time price to succeed less aggregate demand, but only the non-affected households react to it.

Overall, our results confirm the initial hypothesized behavior of the aggregate load during a cyber-attack (load shifting – see Figure 3). When the attack occurs the aggregate demand increases as households tend to increase their demand on lower prices. We observe an increase of 15% and ~30% on the demand during DoS and MITM attack respectively. The affected households shift their loads to the period that is most favor for them. However, the load shifting is not clear in our simulations. This happens because the load profiles are restricted to certain boundaries, so it is impossible to observe apparent shifts between different peak periods. Only after the attack there is a steep drop of the demand which quickly returns to the normal state.

Even though the findings of this thesis have a scientific contribution, a number of assumptions may limit the potential capabilities of the simulation model. The energy consumption for the households is based on standard

demand profile patterns. So, the consumption of the households is restricted and driven by certain consumption boundaries. A more realistic approach would be to model appliances for each household. In this way, households would be able to shift their demand by switching on and off appliances. The minimum and maximum demand for a household would not follow a certain pattern for a set of households, resulting in a more accurate heterogeneity of the agents. However, due to time restrictions and the complexity of such approach we decided to simplify the default demand patterns. Also, the results of attacks were indicative even with the simplified approach. In addition, the use of household types is constrained only to annual demand and the proportion of occupancy on the Smart Grid. Other assumptions, for example psychographics (such as lifestyle, personality, etc.) of consumers, are not taken into account. These would lead to a more accurate heterogeneity of the households as well. Finally, the distributed algorithm that used for the RTP mechanism considers that households always seek to maximize their satisfaction; consumers are price takers who receive price as fixed parameter. Samadi et al. (2012) argue this assumption is not valid for systems with built-in automated control units and they propose a solution where consumers can anticipate the impact of their actions on price values. This approach would increase the complexity of the model since a set of parameters needs to be defined for the incentives of the consumers.

5.3 Recommendations for stakeholders

Finally, Smart Grid is a multi-actor system and different stakeholders are involved and affected when choosing the price-based program of DR and a cyber-attack is launched into the system. Thus, after the conclusions of this thesis, recommendations for each of the involved stakeholders are provided in the next section.

Consumers: Consumers are residential, households and groups of people, who should be able to make informed decisions about the adaptation of time-varying rates such as price-based demand response. By using DR programs, consumers are able to analyze and decline their electricity consumption in order to gain benefits and minimizing their costs (Gasparin, 2013). The results shown that, consumers are influenced directly by the cyber-attacks, as they receive false price signals and they adapt their energy consumption based on them. They increase their energy demand when fake prices are transmitted to them due to cyber attacks, which results in extra costs for them. In addition, a number of consumers are implicitly affected by the MITM attacks with large magnitude, where the price is increasing due to the increasing demand of the affected consumers. Due to these results and the diversity of consumers that are use smart meters better awareness is needed through training programs and seminars that will make consumers to understand better how to turn information into energy savings and at the same time protect their data from cyber-attacks. In addition, targeted training can provide information on how to respond immediately appropriately in a case of an attack (Mayer & Rupy, 2015). Furthermore, consumer involvement with the smart ICT technologies is essential but also their cyber awareness about the risks of cyber-attacks and how to avoid them are critical.

Utilities: According to the main findings of this thesis, utility companies are affected by cyber-attacks in a way that the stability of Smart Grid is disrupted. In cases when the utility is incapable to provide the demanded energy due to a cyber-attack the whole system is unstable, as the utility miscommunicate with the smart meters (Figure 27). As it was already stated in the literature review, the exchange of information between utilities and consumers about the amount of consuming energy increased significantly the adoption of the ICT technologies in Smart Grid. Utility companies should abide by government's security standards such as Critical Infrastructure Protection (CIP) with the aim to protect from cyber attacker the big amount of information that transferred from and to smart meters (European Commission, 2016). Installation and the implementation of technologies that will control and secure the communication links into the interconnected network and they authenticate the identity of each smart meter in the system are obligatory. Because we observed that even if the half of the smart meters in the system is compromised by an attacker, this has an impact in the whole system. Finally, the system that utility companies will use should be developed under the umbrella of cyber security and detection of cyber-attacks.

Policy makers: Policy makers should develop and adopt the appropriate legal frameworks, cyber-security standards and protocols by adhering to the important goal of ensuring Smart Grid cyber security. By implementing transparent and comprehensible protocols policy makers will make an essential contribution to the widespread acceptance of demand response and other smart grid technologies. Further, establishing a register for monitoring cyber-attacks on Smart Grids would be an important step to raise awareness for the problem and disseminate best practices. Regular, existing processes and policies need to be reviewed and where needed

updated taking into account the findings for the impact of cyber-attack in a critical infrastructure, such as the Smart Grid. According to the results of this thesis, policy makers should develop the appropriate mitigation strategy in order to deal with the DoS attacks when RTP mechanism is implemented and no price signal is transmitted to smart meters. From the results we show that RTP policy is vulnerable to cyber attacks due to continuous up-to-date data that should be transferred through the Internet. Thus, it is important for the policy makers to examine if this policy should be implemented in large scale in real world and if yes, which strategies should be followed for its successful implementation.

Technology providers/ICT companies: This thesis shows that a cyber-attack targeted at the information exchange in a Smart Grid, can disrupt the operation of the system significantly and can have long-lasting negative effects. As a consequence, technology providers should protect themselves against cyber attacks and develop and deliver a system that is resilient to cyber-attacks and retain its core functions even in times of a massive cyber-attack. More specifically, ICT companies should be to develop and deploy systems able to maintain the benefits of demand response by implementing the mandatory security standards and other measurements against cyber-attacks.

6 LIMITATIONS, FUTURE WORK AND REFLECTION

LIMITATIONS

Due to the fact that RTP mechanism is not yet implemented broadly and also because the data from cyber-attacks are not available in public because of privacy and reputation reasons there is a number of limitations regarding this research work and the implemented simulation model. Thus, lack of data accessibility and time limitations of this research concluding in some limitations that are presented in this section.

Limitations of this research work & simulation model:

Due to the lack of real data and the information privacy issues concerning RTP, for the analysis a synthetic profiles database is used. Even though the simulation results can be partly validated through literature review, further validation with historic data, when they will be provided, is still needed. Moreover, during the design of this model, time limitations drove us to simplify the simulation process with the use of some assumptions. A more advanced implementation, with greater details, could be used with the aim to keep the efficiency of the simulation results by exceeding the scope and purpose of this work. For example, by adding more attributes to the agents (e.g. adding probabilistic behavior models in attackers). Also, the households could be classified in more than 3 different types based on various factors. In this thesis, a classification was made to represent sufficiently the real world. The three chosen households types (1 person, 2/3 persons and 4+ persons) was constructed for the purpose of this research. However, every household should be of a unique type, which means each of the households' type have to be modeled individually which is not possible to happen.

FUTURE WORK

Taking into account the limitations of the research work in this thesis, a number of suggestions for future work are shown as following:

Firstly, due to the time limitations and the lack of data due to privacy reasons the validation of the model became only based on the literature review. So, a deeper validation could be succeeding with the use of really data from companies applied the RTP mechanisms and are victims of cyber-attacks that could be available after a privacy agreement in the future. Other suggestion, as concern as the model, is the implementation of different appliances such as refrigerators, kettles, TV, washing machines etc. for each household. Through this implementation, the total amount of demand could be more accurate and the load could be well defined. In a case of a cyber-attack, the consequences could be more apparent due to the scheduling of the various appliances (when they will switch ON or OFF) due to a day. One more important suggestion for further research could be to extend our model in order to give to consumers more incentives expect of the price signals, which can influence their energy consumption, such as the use eco-friendly devices which will consume less energy (so, lower demand) and will contribute to the reduction of their bills and to protection of the environment.

In this thesis of the implications that can be achieved by two different types of cyber-attack on price signals and on demand curve are examined. Next step of the research could be the investigation of mechanisms on how to protect the system from the data manipulation (man-in the middle attack) and the availability of DR properties/resources (DoS attack), which violate the security objectives integrity and availability in Smart Grid. For a more detailed analysis of DR programs in Smart Grid and the consequences of cyber-attacks on their processes, the use of interviews, with households or utilities companies that are already victims of these types of attacks, are recommended. A final idea for future research would be to use the adaptability of the model and to extent it apart from the residential sector by adding more system components to commercial and industrial sector. Also, to add in the existing model other types of cyber-attacks and to evaluate their impact and also to find out cyber security solutions for mitigating the attacks to communication network.

REFLECTION

At the beginning, everything was so vague in my mind. The only thing that I knew it was that I wanted to do something that it would be really helpful for researchers around the world. But at the same time, it was too difficult for me to narrow my thesis' scope and to understand that due to the time limitations it was not possible to do everything that I was willing. After my Kick off meeting, and the advice from my committee I took the choices and I knew exactly what I was willing to do and how. That was the first time that I really felt relief during this process.

In the initial stage of my thesis, my motto was "the more you know the better for you". So, I read a huge amount of papers to learn what I was able to learn about Smart Grids, cyber-attacks, simulation models and all the relevant topics. But after reading all these papers, I was lost and I did not know which information I would use in my thesis. This process caused a delay because I understood that it was necessary to read the most interesting papers again with a more critical view the in order to write my literature review and to continue to the next steps.

However, the modeling process always takes time and I do not think that there is an easy way for someone to do it faster. I was starting to think which software I would use for the implementation of my idea. It was really

important the chosen software to satisfy my research objectives. So, after a discussion with my first supervisor and some research, I concluded that the best way to achieve my research goal was to develop the model into a simulation model using Python3 in Mesa software. This was the most time consuming part of the thesis and I was not always able to keep a good working flow. The step of the data analysis was one of the most interesting parts of the thesis. I was really happy to realize that my work paid off and the results of my thesis recompense me and may provide valid insights for future work.

One of the main obstacles of this thesis was to write the final report. Even if, I had all the information that I was needed and my model was done, it was so difficult for me to start writing my report. I was afraid that I was not able to write a clear and understandable report for the readers. I finally succeed it because I was really interested on the topic, that I chose, and also, because my supervisor gave me the opportunity to send him my draft parts of the report and he always encouraged me.

During the process of my thesis, I regularly had meetings with my first supervisor. Through our discussions, I gained many valuable insights that they had a great impact on my work. Also, these meetings helped me a lot to find solutions when I was stuck through the process and to find again my motivation. Moreover, his advice and guidelines contribute to surpass any difficulties that I faced. I am honestly grateful for the effort my supervisor gave to these meetings.

In conclusion, I can say that this thesis was the most important achievement in my whole life till now. It was really interesting to work in the totally new fields of the Energy and Cyber security and to gain so much knowledge on them. In my future plans, I will definitely use all the knowledge and experience that I gain to protect the critical infrastructures and to find a position in the Cyber security community.

References

Albadi, M. H., & El-Saadany, E. F. (2007). Demand response in electricity markets: An overview. In *Power Engineering Society General Meeting, 2007. IEEE* (pp. 1–5).

APCS. (2017). Synthetic load profiles. Retrieved from http://www.apcs.at/en/clearing/physical-clearing/synthetic-load-profiles

Asri, S., & Pranggono, B. (2015). Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure. *Wireless Personal Communications*, *83*(3), 2211–2223. https://doi.org/10.1007/s11277-015-2510-3

Bhatt, J., Shah, V., & Jani, O. (2014). An instrumentation engineer's review on smart grid: Critical applications and parameters. *Renewable and Sustainable Energy Reviews*, *40*, 1217–1239. https://doi.org/10.1016/j.rser.2014.07.187

California Energy Commission, C. (2014). Public Interest Energy Research 2013 Annual Report, (April).

CBS. (2015). Huishoudens; grootte, positie in het huishouden, 1 januari 1995-2013. Retrieved from http://statline.cbs.nl/StatWeb/publication/?DM=SLNL&PA=37312&D1=a&D2=a,!1-4,!6-7&HDR=G1&STB=T&VW=T

Chambers, D., & Gravely, M. (2012). Interim Project Report Smart Grid Cyber Security Potential Threats ,. *Pier*, *CEC-500-20*(May), 93.

Chiesa, R. (2010). HPP – The Hackers Profiling Project. Retrieved March 10, 2017, from https://www.chmag.in/articles/special-feature/hpp-the-hackers-profiling-project/

Clements, S., & Kirkham, H. (2010). Cyber-security considerations for the smart grid. In *IEEE PES General Meeting* (pp. 1–5). IEEE. https://doi.org/10.1109/PES.2010.5589829

Cleveland, F. M. (2008). Cyber security issues for advanced metering infrasttructure (AMI). In *Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE* (pp. 1–5).

Council, W. E. (2016). World Energy Council. Retrieved April 16, 2017, from https://www.worldenergy.org/

Dam, K. H., Nikolic, I., & Lukszo, Z. (2013). *Agent-Based Modelling of Socio-Technical Systems*. (K. H. Dam, I. Nikolic, & Z. Lukszo, Eds.). Dordrecht: Springer Netherlands. https://doi.org/10.1007/978-94-007-4933-7

Deconinck, G., Delvaux, B., De Craemer, K., Qui, Z., & Belmans, R. (2017). *Study of smart meters from the angels of the cosumers protection and public service obligations*. Belgium.

Douw, J. V, Lukszo, Z., & Herder, P. M. (2016). Incentivising consumers in smart grids to shift their electricity use. In *Networking, Sensing, and Control (ICNSC), 2016 IEEE 13th International Conference on* (pp. 1–6).

Epstein, S. D., & Seely, T. D. (2006). *Derivations in minimalism* (Vol. 111). Cambridge University Press.

European Commission. (2016). *Secure societies – Protecting freedom and security of Europe and its citizens*. Retrieved from http://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf

Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart Grid — The New and Improved Power Grid: A Survey. *IEEE Communications Surveys & Tutorials*, *14*(4), 944–980. https://doi.org/10.1109/SURV.2011.101911.00087

Federal Energy Regulatory Commission. (2008). *Assessment of Demand Response and Advanced Metering*. Retrieved from http://www.ferc.gov/legal/staff-reports/12-08-demand-response.pdf

Flick, T., & Morehouse, J. (2011). *Securing the Smart Grid. Securing the Smart Grid*. Elsevier. https://doi.org/10.1016/B978-1-59749-570-7.00015-7

Gasparin, F. (2013). Smart Grid Systems, 40.

Gelazanskas, L., & Gamage, K. A. A. (2014). Demand side management in smart grid: A review and proposals for future direction. *Sustainable Cities and Society*, *11*, 22–30.

Gellings, C. W. (1985). The concept of demand-side management for electric utilities. *Proceedings of the IEEE*, *73*(10), 1468–1470.

Ghansah, I. (2009). Smart Grid Cyber Security Potential Threats, Vulnerabilities And Risks. *California Energy Commission, PIER Energy - Related Environmental Research Program*, *CEC-500-20*.

Gungor, C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2013). A survey on smart grid potential applications and communication requirements. *IEEE Transactions on Industrial Informatics*, *9*(1), 28–42.

Gungor, V., Lu, B., & Hancke, G. P. (2010). Opportunities and Challenges of Wireless Sensor Networks in Smart Grid. *IEEE Transactions on Industrial Electronics*, *57*(10), 3557–3564. https://doi.org/10.1109/TIE.2009.2039455

Herring, A. (2016). How Energy Companies Can Manage the Growing Threat of Cyber-Attack. Retrieved from

https://www.marsh.com/uk/insights/risk-in-context/how-energy-companies-can-manage-the-growing-threat-of-cyber-attack.html
Hull, J., Khurana, H., Markham, T., & Staggs, K. (2012). Staying in control. *IEEE Power & Energy Magazine*, *10*(february), 41–48. https://doi.org/10.1109/MPE.2011.943251
Kalogridis, G., Efthymiou, C., Denic, S. Z., Lewis, T. A., & Cepeda, R. (2010). Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures. In *2010 First IEEE International Conference on Smart Grid Communications* (pp. 232–237). IEEE. https://doi.org/10.1109/SMARTGRID.2010.5622047
Kazil, J., & Vērzemnieks, N. (2014). Mesa. Retrieved from https://github.com/projectmesa
Koliou, E. (2016). *Demand Response Polices for the Implementation of Smart Grids*. Delft University of Technology.
Lättilä, L., Hilletofth, P., & Lin, B. (2010). Hybrid simulation models--when, why, how? *Expert Systems with Applications*, *37*(12), 7969–7975.
Mahalingam, A. (2013). Modeling of residential demand response of smart electricity grids to day ahead markets.
Mayer, R., & Rupy, K. G. (2015). COMMENTS OF THE UNITED STATES TELECOM ASSOCIATION, *20005*(202).
Mwasilu, F., Justo, J. J., Kim, E.-K., Do, T. D., & Jung, J.-W. (2014). Electric vehicles and smart grid interaction: A review on vehicle to grid and renewable energy sources integration. *Renewable and Sustainable Energy Reviews*, *34*, 501–516.
NESCOR. (2015). Electric Sector Failure Scenarios and Impact Analyses – Version 3.0, (December). Retrieved from http://smartgrid.epri.com/doc/NESCOR Failure Scenarios v3 12-11-15.pdf
Nibud, B. (2017). RVO 2017. Retrieved March 5, 2017, from https://www.nibud.nl/consumenten/energie-en-water/
North, M. J., Collier, N. T., Ozik, J., Tatara, E., Altaweel, M., Macal, C. M., … Sydelko, P. (2013). Complex Adaptive Systems Modeling with Repast Simphony. Retrieved from http://www.casmodeling.com/content/1/1/3
Palensky, P., & Dietrich, D. (2011). Demand side management: Demand response, intelligent energy systems, and smart loads. *IEEE Transactions on Industrial Informatics*, *7*(3), 381–388.
Pearson, I. L. G. (2011). Smart grid cyber security for Europe. *Energy Policy*, *39*(9), 5211–5218. https://doi.org/10.1016/j.enpol.2011.05.043
Perez, F., Granger, B. E., & Hunter, J. D. (2011). Python: An Ecosystem for Scientific Computing. *Computing in Science & Engineering*, *13*(2), 13–21. https://doi.org/10.1109/MCSE.2010.119
Queiroz, C., Mahmood, A., & Tari, Z. (2011). SCADASim — A Framework for Building SCADA Simulations, *2*(4), 589–597.
Samadi, P., Mohsenian-Rad, A.-H., Schober, R., Wong, V. W. S., & Jatskevich, J. (2010). Optimal Real-Time Pricing Algorithm Based on Utility Maximization for Smart Grid. *2010 First IEEE International Conference on Smart Grid Communications*, 415–420. https://doi.org/10.1109/SMARTGRID.2010.5622077
Samadi, P., Mohsenian-Rad, H., Schober, R., & Wong, V. W. S. (2012). Advanced demand side management for the future smart grid using mechanism design. *IEEE Transactions on Smart Grid*, *3*(3), 1170–1180. https://doi.org/10.1109/TSG.2012.2203341
Sgouras, K. I., Birda, A. D., & Labridis, D. P. (2014). Cyber attack impact on critical Smart Grid infrastructures. In *ISGT 2014* (pp. 1–5). IEEE. https://doi.org/10.1109/ISGT.2014.6816504
Sridhar, S., Hahn, A., & Govindarasu, M. (2012). Cyber–Physical System Security for the Electric Power Grid. *Proceedings of the IEEE*, *100*(1), 210–224. https://doi.org/10.1109/JPROC.2011.2165269
Standards for security categorization of federal information and information systems. (2004). Gaithersburg, MD. https://doi.org/10.6028/NIST.FIPS.199
U.S. Department of Commerce. (2010). *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0*.
Wang, W., & Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, *57*(5), 1344–1371. https://doi.org/10.1016/j.comnet.2012.12.017
Wilensky, U. (1999). NetLogo. Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL. Retrieved from http://ccl.northwestern.edu/netlogo/
Wissner, M. (2011). The Smart Grid--A saucerful of secrets? *Applied Energy*, *88*(7), 2509–2518.
Worm, D., Langley, D., & Becker, J. (2015). Modeling interdependent socio-technical networks: The smart grid—an agent-based modeling approach. In *Simulation and Modeling Methodologies, Technologies and Applications* (pp. 87–100). Springer.

Appendix I

Time (tick)	Price (%)	Demand (%)	Time (tick)	Price (%)	Demand (%)	Time (tick)	Price (%)	Demand (%)
Hour 2			**Hour 4**			**Hour 6**		
8	0,75	0,8	16	-1,48	-0,71	24	-4,37	0,95
9	0,75	0,83	17	-1,48	-0,52	25	-4,37	0,92
10	0,75	0,98	18	-1,48	-0,33	26	-4,37	1
11	0,75	1,12	19	-1,48	-0,28	27	-4,37	0,96
12	0,46	0,83	20	-6,77	0,8	28	-13	4,12
13	0,46	0,8	21	-6,77	1,04	29	-13	4,22
14	0,46	0,8	22	-6,77	0,84	30	-13	4,35
15	0,46	0,76	23	-6,77	0,93	31	-13	4,46
16	-1,03	0,65	24	-10,84	3,65	32	-25,34	10,37
Hour 8			**Hour 10**			**Hour 12**		
32	-14,19	5,5	40	-1,16	0,43	48	-1,45	2,14
33	-14,19	5,55	41	-1,16	0,35	49	-1,45	2,2
34	-14,19	5,59	42	-1,16	0,23	50	-1,45	2,13
35	-14,19	5,59	43	-1,16	0,05	51	-1,45	2
36	-17,29	8,82	44	-5,11	-0,12	52	15,76	-4,13
37	-17,29	8,83	45	-5,11	-0,23	53	15,76	-4,15
38	-17,29	8,89	46	-5,11	-0,27	54	15,76	-4,14
39	-17,29	9,01	47	-5,11	-0,4	55	15,76	-4,07
40	-18,26	9,31	48	-6,49	1,27	56	26,25	-7,76
Hour 14			**Hour 16**			**Hour 18**		
56	9,06	-3,93	64	-3,93	1,85	72	-10,98	5,37
57	9,06	-3,79	65	-3,93	1,81	73	-10,98	5,39
58	9,06	-3,63	66	-3,93	1,75	74	-10,98	5,33
59	9,06	-3,52	67	-3,93	1,65	75	-10,98	5,23
60	13,17	-5,62	68	-20,46	10,22	76	-13,52	5,73
61	13,17	-5,49	69	-20,46	10,05	77	-13,52	5,47
62	13,17	-5,35	70	-20,46	9,89	78	-13,52	5,1
63	13,17	-5,24	71	-20,46	9,66	79	-13,52	4,76
64	8,72	-3,94	72	-29,19	15,56	80	-5,24	2,75
Hour 20								
80	9,57	-2,21						
81	9,57	-2,45						
82	9,57	-2,69						
83	9,57	-2,84						
84	28,77	-9,04						
85	28,77	-8,99						
86	28,77	-8,89						
87	28,77	-8,75						
88	47,67	-15,33						

Figure A 1: Results from ten independent DoS attack scenarios on different time during a day. The values for the price and the demand show the deviation from the values of the baseline scenario. The general observation is that when the price percentage is negative (i.e. smaller than the baseline value) then the demand is positive (higher than the one of the baseline scenario) and vice versa.