Literature Review on Smart Grid Cyber Security

Todd Baumeister
Collaborative Software Development Laboratory
Department of Information and Computer Sciences
University of Hawai‘i
Honolulu, HI
baumeist@hawaii.edu

December 2010

Contents

Abstract

The current U.S. electrical power grid is an out-of-date infrastructure, and the Smart Grid is an upgrade that will add many new functionalities to meet customers' new power requirements. Updating a system as complex as the electrical power grid has the potential of introducing new security vulnerabilities into the system. This document presents a review of the work related to Smart Grid cyber security. The work reviewed is separated into five categories that make up different components of the Smart Grid: Process Control System (PCS) Security, Smart Meter Security, Power System State Estimation Security, Smart Grid Communication Protocol Security, and Smart Grid Simulation for Security Analysis. The Smart Grid is a large complex system, and it still requires a lot of cyber security design work.

Chapter 1

Introduction

The current U.S. electrical power grid is an out-of-date infrastructure. It has met our needs in the past; however, as our society advances technologically so do the expectations we have of our electrical power delivery system. The Smart Grid is a movement to bring the electrical power grid up to date so it can meet the current and future requirements of its customers. Updating our electrical power grid could introduce new security vulnerabilities into the system. This document presents a review of the work related to Smart Grid cyber security.

What is the Smart Grid? The Smart Grid is an electrical power infrastructure that makes intelligent decisions about the state of the electrical power system to maintain a stable environment. The easiest way to define the Smart Grid is by its characteristics. The Smart Grid is an upgrade to the current electrical power system, so it has all of the functionality of our current power system plus several new functionalities [1].

- Self-healing
- Motivates and includes the consumer
- Resists attack
- Increases power quality
- Accommodates all generation and storage options
- Enables electrical markets
- Optimizes assets and operates efficiently

The Smart Grid will be self-healing. This means that it can redirect and adjust the flow of electricity in the event that an electrical transmission path is interrupted. This is done by a continuous self-assessment of the state of the power system. As a result, this can reduce the frequency and duration of major blackouts. It is estimated that the August 14, 2003 blackout in the U.S. and Canada had a societal cost of $10 billion [2]. Reducing the number of major blackouts and their severity will reduce the economic losses our society incurs during these blackouts.

The Smart Grid will motivate and include the customers. There is currently minimal interaction between customers and suppliers in the electrical power system. The Smart Grid provides customers with more information and options about their electrical power. In theory this will allow

customers to make better decisions about their power usage that will not only save them money, but will also promote competition between power suppliers. This is done by enabling two-way communication between energy consumers and suppliers. The Smart Grid can also interact with electrical appliances in a customer's home. This interaction allows appliances to schedule their run time when electricity is at the cheapest price.

The Smart Grid will be resilient to attacks and natural disasters. The Smart Grid will not only be resilient to physical attacks, but also cyber attacks. The electrical power grid is a complicated system that is at the root of most U.S. economic growth. This makes the electrical power grid a critical asset, and damage to it can have devastating affects to our society's welfare. Parallels are drawn between the electrical power grid and the Roman aqueduct system in [3]. Over time the Roman aqueducts underwent design changes. As the Roman Empire grew, the level of perceived threat lowered. This lead to design changes that were less concerned with security and more with form and functionality. Then towards the end of the Roman Empire these aqueducts became easy military targets for invading forces because of the design changes. Attacks against Roman aqueducts had major social impacts because they had become a critical system that the Romans depended on. The electrical power system is a critical asset that we rely on, and it needs to be resilient to all forms of attack.

The Smart Grid will provide an increase in electrical power quality. Electricity is not only required to be available at all times from the power grid, but it must also maintain a constant voltage. Some manufacturing processes are very sensitive to voltage variations. A dip in voltage lasting less than 100 milliseconds can have the same effect as power loss for several minutes or more on some industrial processes. These voltage fluctuations are estimated to cause productivity losses in commercial facilities ranging from thousands to millions of dollars per event. It is estimated that by 2011, 16% of the electrical load will require digital quality power [1].

The Smart Grid will accommodate all generation and storage options available. The integration of renewable energy sources into the electric power grid has several complications. The current electric power grid is a broadcast model that is designed to only allow the one-way flow of electricity from a one-generation source to many consumers. Renewable energy sources are often geographically separated from traditional power sources, and when they are integrated into the power grid it is as distributed power sources. Since the electrical power grid was designed for only a single power source and not multiple distributed power sources, this causes complications. Germany has experienced issues related to problems in their electrical power grid. Customers using solar panels could overload the electrical power system when surges of power come from the solar panels [4]. Fossil fuels are not a sustainable energy source, and as a result new alternative power sources will be explored. The Smart Grid will be able to support these new energy sources along with the traditional power sources.

The Smart Grid will enable electrical markets. Electrical markets in the Smart Grid will encourage competition among power suppliers. This competition will promote power suppliers to develop cheaper and more efficient means of power generation. This will drive down the prices of electrical power for customers as suppliers compete for their business. The Smart Grid will also support distributed power sources. This opens the door for new electrical power suppliers and electrical service providers to enter the electrical market. The electrical market will broadcast current electricity prices based on a supply-demand model. Electricity will be more expensive when the load or demand is high, and it will be cheaper when there is surplus electricity. Customers can use this information to schedule tasks that use large amounts of electricity at a time when electricity

is cheaper.

The Smart Grid will optimize assets and operate efficiently. The features that will make the Smart Grid self-healing can also be used for asset management. The Smart Grid will be able to automatically assess equipment condition and manage equipment configuration. This management automation can be done at substantially lower costs compared to manual management. The automation of equipment management will also reduce the chance of equipment failure since the degradation of equipment can be tracked. The Smart Grid will also incorporate new technologies that will reduce energy loss during electrical transit. This reduction in energy loss will increase the electrical power grid's efficiency by eliminating excess power waste.

1.1 Smart Grid Cyber Security Risks

The Smart Grid is going to add new functionality to the current electrical power system. However, it will also introduce several new security risks into the system. We rely on the electrical power grid for electricity, and our dependence on electricity makes the electrical power grid a critical asset. Disruption of the electrical power supply will have large societal impacts. The security of the electrical power grid is an important issue. The Smart Grid will introduce several new security risks related to its communication requirements, system automation, new technologies, and data collection [5].

The backbone of the Smart Grid will be its network. This network will connect the different components of the Smart Grid together, and allow two-way communication between them. Networking the components together will introduce security risks into the system, but it is required to implement many of the main functionalities of the Smart Grid. Networking the different components together will increase the complexity of the electrical power grid, which will then increase the number of opportunities for new security vulnerabilities. Also, the number of entry points that can be used to gain access to the electrical power system will increase when all of the components are networked together.

The Smart Grid will use the data transported by the electrical power grid network and software to maintain the power system automatically. Relying on the power grid network to transport system information introduces security risks. Some of the components require real-time data, and latency or data loss can have adverse affects on the electrical power grid. The software managing the system state is also at risk to malicious code that can alter its functionality. A disruption to communications or the state management software can lead to loss of power or in extreme cases injury or loss of life.

Networking the different components of the electrical power system together is going to require that different technologies interact with each other. This interaction between different technologies will introduce new security risks. The Smart Grid will have to support legacy systems. Legacy systems typically do not implement newer security features that modernized systems have, and a system is only as secure as its weakest link. In addition, the new technologies that are being used in the Smart Grid may have security vulnerabilities in them that can be exploited.

The Smart Grid will be collecting more data than the current electrical power system. It is estimated that there will be a data increase of an order of magnitude. This increase in data collection can have possible security privacy issues. The Smart Grid will also be collecting new types of information that were not recorded in the past, and this can lead to more privacy issues.

1.2 Smart Grid Security Objectives

The security objectives of the Smart Grid cyber security are different from most of the other industries. It is important that any security countermeasure implemented in the Smart Grid do not impede power availability or safety. An example of this would be locking a system after too many failed password attempts. The power system always needs to be available, and locking the system during an emergency could cause safety issues. The security objectives being evaluated are confidentiality, integrity, and availability. In most industries confidentiality and integrity have higher precedence over availability. In the electrical power system, electricity must always be available, so this is the most important security objective. Integrity is the next important security objective followed by confidentiality.

Availability is the most important security objective. The critical real-time systems in the Smart Grid have an estimated maximum latency of 4 milliseconds. These systems continuously monitor the state of the electrical power grid, and a disruption in communications can cause a loss of power. The table 1.1 lists the estimated maximum latency requirements from [5]. The availability of the electrical power grid is its most important factor. By extension the most important security object of most of the electrical power system components is also availability.

Maximum Latency	**Communication Type**
$\leq$ 4 ms	Protective relaying
Sub-seconds	Wide area situational awareness monitoring
Seconds	Substation and feeder supervisory control and data acquisition (SCADA)
Minutes	Monitoring noncritical equipment and marketing pricing info
Hours	Meter reading and longer-term pricing info
Days/Weeks/Months	Collecting long-term usage data

Table 1.1: Estimated Maximum Communication Latency Requirements

Integrity is the next important security objective in the Smart Grid. The Smart Grid uses data collected by various sensors and agents. This data is used to monitor the current state of the electrical power system. The integrity of this data is very important. Unauthorized modification of the data, or insertion of data from unknown sources can cause failures or damage in the electrical power system. The electricity in the power grid not only needs to always be available, but it also has to have quality. The quality of the electrical power will be dependent on the quality of the current state estimation in the power system. The quality of the state estimation will rely on many factors, but integrity of input data is very important.

The final security objective is confidentiality. The loss of data confidentiality in the Smart Grid has a lower risk than loss of availability or integrity. There are certain areas in the Smart Grid where confidentiality is more important. The privacy of customer information, general corporation information, and electric market information are some examples.

1.3 Smart Grid Security Research Trends

Smart Grid cyber security research typically focuses on the different components of the electrical power system. The earliest work related to the Smart Grid is in Process Control Systems (PCS) security. Recent research has focused on the new Smart Grid components and their interactions.

Smart Grid security work has been done with user privacy, Smart Meters, electrical power system state estimation, component communications, and cyber attack analysis.

Process Control Systems (PCS) have been used by many different industries over the years. A PCS is an automated system that monitors and controls a process using computers. PCSs are typically run as isolated systems that have limited or no outside network connections. PCSs are used in manufacturing to control some aspect of production. PCSs are changing from running in isolated environments to being connected to larger networks. This introduces new security risks because traditional PCSs were designed with limited security. Since PCSs were run in isolation, cyber security was not an important concern.

The Smart Grid will be collecting much more user data and new kinds of information. This new data coupled along with the inter-connectivity in the Smart Grid has caused user privacy concerns. There are laws and regulations that protect user privacy. These laws will need to be extended to protect Smart Grid users. The new data types will need to be identified and analyzed, so security risks can be identified and steps can be taken to ensure user privacy.

Smart Meters are a digital version of the current power meters. Smart Meters will be installed at a customer's location, and they will be used to take electrical power usage measurements called readings. Smart Meters will be connected to the Smart Grid, and they will periodically send readings to the Smart Grid. These readings are used for electrical power state estimation and for billing purposes. There are a few security challenges with Smart Meters ranging from tampering with device functionality to communication issues between the meter and power supplier.

The PCSs in the Smart Grid must model the current state of the electrical power system. Each of the models that could be used has several security risks. The state estimation models are part of the PCS, but they are looked at separately because there has been a lot of research on this specific topic. The integrity of the state estimation model is an important issue in Smart Grid security.

Networking the different components of the Smart Grid together means that many varying components must interact with other components. This is a large topic in the Smart Grid because of the great number of components that must communicate. There are different requirements for each pair of communicating components. These communication requirements include latency, bandwidth, reliability, and security needs. This means that there will need to be many different protocols used in the Smart Grid to enable communication between components.

There are many different design considerations to be evaluated before the Smart Grid can be built. This means that methods need to be developed to analyze the different designs. There have been several projects that are designed to simulate the Smart Grid using software and hardware. These projects can be used to run simulations and do some initial testing of different Smart Grid designs. One of the aspects of Smart Grid design that can be tested using these systems is cyber security. Impact analysis can be performed to gauge potential security risks.

Chapter 2

Categories

The work that is reviewed in this document will be categorized by the component of the Smart Grid that it focuses on. It is possible that a work may fit into one or more of the possible categories, but it will be listed under the most prominent category. The Smart Grid is a large and complex system. Because of this complexity, research work typically only focuses on a single component. The different categories are listed below along with a detailed discussion of each.

- PCS Security
- Smart Meter Security
- Power System State Estimation Security
- Smart Grid Communication Protocol Security
- Smart Grid Simulation for Security Analysis

2.1 PCS Security

Process Control Systems (PCS) are used by the Smart Grid to monitor and control physical aspects of the electrical power grid. Traditional PCSs are designed to run in isolated environments with no outside network connection, so they typically do not have any security built in. This is an issue for the Smart Grid since these PCSs will be monitoring large geographical areas of the power grid. This means that there will be many entry points to get into the network. PCSs used in the Smart Grid will need to address these security issues. There are several different kinds of PCS. The most commonly used in the electrical power grid is the Supervisory Control And Data Acquisition (SCADA) system.

Since the PCSs will be controlling physical aspects of the electric power grid, the security of these systems is very important. When a computer is compromised only the data on the computer is compromised, and in extreme cases some of the hardware in the computer may be damaged. When a PCS is compromised, multi-million dollar equipment can be physically damaged in addition to data being lost. In extreme cases it can cause human injury or loss of life. The most important security objective of the PCS is availability. The electrical power system must be available at all times, so the PCS controlling the power system must also be always available. The integrity of the PCS is the next important security objective. It will not be able to make correct decisions if

it is given false data as input. Confidentiality is the least important security objective. The PCS needs to run in real time, and that means the system must have minimal overhead. Implementing confidentiality may be too time-consuming to meet latency requirements.

Security in PCSs has traditionally been disregarded. Most PCSs run in isolated locations with no outside network connection. This has caused them to be designed with limited or no security considerations. Over time business requirements have led to corporate networks being connected to the PCS network. Doing this has led to security breaches resulting in physical damage and injuries [6]. The Smart Grid is using PCSs that are connected to a large network that has many access points, and this means that PCSs must address security concerns that large networks have.

2.2 Smart Meter Security

Smart Meters are the next category of Smart Grid security research. Smart Meters are devices installed at a customer's site, and they are used to measure the amount of power used. They are an electronic version of the current power meters that are currently used. The electrical power readings are be sent back to the power suppliers on regular intervals. Smart Meters are not used just for recording the amount of energy that a customer uses. They also give the Smart Grid a feedback mechanism that can be used to model power usage requirements at a much more detailed level then what is currently possible.

The security of Smart Meters is important because altered readings from the device can lead to incorrect billing, and false power usage approximations. Altering Smart Meters can provide attackers with monetary gains, and since the device is installed at a customer's site access to these devices is readily available. It is estimated $6 billion worth of power has been stolen from the U.S. electrical power system [7]. The most important security objectives are integrity and confidentiality. It is important that the Smart Meter readings are correct and not modified. The confidentiality of the Smart Meter reading is also important. Tools have already been built that can profile a users electrical usage readings to determine which household appliances are being used [8, 9]. This information can be used by different companies and individuals, and it is a privacy concern. The availability of Smart Meters is more flexible than other Smart Grid components. The maximum latency of Smart Meters from the table 1.1 is in terms of hours. This is far greater than the real-time latency requirements, which are in terms of milliseconds.

Smart Meter security is a challenge because it is easy to gain physical access to the Smart Meter device and there are instant monetary gains from altering these systems. The integrity of Smart Meters and their data needs to be verified in the Smart Grid before use. Confidentiality of the Smart Meter readings is also a challenge. Smart Meters need to be networked to power suppliers, so they can carry out their functionality. This means that it may be possible for anyone else connected to that same network to observe others' power usage readings. This information can then be used to profile a user's behavior.

2.3 Power System State Estimation Security

Power system state estimation is another category of Smart Grid cyber security research. The Smart Grid has the ability to control physical properties of the electrical power system. This is done so that the Smart Grid can maintain a stable state in the electrical power grid. The Smart

Grid must model the current state of the power system in order to make informed decisions and take action on them. The state estimation model makes up part of the PCS.

The security of the power system state estimation model is important because it is used by the Smart Grid to maintain the electric power system. The power system state estimation model is a tool that the Smart Grid PCSs use to model sensor and agent data. This means that the security objectives important to PCSs are also important here. Availability is very important followed by integrity. Confidentiality is the least important objective because it adds overhead to a real-time system.

The security of the power system state estimation model is a challenge because of the possibility of receiving false input data into the model. There are a few reasons for inserting false data into the model. System instability and financial gain are a couple of motivations for attackers. Many PCSs have the false-data injection security issue, and distinguishing between actual and false data is a difficult problem. Typically there are mechanisms that can distinguish bad data from normal data, but these mechanisms are not effective against false-data attacks.

2.4 Smart Grid Communication Protocol Security

The Smart Grid communication protocols are the next category of Smart Grid security research. The Smart Grid relies on communication between its different components in order to function. Each of the components has different communication requirements. The communication requirements range from very low latency to high data throughput, and each have a set of security needs. The Smart Grid will need several communication protocols to meets the varying connection requirements.

The security of Smart Grid communication protocols is important because the network communication is the backbone of the Smart Grid. Many of the major Smart Grid functionalities cannot take place without communication. The security objectives that are important depend on which components are communicating, and what data they are exchanging.

Smart Grid communication protocol security is a challenge because there are many different components communicating, each with their own set of communication requirements. Another issue is that the Smart Grid technology needs to integrate with legacy power systems, and many of these devices have constraints that must be considered. Legacy devices can typically introduce security vulnerabilities into the system because of a lack of security support.

2.5 Smart Grid Simulation for Security Analysis

The last category of Smart Grid security research is security analysis with simulation. Testing any Smart Grid designs or changes is very difficult. The power system must always be available so taking it down to perform tests is not possible. Instead, it is possible to model the Smart Grid in software or hardware. These models can then be used to analyze security and other Smart Grid aspects.

Smart Grid simulation is important because of issues with testing the Smart Grid. It is expensive to build a Smart Grid. It cost an estimated $42.1 million to install a Smart Grid in Boulder Colorado [10]. Therefore building or modifying a separate large scale Smart Grid for each test is impractical. It is also difficult to use any power systems in operation to test because tests cannot be allowed to compromise system availability.

Smart Grid simulation and analysis is a challenge because the Smart Grid is a large and complex system. Many of the Smart Grid components are connected together, and changes in one component may cause unforeseen affects on other components in the system. Another challenge is that a component may have a single functionality in the power system, but how it is implemented may be different at various installations.

Chapter 3

Literature Review

The research work reviewed in this document has been separated into five different categories. A list of the categories and the work in each category can be found in table 3.1. The work done in each category is further broken down into sections. These sections can be found at the beginning of each category below.

Research Category	**Work Done**
PCS Security	[11] [12] [13]
Smart Meter Security	[14] [15] [16] [7] [17] [18]
Power System State Estimation Security	[19] [20] [21] [22]
Smart Grid Communication Protocol Security	[23] [24] [25] [26] [27]
Smart Grid Simulation for Security Analysis	[28] [29] [30]

Table 3.1: Smart Grid Research Categories and Work Done

3.1 PCS Security

Process Control Systems (PCS) are the components responsible for monitoring and controlling physical properties of the electrical power grid. A detailed explanation of PCSs can be found in 2.1. The research work done on PCS security covers several different issues, and each issue has its own section. The work reviewed in this document covers PCS security risks, security assessment methods, and Intrusion Detection Systems (IDS). The table 3.2 lists all of the sections, and the research work done in each section.

PCS Security Section	**Work Done**
PCS Security Risks	[11] [13]
IDS	[12]
PCS Security Assessment Methods	[11]

Table 3.2: PCS Security Sections and Work Done

3.1.1 PCS Security Risks

Several authors have done work with PCS security risks in electrical power systems. Watts worked in this area in [13], and wrote a review of the risks that actual electric power systems face. Jiaxi, Anjia, and Zhizhong also provide a review of several PCS security risks in [11]. Work in PCS security risks is needed so that when the systems are updated or new systems are designed any existing security risks can be taken into account.

The contribution of Watts' work in [13] is a review of cyber security risks to electrical power systems. This document focuses on risks pertaining to PCS security. Watts provides a detailed and comprehensive overview of electrical power system security risks. A list of security mitigation actions is also provided along with any implementation concerns. A brief summary of PCS cyber security risks is also provided in [11]. However, this is not the main contribution of this work, and it will be discussed later.

The benefit of Watts' work in [13] is a good review of PCS security and other network related risks. A draw back to the work is that the security risks are relevant to traditional electrical power systems. The work does not address any of the new security vulnerabilities introduced by the Smart Grid. The document does make references to early work on the Smart Grid. Mainly it references work with self-healing energy infrastructure systems [31].

The work in [13] does focus on traditional power system security risks; however, the work may still be applicable to Smart Grids. The Smart Grid is an extension of current electrical power systems, so any security risks they have may translate over to the Smart Grid. The document also provides a starting point for Smart Grid security risk assessment.

3.1.2 IDS

Valdes and Cheung proposed an Intrusion Detection System (IDS) that can be used for different PCSs in [12]. The motivation for their work was a trend in how PCSs were being used in practice. Most PCSs are designed to run in isolated environments so little or no security was designed into them. However, these systems were being connected to corporate networks in practice. This could lead to security concerns because PCSs could now be manipulated by outside connections through the corporate domain. Security compromises to PCSs not only cause financial loss, but can also cause expensive equipment damage or even physical injury in extreme cases. The figure 3.1 is representation of the IDS in a PCS.

The contribution from [12] is an IDS that is designed to run in PCSs. The IDS uses a model-based approach. This approach is possible because the PCS configuration is relatively static, and their network traffic is relatively predictable. The model-based approach is also complemented with a signature-based approach, which is useful for detecting known or foreseeable attacks. The IDS and a set of support tools for running the IDS were developed.

There are several benefits of using a model-based approach. The signature of an attack is not critical for the system to function. This approach is also able to detect unknown attacks that a signature-based attack could not detect. Since the system also uses a signature-based system in conjunction with the model-based system, it is able to capture known security issues. There are some drawbacks to using this type of IDS. Since it uses a model-based IDS, that means a model must be built for a given PCS. It can be difficult and costly to develop an accurate model that represents a PCS. This type of approach also requires that a relatively static configuration be maintained. Another issue is that if the PCS is complicated it may be very difficult to develop an

accurate model.

Valdes and Cheung's work focused on traditional PCSs that are relatively isolated. The Smart Grid will use PCSs to accomplish some of its main functionalities. These PCSs will need to be secure, and part of their security should be continual monitoring. The form of monitoring does not necessary need to be an IDS system, but it is one possibility. The main issue with using the model-based IDS approach in the Smart Grid is that the power system is very complex, and designing an accurate model could be an issue.

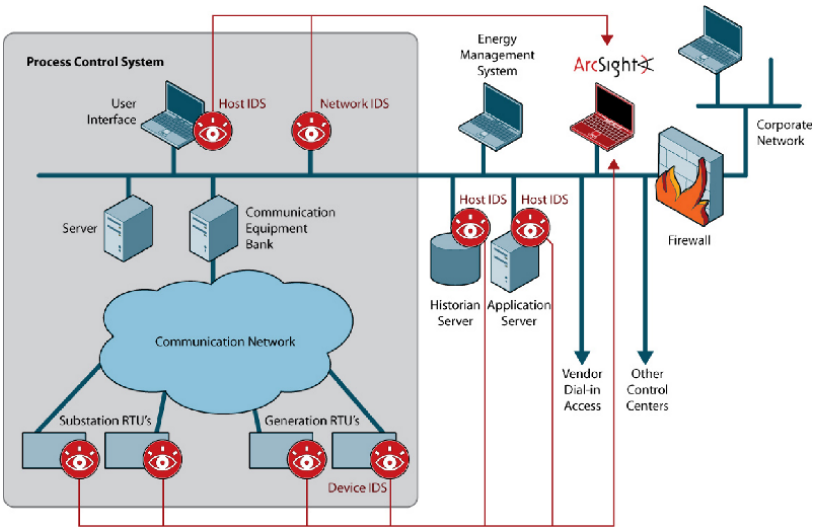

Figure 3.1: Process Control System Intrusion Detection System, reproduced from [12]

3.1.3 PCS Security Assessment Methods

As previously mentioned in 3.1.1 Jiaxi, Anjia, and Zhizhong have done work with PCS security. Their work in [11] is on PCS security assessment methods. The motivation for their work is to develop a means to assess cyber security vulnerabilities. Mainly they focus on PCS security vulnerabilities.

The main contributions of Jiaxi, Anjia, and Zhizhong's work in [11] are two different cyber security assessment methods. The first method is a probabilistic assessment. In this method the probability of occurrences along with probability of a resulting accident are used to calculate a vulnerability index of the cyber systems. The second method is an integrated approach. Cyber security risks are first categorized into five different categories based on severity. Then probabilities of a risk belonging to a category are assigned. Using this information and a formula, the degree of cyber security risk can be obtained.

The benefit of this work is that it establishes a procedural method for evaluating cyber security risks. There are some cons to the methods proposed. The document does not provide any support for the use of one method over the other, and there is no evidence presented that supports the effectiveness of either method. A problem mentioned about the probabilistic method is that it is difficult to identify the probability distribution to use for the security vulnerabilities.

The work done in [11] could be extended upon to use within the Smart Grid. Since there is a lack of evidence supporting either of the methods proposed, it might be appropriate to use other

more established security assessment methods from similar industries. The only difficulty with this is that most non-PCS industries do not have the same security objectives.

3.2 Smart Meter Security

Smart Meters are responsible for measuring energy usage for individual users. A detailed explanation of Smart Meters can be found in 2.2. The research work done on Smart Meter security covers several different issues, and each issue has its own section. The work reviewed in this document covers Smart Meter Intrusion Detection Systems (IDS), redundant readings, and data anonymization and privacy. The table 3.3 lists all of the sections, and the research work done in each section.

Smart Meter Security Section	Work Done
IDS	[14]
Redundant Smart Meter Reading	[18]
Smart Meter Data Anonymization and Privacy	[15] [16] [7] [17]

Table 3.3: Smart Meter Security Sections and Work Done

3.2.1 IDS

Berthier, Sanders, and Khurana proposed a Smart Meter IDS system in [14]. The motivation for doing this work was to provide Smart Meters with a comprehensive set of security tools. The Smart Meter system is a critical component of the Smart Grid, and security measures that prevent vulnerabilities are only part of a security solution. Continuous monitoring is also needed to maintain security. The figure 3.2 provides a representation of the Smart Meter IDS with a list of operations to be performed at each Smart Meter component.

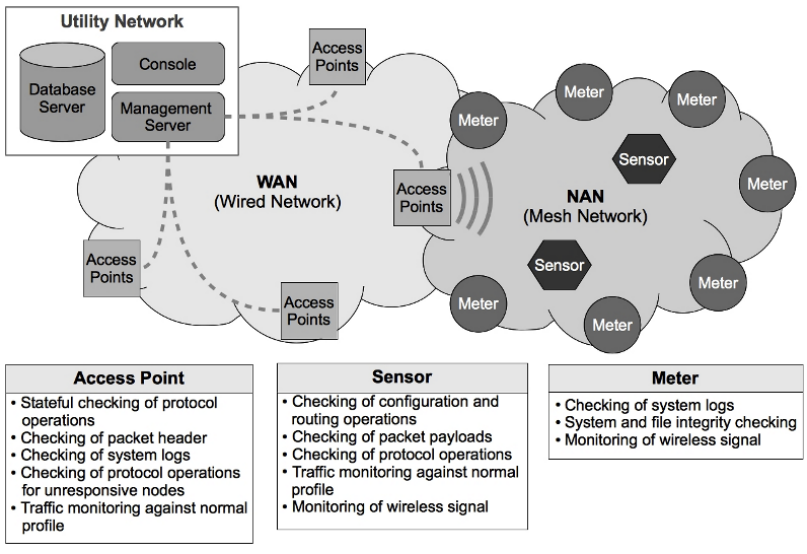

Figure 3.2: Smart Meter Intrusion Detection System, reproduced from [14]

The contribution from the work in [14] is a specification-based IDS. The advantage of specification-based IDSs is that they do not require empirical data to detect intrusions. Since Smart Meters are a new technology, there is a lack of empirical data. Smart Meters also use a limited number of protocols and applications which simplifies the system, and makes using a specification-based IDS possible.

There are several benefits to using a specification-based IDS. They can provide higher accuracy than signature and anomaly-based systems. Specification-based IDSs also do not require empirical data to detect intrusion. There are some drawbacks to using a specification-based IDS. There is a high overhead associated with these systems. Smart Meters are constrained devices that have limited memory and computational power. It may be impractical to run a specification-based IDS directly on some Smart Meters. Another issue with this type of system is that it is very costly to develop.

Berthier, Sanders, and Khurana's work in [14] is a step in the right direction towards a Smart Meter IDS. However, a purely specification-based IDS may not be the best solution. A better solution may be to leverage the strengths of the different IDS types, and use a combination of them in the Smart Meter system.

3.2.2 Redundant Smart Meter Reading

A method to secure redundant Smart Meter readings was proposed in [18] by Varodayan and Gao. The accuracy of Smart Meter readings is a concern for many customers. One method to verify the accuracy of Smart Meters is to install a separate electrical energy-measuring device that compares its reads to the reads that the power supplier received from the Smart Meter. The problem with this approach is that it introduces confidentiality risks. Attackers can intercept the data used to verify the integrity of the Smart Meter. The figure in 3.3 is a representation of the redundant Smart Meter feedback loop.

The contribution from the work in [18] is a secure method for power suppliers to echo the energy readings they receive from Smart Meters back to the customers. These data echoes can then be used by customers to verify the integrity of the Smart Meter readings. The work in [18] provides a method of encoding the reading echoes such that it can only be decoded with the original Smart Meter readings. This means that if an echoed reading cannot be decoded with the original reading then the two readings do not match.

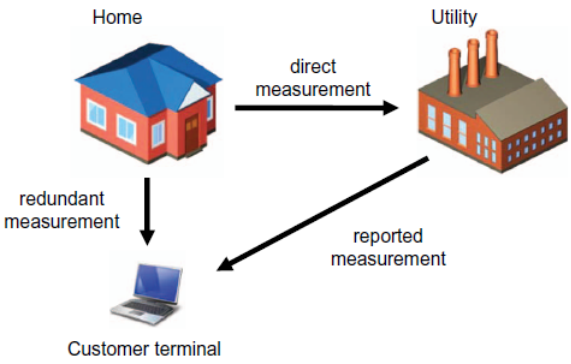

Figure 3.3: Smart Meter Redundant Meter Reading, reproduced from [18]

The benefit of this redundant reading system is that it adds confidentiality to the echoed readings. This is done by making the original power readings the security key for decoding the echoed readings. A criticism of the work is that it does not provide any evidence of how this method compares to other means to achieve confidentiality. An example would be the benefits of using this proposed method over a data exchange using public key encryption.

The concept of redundant Smart Meter readings does provide the Smart Gird with a feedback loop that can verify the integrity of Smart Meters. The only issue with implementing [18] to secure

the feedback is that there may be more efficient ways to ensure confidentiality.

3.2.3 Smart Meter Data Anonymization and Privacy

Smart Meters will gather more electrical power usage data than has been collected in the past. This causes privacy concerns because this data can be analyzed to determine behavioral patterns. An example energy load signature can be found in figure 3.4. Efthymiou and Kalogridis did some work with a method to anonymize the bulk of the data coming from Smart Meters in [15]. The concept is to associate the frequent Smart Meter readings with a larger group of users so that the identity of individuals can be masked. This does not include Smart Meter readings that must be associated with a specific user such as readings used for billing purposes.

The contribution of the work in [15] is an escrow system that can be used to authenticate the anonymous Smart Meter data. Each Smart Meter will have two different identifiers. One will be used for readings that are associated with a particular Smart Meter such as readings used for billing, ID_{Known}. The other identifier will be used for anonymous readings, $\mathrm{ID}_{Anonymous}$. The escrow is the only party that knows the relationship between the two identifiers, and it can be used to validate the anonymous reading data.

The benefit of this system is that it provides a means to hide an individual's identity in a crowd. There are a few issues with this system. This system relies on a third party to maintain the relationship between users and anonymous data. The trust of the system relies then on the trust of the third party. Another issue with this system is that it's sending all of the anonymous data out with $\mathrm{ID}_{Anonymous}$ and the less frequent readings associated with a customer with ID_{Known}. It may be possible for an attacker to collect all of the $\mathrm{ID}_{Anonymous}$ readings and ID_{Known} readings. Then sum up the $\mathrm{ID}_{Anonymous}$ readings over a time period and compare them to the ID_{Known} readings to find relationships between anonymous identifiers and known identifiers. Another issue with this approach is that each Smart Meter contains both of the identifiers needed, and it may be possible to manipulate those identifiers.

The method of anonymizing Smart Meter data in [15] does protect a user's identity. However, the Smart Meter readings can still be data-mined for electrical usage patterns since the anonymous readings still have an identifier. This information can then be mapped to groups of people to determine average behaviors. In addition, the size of the group that a user is being masked in can affect the level of anonymity provided.

Kalogridis, Efthymiou, Denic, Lewis, and Cepeda did work with the privacy of Smart Meter data in [16]. Instead of achieving privacy through the network traffic between the Smart Meter and the electrical power supplier, their work focuses on transforming the Smart Meter readings. Each customer produces an electrical energy signature that can describe their electrical power usage behavior, which can be seen in figure 3.4. The work in [16] provides a method that transforms a customer's electrical energy signature to hide behavioral patterns. Figure 3.5 is a representation of a home power network with a load signature moderator.

The contribution from [16] is a function designed to mask the load signatures of certain electrical appliances in a customer's home by offsetting portions of electrical power demands from an energy storage device. The work assumes that a battery and a power switch that can draw streams of power from different sources at once are available to a customer. Using these, the electrical energy signature of a customer could be masked from the network outside of the home by drawing random amounts of power from the battery to transform the appearance of the electrical energy

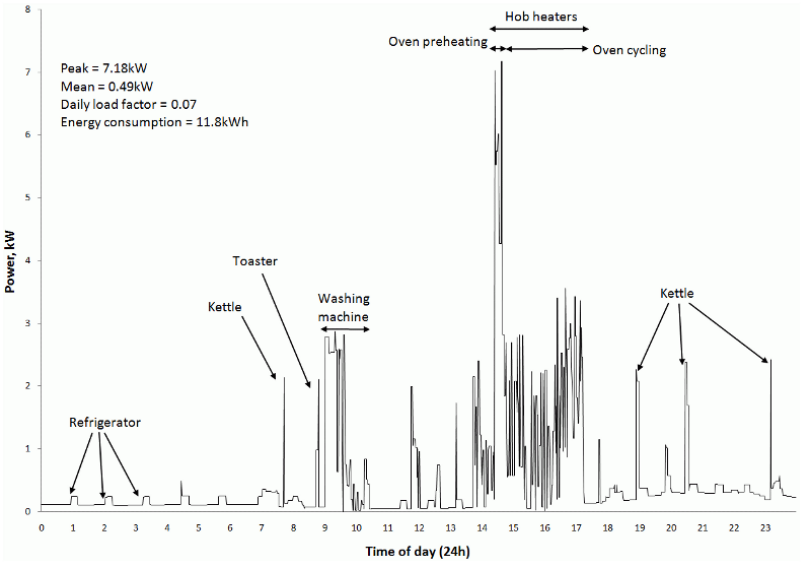

Figure 3.4: Electrical Power Usage Signature, reproduced from [32]

load signature. Theoretically the same amount of power would be used since power would be needed to charge the battery.

The benefit of this work is that it can be used as a means to obfuscate energy usage patterns to outside observers. An issue with this method is that it's designed under the assumption that the battery storage device is running at 100% efficiency. The problem with using a battery storage device is that there will be energy loss, which will lead to higher energy consumption. The document does recognize this issue, and it also suggests the integration of renewable energy sources into the system as another source of power for load signature obfuscation.

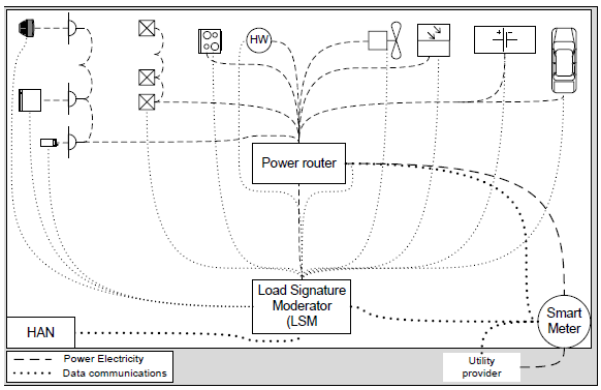

Figure 3.5: Example Home Network with Load Signature Moderator, reproduced from [16]

The work in [16] could definitely have its place in the Smart Grid. The load signature obfuscation method could be used by individuals in conjunction with other privacy measures that are implemented at a network level between the customer and power supplier. This method would provide an added layer of privacy.

There have been several people working in the area of Smart Meter data privacy. McDaniel and McLaughlin worked on Smart Grid security in [7]. There has also been related work by the National Institute of Standards and Technology (NIST) that focused more on the data instead of the system in [17]. The motivation for both works was to provide a review of possible privacy risks that could be created by the Smart Grid. Works from [14, 18, 15, 16] also all contain brief sections pertaining to Smart Meter privacy risks.

The contribution of the work in [7] is a review of possible data privacy risks from a viewpoint of the Smart Grid design. The contribution from [17] was identifying what data could be collected from the Smart Grid, how it could be exploited, and risk mitigation measures.

The information from [17, 7] can be used to better design Smart Meter systems that address the privacy concerns. The work can also be used in other aspects of the Smart Grid. It may be useful for business policy creation, and also help with any privacy laws that may need to be created to protect the Smart Grid users.

3.3 Power System State Estimation Security

Power system state estimation models are used by the PCS to maintain the electrical power grid in a stable state. A detailed explanation of power system state estimation can be found in 2.3. The research work done on power system state estimation security covers several different issues, and each issue has its own section. The work reviewed in this document covers false data injection attacks and communication channel capacity. The table 3.4 lists all of the sections, and the research work done in each section.

Power System State Estimation Security Section	**Work Done**
False-Data Injection Attacks	[19] [20] [22]
Communication Channel Capacity	[21]

Table 3.4: Smart Meter Security Sections and Work Done

3.3.1 False-Data Injection Attacks

Xie, Mo, and Sinopoli worked on false data injection attacks in [22]. This attack can be used to alter the electrical power system state in the state estimation model. The motivation for this work is to show that it is possible to carry out the attack without being detected as an incorrect measurement by the PCS.

The contribution of the work in [22] shows the impacts of performing a false-data injection attack on the Smart Grid. The impact of the attack is measured in terms of monetary gain by manipulating pricing of the electrical market. The work also shows that it is possible to perform this attack without being detected. The attacker does need to know the pricing model that is being used by the system to carry out this attack successfully.

The benefit of this work is that it quantifies the cost of an attack in terms of currency. It is often difficult to measure security threats in business terms. Placing a monetary value on the attack puts it in terms that most people are able to understand. The monetary gain from manipulating the electric market is only one aspect of attacking the Smart Grid, and there are many other that also need to be considered.

The work in [22] demonstrates one of the possible attacks against the Smart Grid that can be exploited for financial gain. It will be important to consider this work when building the state estimation model for the electrical power system. This work also suggests that further work should be done with methods of detecting false-data injection.

Kosut, Jia, Thomas, and Tong did work with compromising the Smart Grid state estimation in [20]. There are two categories of attacks against power state estimation models: observable and

unobservable. The motivation for the work in [20] was to find the minimum number of attackers required to carry out an unobservable attack. Some work was also done with counter measures to observable attacks.

The contribution from the work in [20] is an algorithm to find the minimum number of compromised input sources that are needed to carry out an unobservable attack. An unobservable attack cannot be detected. An unobservable attack happens when a certain number of input sources out of all of the available input sources are compromised. Another contribution of [20] is a heuristic to detect observable attacks. The heuristic is built off of previous work by Kosut, Jia, Thomas, and Tong, but is slightly modified to provide better run time performance.

The work in [20] can be used to determine how many meters would need to be compromised in the Smart Grid to carry out an unobservable attack. This information can then be used to find areas of the Smart Grid that are prone to attacks, and take measures to mitigate the risk. It may also be possible to use the heuristic presented in the work to detect observable attacks.

Dan and Sandberg worked on finding and mitigating false-data injection attacks against the state estimation model in [19]. In their work, they are concerned with being able to compute a security index that can be used to identify input source flows that are vulnerable to manipulation. Work was also done to create an algorithm that can be used to identify what security is needed to protect against false-data injection attacks.

A contribution of the work in [19] is an algorithm to compute a security index for a state estimator. This security index will identify which input sources to the state estimator are susceptible to manipulation. Using this they proposed an algorithm that can find the least cost false-data injection attack. This algorithm can then be used to identify locations where installing an encrypted input source communication will provide the most benefit.

The Smart Grid is going to rely on an accurate state estimation model more than the current electrical power system. This means ensuring the accuracy by verifying the integrity of the state model inputs. This can be done by using encryption; however, it is expensive to install encryption. The work in [19] can be used to identify locations where the encryption will have the most affect.

3.3.2 Communication Channel Capacity

In [21], Li, Lai, and Qiu worked on the problem of Smart Grid state estimation security. They focus on the communication theory side of the problem. The motivation for their work was to determine how much channel capacity was needed for the security of the state estimation model.

The contribution from [21] is determining what communication channel capacity is needed to guarantee security. The model used in [21] is simplified to consider only a single receiver and sender, and it is assumed that there is an eavesdropper listening. The channel capacity that is needed to convey information without being intercepted by the eavesdropper is then calculated. The results are applied to a simplified dynamic Smart Grid model.

The work in [21] is a step toward better understanding of the kind of network topology that will be needed for the Smart Grid. The work was simplified, but the authors plan future work on expanding this to multiple simultaneous communication channels. The work also models the communication requirements of the simple Smart Grid model as the parameters are changed.

3.4 Smart Grid Communication Protocol Security

Smart Grid communication protocols are used by the Smart Grid to communicate between separate components. A detailed explanation of Smart Grid communication protocols can be found in 2.4. The research work done on Smart Grid communication protocol security covers several different issues, and each issue has its own section. The work reviewed in this document covers false-data injection attacks and communication channel capacity. The table 3.5 lists all of the sections, and the research work done in each section.

Smart Grid Communication Protocol Security Section	Work Done
Protocol Design Principles	[24]
Real Time Communications	[27]
Smart Meter Communication	[23] [25]
Cryptography	[26]

Table 3.5: Smart Meter Security Sections and Work Done

3.4.1 Protocol Design Principles

Khurana, Bobba, Yardley, Agarwal, and Heine proposed a set of design principles to use when designing Smart Grid authentication protocols in [24]. The motivation for their work was to propose a set of guidelines that could be used by protocol designers to develop authentication protocols with fewer vulnerabilities.

The contribution of the work in [24] is a set of design principles that can be used when creating authentication protocols in the Smart Grid. The design principles are based off of principles used when designing Internet-based authentication protocols. The Internet-based principles were altered to better fit the security objectives that are important in the Smart Grid.

The work in [24] can provide authentication protocol designers with valuable design guidelines. Since the design principles are based off the Internet, many of them are only slightly altered. The document does briefly discuss the impacts and tradeoffs of supporting one communication goal over another, but further work could be done in this area.

3.4.2 Real Time Communications

Zhang and Gunter worked on a secure multi-cast protocol that can be used in the Smart Grid in [27]. The motivation for their work was to create a secure communication protocol that could be used to efficiently communicate in the Smart Grid. Multi-cast is used because it uses bandwidth efficiently.

The contribution from [27] is a secure multi-cast communication protocol that is able to automatically determine group membership. This is accomplished by making the communication protocol application-aware, so group membership can be determined. Automating configuration will help reduce the number of configuration errors in the system. The communication protocol was implemented using IPsec. The document also gave evidence that IPsec meets the latency requirements for medium sized networks.

The work in [27] would benefit the Smart Grid. There are many devices used in the system and automating their configuration would reduce the chance of manual configuration errors. It would

also ensure that device configurations were up to date. Further work would be needed to test the scalability of the protocol with large networks. An issue that needs to be addressed with using IPSec in the communication protocol is connection refusals. Security does not take precedence over availability and safety, and a connection cannot be refused to a critical device because of security parameter mismatches.

3.4.3 Smart Meter Communication

Bartoli, Hernandez-Serrano, Soriano, Dohler, Kountouris, and Barthel worked on a communication protocol for Smart Meters in [23]. These networks are typically composed of resource-constrained devices. The authors use data aggregation in the network to efficiently deliver the data to a gateway. Figure 3.6 is an example of a possible aggregation structure.

The contribution of the work in [23] is a lossless data aggregation protocol that has a security-to-communication tradeoff. It is assumed that the Smart Meter connection to a gateway is a tree topology. The aggregation protocol would combine packets from child nodes before sending them to a parent node. This way the overhead of repeating packet headers can be reduced. There are two ways of securing the data. End-to-end security provides confidentiality and integrity since only the end nodes can decrypt the data; however, this method is less efficient at data aggregation. The other way is per-hop security, which provides security between each hop. This does not guarantee end-to-end security since the intermediate nodes can view the data. The work in [23] proposes a per-hop security protocol that still maintains end-to-end security.

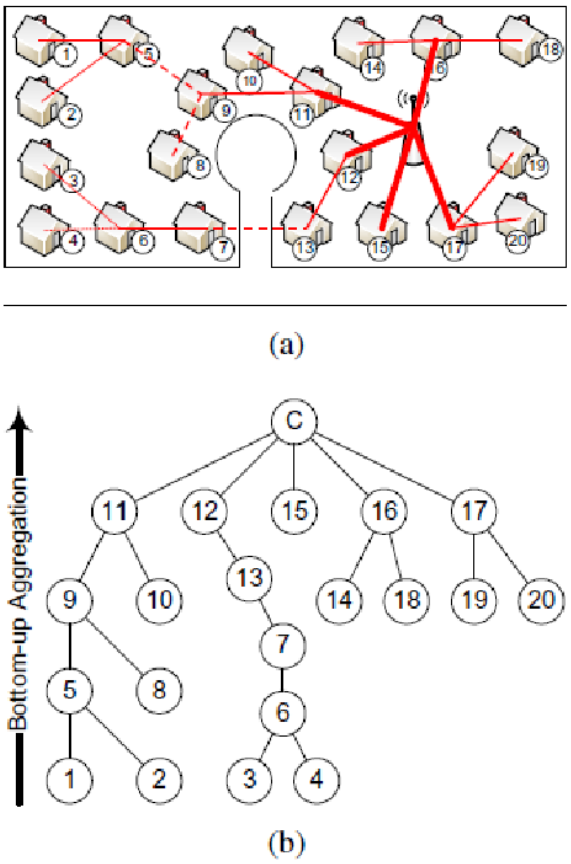

Figure 3.6: Example Aggregation Tree Structure, reproduced from [25]

The work in [23] is one possible solution that could be used to efficiently transmit data though a tree-based network topology that does not have high noise. The evidence presented supports the use of this protocol, but it needs to be compared with other alternatives. Its place in the Smart Grid will depend on the network topology that is used in practice. It may be worthwhile to extend the work here to encompass the entire connection from the Smart Meter to the power supplier.

Li, Luo, and Liu worked on a communication protocol for Smart Meters in [25]. The authors proposed a data aggregation protocol that can be used to aggregate Smart Meter communications to a gateway. The motivation for the work is to develop a secure and efficient communication protocol. Figure 3.6 is an example of a possible aggregation structure.

The contribution from [25] is a lossless Smart Meter aggregation protocol. The protocol uses a spanning tree rooted at the gateway device, and performs aggregation at each node by combining child node packets and sending the resulting packet to its parent. This protocol uses homomorphic encryption to protect the privacy of the data.

The work in [25] proposes a simple network aggregation protocol. However, there is a lack of evidence to support this protocol. There is no evidence that indicates this method would yield better results than not performing data aggregation. The use of homomorphic encryption reduces the computation load on the devices in the network, but at the cost of aggregation efficiency.

3.4.4 Cryptography

So, Kwok, Lam, and Lui worked on an encryption protocol for the Smart Grid in [26]. The protocol was specifically designed for use in Smart Meters and the devices attached to them. The motivation for their work was to develop an encryption protocol that required minimal user setup.

The contribution from [26] is a zero-configuration identity-based encryption and signature scheme. It uses a device's identifier to sign and encrypt data, and a sender contains all of the information needed for encryption keys so no central server is needed. The protocol can also generate a per-packet key so it eliminates key hijacking. This encryption protocol also does not require a per-device user setup, which simplifies configuration.

The work in [26] would be helpful in reducing encryption configuration issues with Smart Meter systems. An issue with this is that the devices will now be responsible for their configuration as a system. This means that a clear and precise set of standards would need to be developed. The success of a protocol like this depends on a set of standards being developed and followed by manufacturers.

3.5 Smart Grid Simulation for Security Analysis

Smart Grid simulation can be used for evaluating different Smart Grid designs and cyber security. A detailed explanation of Smart Grid simulation for security analysis can be found in 2.5. The research work done on Smart Grid simulation can be broken into two separate sections. The work reviewed in this document covers software simulation and hardware simulation. The table 3.6 lists all of the sections, and the research work done in each section.

Smart Grid Simulation for Security Analysis Section	Work Done
Software Simulation	[28] [29]
Hardware Simulation	[30]

Table 3.6: Smart Meter Security Sections and Work Done

3.5.1 Software Simulation

Godfrey, Mullen, Dugan, Rodine, Griffith, and Golmie worked on simulating network communications and power systems in [28]. The motivation for this work was to perform an analysis on the impact of communication failures in the Smart Grid. This was accomplished by integrating OpenDSS [33] a power system simulator and ns-2 [34] a network communication simulator. Figure 3.7 depicts the interaction between OpenDSS and ns-2.

The contribution of [28] is a co-simulation model that can be used to analyze communication failure impacts on the Smart Grid. The simulator was run on power configuration with a solar power source that had several small-scale storage batteries. The storage batteries are used to offset the variable voltage output of the solar power source. The simulator was used to analyze the power system impacts caused by communication failures. The benefit of this work is that it is using two exiting simulation models and combining them to predict Smart Grid behaviors.

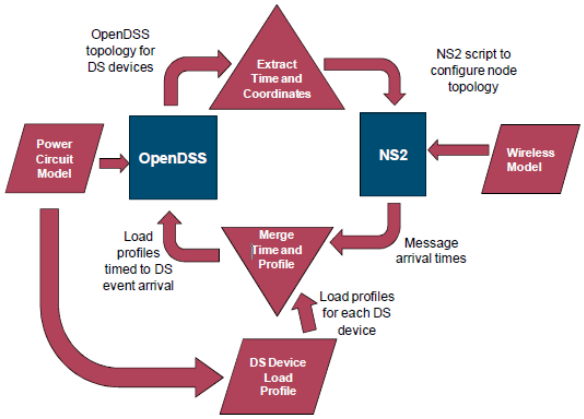

Figure 3.7: Interaction Between OpenDSS and ns-2, reproduced from [28]

It is expensive and time consuming to build a Smart Grid. The work in [28] provides the Smart Grid designers with a valuable tool that can be used to evaluate different designs. The tool can also be used to identify possible security risks that could exist. Simulation using software is a powerful evaluation tool, but it is not the only one. Any analysis process should use multiple methods of evaluation.

Kundur, Feng, Liu, Zourntos, and Butler-Purry worked on Smart Grid cyber attack analysis in [29]. The motivation for their work was to develop a framework that could be used to model Smart Grid cyber and physical interactions. The model could then be used to analyze the physical impact of cyber attacks. The impact analysis is represented in figure 3.8.

The contribution from the work in [29] is a partial model that can represent cyber and physical relationships of the Smart Grid as a directed graph. The model can then be transformed over time to simulate the physical and cyber interactions. Each node in the graph stores system state information that is governed by equations. The benefit of this type of system is that it can be used to produce a cause-effect relationship between cyber and physical properties.

The work in [29] covers preliminary steps to developing a framework for Smart Grid security analysis. This work can be used in the Smart Grid to identify which cyber-to-physical relationships pose a high risk. An issue with using this type of model is that it requires a significant amount of detailed information to perform the analysis, which may cause issues when modeling large and complex systems.

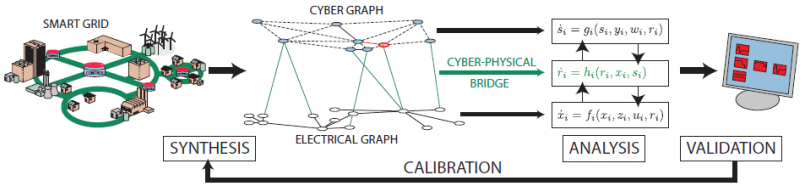

Figure 3.8: Stages of Proposed Impact Analysis Approach, reproduced from [29]

3.5.2 Hardware Simulation

Lu, De, and Song worked on developing a Smart Grid test-bed in [30]. The motivation for doing this was to develop a tool that could be used by researchers to test different designs. Software simulations can only provide approximate models of the Smart Grid, and because of this a physical model was built in [30]. This test-bed can be used to test many different aspects of the Smart Grid including security.

The contribution from [30] is a scaled down Smart Grid model using hardware. The benefit of using this type of model is that it can capture many of the physical characteristics that are too complicated to model using software. However, using this type of model does restrict what kind of tests can be run since hardware must be configured to run the test.

The work in [30] provides designers with a method of testing different Smart Grid designs. There are definite benefits of using hardware to model the Smart Grid, but it also has limits. The hardware model is scaled down so it will not accurately represent the power flow that the Smart Grid would have. Also this type of model requires more hardware to be scaled up, so it is not as flexible as software simulation.

Chapter 4

Conclusion

The Smart Grid is an upgrade to the current electrical power grid. This upgrade is in response to changing consumer requirements for the 21^{st} century. Several cyber security risks will be present in the Smart Grid, and research has been done to identify and mitigate these risks. The Smart Grid cyber security research is separated into five different categories: PCS Security, Smart Meter Security, Power System State Estimation Security, Smart Grid Communication Protocol Security, and Smart Grid Simulation for Security Analysis.

PCSs have been in use for some time now, but not in an environment like the Smart Grid. Traditional PCSs were designed with limited or no security, so a complete set of security tools and policies will need to be developed for these systems. The security vulnerabilities provided in [11, 13] and the risk assessment methods in [11] can be used to develop security tools and policies for the PCS. One of the security tools that can be used on the Smart Grid PCS is the IDS in [12].

There have been several security risks identified with Smart Meters, and many of these risks need to be addressed before Smart Meters can be used in large-scale environments. So far work has been done in three security areas for Smart Meters. An IDS is designed for Smart Meters in [14]. Work has been done with securing redundant Smart Meter reading systems in [18]. Finally, several researchers have looked into Smart Meter anonymity and privacy in [15, 16, 7, 17].

The power system state estimation model used in the Smart Grid will be at risk of cyber attacks. One of the attacks against this model is a false-data injection attack. The work in [19, 20, 22] addresses different aspects of this type of attack. Since the power system state estimation model makes up a critical section of the Smart Grid's functionality, the work in [21] uses the power system state estimation model to determine the communication channel capacities that will be needed to ensure secure communications. There are many other kinds of attacks that can be performed against the state estimation model that will need to be researched.

The Smart Grid will need to use many different communication protocols because of the varying requirements of the many Smart Grid components. An authentication protocol design guideline was developed in [24] that can be used by protocol designers. There has also been work done with real-time communication in [27] and Smart Meter communication in [23, 25]. In addition to communication protocol work, some work has been done with cryptography in [26].

Simulating the Smart Grid can be used to evaluate cyber security. Smart Grid simulation is broken up into two types: software and hardware. Two software simulations [28, 29] and one hardware simulation [30] have been developed for the Smart Grid. Work in developing viable Smart Grid simulators will help improve the Smart Grid design process.

In conclusion, security is a never-ending game of wits, pitting attackers versus asset owners. Smart Grid cyber security is no exception to this paradigm. The Smart Grid is a large and complex system that will be geographically spread out over a large area, and protecting it against attackers will be a challenge.

Chapter 5

Future Research

5.1 Smart Grid Cyber Security Simulation

Smart Grid simulation is needed by designers to evaluate different Smart Grid design options. There are already several systems available for simulating different aspects of the Smart Grid. However, there is still a need to develop a simulation system for Smart Grid cyber security. The existing simulation systems can be used to some extent to test cyber security, but it is not their main focus. A Smart Grid cyber security simulator would need to be able to model the interactions of different components within the Smart Grid. There is also a demand for a simulator that can be used to model the Smart Grid at a national level, so the Smart Grid cyber security simulator should be able be to collaborate with a larger system running several different simulations. The resulting output should be a theoretical model for simulating Smart Grid cyber security and a working prototype.

There are several benefits to doing this research. The cyber simulator would be valuable to Smart Grid designers when evaluating cyber security. In addition, developing a cyber security simulator would provide experience in theoretical model design and implementation. The combination of knowledge in cyber security, theoretical modeling, and Smart Grid design will provide many career path opportunities. This research can also be used as a prelude to work on a comprehensive Smart Grid simulator.

There will be many challenges in creating a Smart Grid cyber security simulator. The first challenge will be developing a comprehensive model. The Smart Grid is a large and complex system, and accurately modeling it will be a challenge. Another challenge will be making the model scalable. The simulator will need to handle a large amount of inputs to model the Smart Grid at a national level. It will be a challenge developing a model that can be arbitrarily modified to accommodate different Smart Grid designs.

5.2 Smart Grid PKI

Cryptography is needed in the Smart Grid to provide data integrity and confidentiality. Before cryptography can be used, a method of securely issuing and exchanging cryptographic keys is needed. Smart Grid Public Key Infrastructures (PKI) research is a possible future research topic. The Smart Grid will have many different communication protocols, and each of them will have their own set of cryptography requirements. A PKI will need to be developed that can meet the needs of all the different communication types. One possible PKI design could mimic the

layered approach that communication models use. This would allow better interoperability between different cryptographic systems.

There are several benefits to doing PKI research. A Smart Grid PKI is needed for the Smart Grid to operate securely. Work in designing public key interfaces would provide valuable experience with cryptographic methods and protocols. There is always a need for better cryptographic systems, and this research could lead to many different research areas.

There are several challenges in developing a Smart Grid PKI. The Smart Grid is a large system made up of many different types of devices and communication requirements. The Smart Grid PKI will need to be able to accommodate the different devices and security needs. The Smart Grid will also have limited bandwidth available, so the PKI will need to have low network traffic overhead. Another challenge is that access to a central server is not ideal, so it will need to be distributed.

5.3 Smart Grid Message Anonymization

The data that the Smart Grid is collecting and generating has raised several privacy concerns. Much of the data in the Smart Grid does not need to be attributed to a specific sender. Research is needed into methods of sending data anonymously that do not violate data integrity constraints. Smart Grid users will expect some level of anonymity relative to what they have with the current electrical power grid. There has already been some work in several areas of this topic.

There are several benefits to doing research in message anonymity. Anonymity can be a very powerful tool in the age of digital media. Anonymity is useful for maintaining freedom of speech, and it allows individuals to express their thoughts without fear of prosecution. Anonymity is a double-edged sword, and with the ability to do good also comes the ability to do bad. Anonymity is an important topic as digital media changes over time, and it would be a rewarding research topic that would provide many career and research opportunities.

There are many challenges with developing data anonymity protocols in the Smart Grid. The anonymity cannot violate any data integrity constraints on the system. Also, the Smart Grid is a critical structure so complete anonymity may not be desirable. Authorities will need to be able to track any parties that attack the Smart Grid, but it should not be easy for any other parties to break the data anonymity.

Bibliography

[1] NETL, *The NETL Modern Grid Initiative Powering our 21st-Century Economy: MODERN GRID BENEFITS*. Department of Energy, 2007.

[2] DOE, *Final Report on the August 14, 2003 Blackout in the United States and Canada*. U.S.-Canada Power System Outage Task Force, 2004. [Online]. Available: https://reports.energy.gov/BlackoutFinal-Web.pdf

[3] M. J. Assante, "Infrastructure Protection in the Ancient World," *Hawaii International Conference on System Sciences*, vol. 0, pp. 1–10, 2009. [Online]. Available: http://www.inl.gov/nationalsecurity/energysecurity/d/infrastructure_protection_in_the_ancient_world.pdf

[4] NewScientist, "Solar power could crash Germany's grid," 2010. [Online]. Available: http://www.newscientist.com/article/mg20827842.800-solar-power-could-crash-germanys-grid.html

[5] NIST, "Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, NISTIR 7628," 2010. [Online]. Available: http://csrc.nist.gov/publications/PubsNISTIRs.html

[6] CNN, "Staged cyber attack reveals vulnerability in power grid," 2007. [Online]. Available: http://www.youtube.com/watch?v=fJyWngDco3g

[7] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Security Privacy Magazine*, vol. 7, no. 3, pp. 75–77, 2009. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5054916

[8] G. W. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870–1891, 1992. [Online]. Available: http://www.georgehart.com/research/nalm.html

[9] C. Laughman, K. Lee, R. Cox, S. Shaw, S. Leeb, L. Norford, and P. Armstrong, "Power signature analysis," *Power and Energy Magazine IEEE*, vol. 1, no. 2, pp. 56–63, 2003. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1192027

[10] L. Snider, "Xcel smart grid costs blow up, PUC orders more transparency," 2010. [Online]. Available: http://www.coloradodaily.com/cu-boulder/ci_14346139#axzz17mrIQg00http://www.smartgridnews.com/artman/publish/Business_Policy_Regulation_News/Boulder-SmartGridCity-Cost-Overruns-How-Bad-is-it-Really-1868.html

[11] Y. Jiaxi, M. Anjia, and G. Zhizhong, *Cyber Security Vulnerability Assessment of Power Industry*. IEEE, 2006. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=4142474

[12] A. Valdes and S. Cheung, "Intrusion Monitoring in Process Control Systems," in *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences HICSS*, 2009, pp. 1–7. [Online]. Available: http://www.scopus.com/inward/record.url?eid=2-s2.0-63349108749&partnerID=40&md5=eec74ad2fb2139c2337a985db232b55chttp://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.146.3823&rep=rep1&type=pdf

[13] D. Watts, "Security and Vulnerability in Electric Power Systems," in *35th North American Power Symposium 2003*, 2003, pp. 559–566. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.69.4104&rep=rep1&type=pdf

[14] R. Berthier, W. H. Sanders, and H. Khurana, "Intrusion Detection for Advanced Metering Infrastructures: Requirements and Architectural Directions," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 350–355.

[15] C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 238–243.

[16] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 232–237.

[17] NIST, "Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid," 2010.

[18] D. P. Varodayan and G. X. Gao, "Redundant Metering for Integrity with Information-Theoretic Confidentiality," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 345–349.

[19] G. Dan and H. Sandberg, "Stealth Attacks and Protection Schemes for State Estimators in Power Systems," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 214–219.

[20] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 220–225.

[21] H. Li, L. Lai, and R. C. Qiu, "Communication Capacity Requirement for Reliable and Secure State Estimation in Smart Grid," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 191–196.

[22] L. Xie, Y. Mo, and B. Sinopoli, "False Data Injection Attacks in Electricity Markets," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 226–231.

[23] A. Bartoli, J. Hernandez-Serrano, M. Soriano, M. Dohler, A. Kountouris, and D. Barthel, "Secure Lossless Aggregation for Smart Grid M2M Networks," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 333–338.

[24] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, and E. Heine, "Design Principles for Power Grid Cyber-Infrastructure Authentication Protocols," in *Hawaii International Conference on System Sciences*, 2010. [Online]. Available: http://netfiles.uiuc.edu/hkhurana/www/IllinoisGridAuthenticationPrinciples.pdf

[25] F. Li, B. Luo, and P. Liu, "Secure Information Aggregation for Smart Grids Using Homomorphic Encryption," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 327–332.

[26] H. K.-H. So, S. H. Kwok, E. Y. Lam, and K.-S. Lui, "Zero-configuration Identity-based Signcryption Scheme for Smart Grid," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 321–326.

[27] J. Zhang and C. A. Gunter, "Application-Aware Secure Multicast for Power Grid Communications," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 339–344.

[28] T. Godfrey, S. Mullen, R. C. Dugan, C. Rodine, D. W. Griffith, and N. Golmie, "Modeling Smart Grid Applications with Co-Simulation," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 291–296.

[29] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 244–248.

[30] G. Lu, D. De, and W.-Z. Song, "SmartGridLab: A Laboratory-Based Smart Grid Testbed," in *2010 First IEEE International Conference on Smart Grid Communications*, 2010, pp. 143–148.

[31] M. Amin, "Toward self-healing energy infrastructure systems," *Computer Applications in Power, IEEE*, vol. 14, no. 1, pp. 20–28, 2002.

[32] E. L. Quinn, "Privacy and the New Energy Infrastructure," *Social Science Research Network*, 2009. [Online]. Available: http://ssrn.com/paper=1370731

[33] "OpenDSS Users Manual." [Online]. Available: http://electricdss.svn.sourceforge.net/viewvc/electricdss/doc

[34] "Network Simulator ns-2." [Online]. Available: http://www.isi.edu/nsnam/ns/