HOME AREA NETWORK SECURITY AND ACCOUNTABILITY

IN THE SMART GRID

by

ERIC MCCARY

YANG XIAO, COMMITTEE CHAIR
MONICA ANDERSON
RANDY SMITH
JINGYUAN ZHANG
VIOLA ACOFF

A DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the Department of Computer Science
in the Graduate School of
The University of Alabama

TUSCALOOSA, ALABAMA

2015

ABSTRACT

The presented dissertation concentrates on the security landscape in smart grid and proposes works to create a more accountable environment in the smart grid home area network (HAN). The principal thought behind the research is security and accountability in the smart grid and the smart grid HAN. Creating a more accountable HAN environment is essential in addressing these matters. More specifically, accountability as it pertains to the HAN, can be described as an assurance that each device within the HAN is held responsible for its own behavior and that those behaviors which belong to it are all provable and non-repudiation is upheld at a more intricate level than current offerings provide. Therefore, the dissertation addresses accountability in the HAN by methods implementing fine grained observation and monitoring of the devices therein.

The first work of the dissertation addresses security in the smart grid. Recent work in smart grid has failed to give detailed holistic accounts of techniques which exploit several issues and vulnerabilities within the infrastructure and software which makes up the smart grid. Therefore, a holistic view which covers malicious actions and their impact on the grid and its components is provided. Countermeasures for these exploits are also discussed. Next, we propose an accountable method which provides for grouping and inspection of the devices in the HAN in order to efficiently pinpoint malicious and malfunctioning devices therein. The experimental results show that the method is effective in its efficiency and scheme. Lastly, we develop a method which addresses accountability of devices in the HAN which use varying amounts of energy during its operational phases. Method analysis and simulation results show that the method is effective, and

that the method maintains a false alarm and error rate that is acceptable based on today's standards without prolonged training times.

DEDICATION

I dedicate this dissertation to my loving parents, Alfonzia and Vanessa McCary. I also dedicate this dissertation to my family, friends, and church family who have supported me through the process.

LIST OF ABBREVIATIONS AND SYMBOLS

HAN Home Area Network

NAN Neighborhood Area Network

NIST National Institute of Technology and Standards

IDS Intrusion Detection System

DR Demand Response

SCADA Supervisory Control and Data Acquisition

AMI Advanced Metering Infrastructure

SM Smart Meter

MMI Malicious Meter Inspection

VC A device which uses varying consumption of energy

LAN Local Area Network

HVAC Heating ventilation and cooling

AMR Automatic meter reading

PDT Probability distribution table

LM Load Monitoring

NILM Non-intrusive Load Monitoring

ESI Energy Services Interface

ST Sub-threshold

d	*D*evice
w_d	Witness of device d in the target-witness device structure
t_d	Target of device d in the target-witness device structure
D	The set of all devices in the HAN
I	The set of inspecting devices in the target-witness device structure
p_d	Probability of detection
p_a	Accuracy of Detection
G_p	Range of possible energy usage for a device
PKI	Public Key Infrastructure
VPN	Virtual Private Network
XSS	Cross-site Scripting
XSRF	Cross-site Request Forgery
PMU	Phasor Measurement Unit
PLC	Programmable Logic Controller
IED	Intelligent Electronic Device
ISO	Independent System Operator
RTO	Regional Transmission Organization

ACKNOWLEDGEMENTS

I would like to thank my committee members who were more than generous with their expertise and precious time. A special thanks to Dr. Yang Xiao, my committee chairman for his effort in reviewing and encouraging, and most of all patience throughout the entire process. Thank you Dr. Viola Acoff, Dr. Monica Anderson, Dr. Randy Smith, and Dr. Jingyuan Zhang for agreeing to serve on my committee.

I would also like to acknowledge the Department of Computer Science at The University of Alabama for continued support and assistantship opportunity.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1. Research Issues

1.1.1. Smart Grid Security Issues

Current literature which addresses security in the smart grid landscape tends to exclusively discuss issues without directing intention toward providing a holistic review of attacks and their countermeasures. While detailing issues in security is important, detailed descriptions of attacks are integral for advancement of knowledge and identification of future attacks and growing trends. Also, understanding current attacks and their countermeasures allows for deeper understanding of security and the smart grid's domain specific requirements as its mission critical components require.

1.1.2. Smart Grid HAN Accountability Issues

Accountability has previously been viewed as a complimentary category to the major components of security (confidentiality, integrity, and accountability), and has a lengthy history of being viewed as a secondary security property. Recently, accountability has assumed a more prominent role in the smart grid security hierarchy, although, while the awareness of this principal has been increasing in current literature, the definition of accountability itself differs from environment to environment. Currently, accountability in the distribution domain of the smart grid has been limited to the aggregated energy usage per home or business and the actions therein. This definition is due to the primary goal of the smart grid which is to distribute and attribute energy

usage and pricing to each of its customers. Therefore, making each of the customers accountable for their usage is of the utmost importance. The inefficiencies of this level of accountability tends to create inaccuracies that fluctuate and are unpredictable, especially when load monitoring techniques are implemented for estimation.

In this domain, where governmental overreach is extremely limited due to privacy laws and concerns, and requirements are different from any other types of networks that have been utilized in the past, organized legislation is severely lagging behind implementation. In some cases standards and requirements are non-existent. Therefore, several immediate challenges arise. First, accountability must be defined for the domain in which we are concerned with. In addition to this, the definition of an event and a device or entity must be defined for the entities which reside on the network of concern. Finally, once the concepts and mechanisms are put into place which extend the capabilities of the network, performance is a major consideration. Especially in the case of smart grid where real-time measurements and communication are required. Many mechanisms which provide for the security of a network create such overhead that they are not ideal for an environment such as this, therefore they are rejected.

Achieving a secure environment in itself is a very difficult task. In the case of smart grid, which is comprised of many distributed systems and has a cyber as well an advanced physical presence in a fairly uncharted research and scientific domain is exceedingly difficult. Therefore, it is important to establish methods which will create and maintain a higher level of accountability in the networks in which a large portion of the smart grid data originates.

1.2. Organization

The rest of the dissertation is organized as follows. Chapter 2 gives some background and basis for the research and methods to be detailed in later sections. This includes security in the smart

grid, and accountability issues in the HAN. Chapter 3 surveys the smart grid security landscape providing details of modern grid vulnerabilities and their exploits. Countermeasures are also specified. Chapter 4 addresses malicious device inspection in the smart grid HAN. Chapter 5 details accountability of devices with varying energy consumption properties in HAN, and proposes a method to address this. Finally, the dissertation is concluded in Chapter 6.

1.3. Publication

Table 1.1: Publications

Chapter 3	Journal	Eric McCary and Yang Xiao, "Smart Grid Attacks and Countermeasures," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems (INIS)*, Volume 2, 2015.
Chapter 4	Journal (TBD)	E. McCary and Y. Xiao, "Malicious Device Inspection in the Smart Grid HAN," Work in progress.
	Conference	E. McCary and Y. Xiao, "Malicious Device Inspection in the Smart Grid HAN," *Proceedings of The 2014 International Conference on Security Management* (SAM '14), 2014.
Chapter 5	Journal	E. McCary and Y. Xiao, "Smart Grid HAN Accountability with Varying Consumption Devices," Manuscript submitted to (Wiley) *Security and Communication Networks*,
	Conference	E. McCary and Y. Xiao, "Smart Grid HAN Accountability with Varying Consumption Devices," *Proceedings of The 2014 International Conference on Security Management (SAM '14)*, 2014.

CHAPTER 2

BACKGROUND

The smart grid can be described as a physical and cyber upgrade to the current power grid which will allow the smart grid to diagnose and heal itself, dynamically integrate renewable energy from various sources, and provide the customer more control over electricity demand and cost [1]. The National Institute of Technology and Standards (NIST) defines six key areas which a smart grid is composed of [2]:

- Bulk Generation Domain
- Transmission Domain
- Distribution Domain
- Operations Domain
- Service Provider Domain
- Customer Domain

These areas are expressed as domains, with each housing several major components which are conducive to the operation of the grid. Each of these domains likely will have a unique distributed computing environment, sub-domains, and equipment to suit its mission-specific needs.

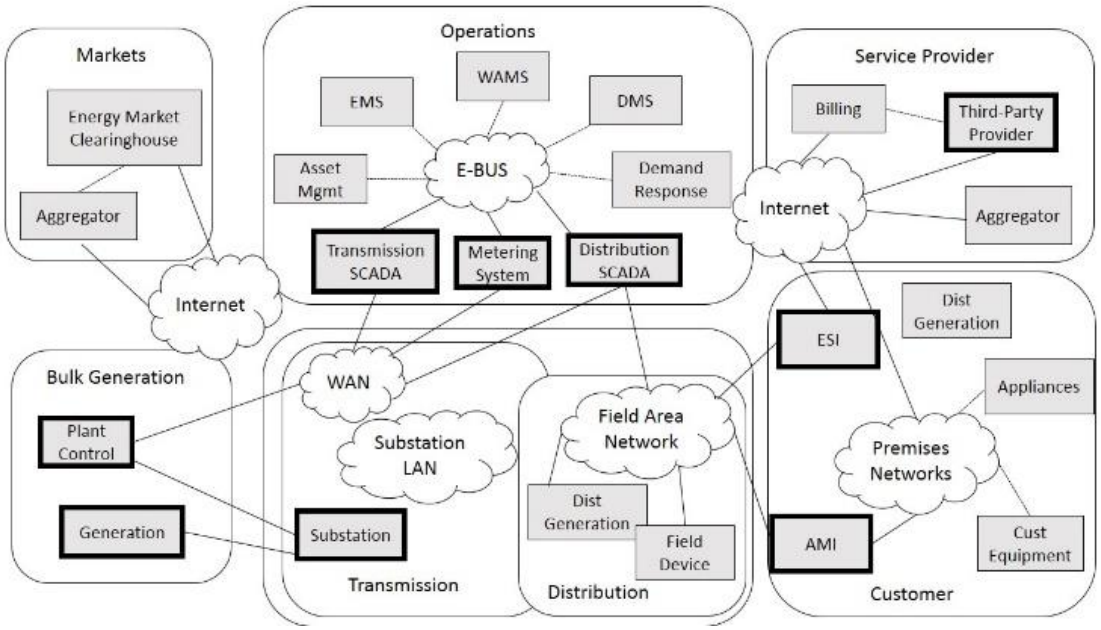

Figure 2.1: Smart grid overview

Figure 2.1 provides an overview of a conceptual smart grid with a view of networks and the physical components therein. It is also important to note that the domains of the grid are interconnected with adjacent domains which provide coordinated functionality. This property creates opportunity for advancement in resources and technology optimization, while also creating new areas of concern that cannot necessarily be circumvented as this type of wide-scaled advancement has not been undertaken in the past.

2.1. Power Grid Physical Infrastructure

In order for the basic operations of a smart grid to be completed in a power grid, specific equipment must be strategically placed in or nearby the regions being serviced. The physical infrastructure of the smart grid can be described as the hardware that will support the functionality of the energy generation, transmission, and distribution mechanisms. The physical entities present on the smart grid are a combination of advanced hardware designed for frequent monitoring of the grid systems and interconnected devices including their load and resources in real-time. In addition

to management and measurement devices, the grid must maintain hardware to carry out its known functions of generating energy and transporting it.

Bulk generation is the first of the responsibilities of the grid. In this domain, power generation plants play a major role as they generate the energy and are overseen by control systems. The interconnection here with the transmission networks is necessary to move energy from its initial location to remote distributors across the entire service area. Centralized generation stations typically rely on coal, nuclear, natural gas, or hydroelectric methods to achieve energy levels required for mass transmission [3]. Also, solar and wind energy may be used for specific purposes. Large turbines are used and propelled by combustion to produce energy, along with fuel burning engines, photovoltaic panels, and various other generation technologies. Other integral portions of the generation stage include the cooling systems and furnaces/boilers. Energy produced in this sector is moved along transmission lines across transmission domains.

The U.S. power grid is made up of roughly 200,000 miles of transmission lines [4]. These lines act as a vehicle for providing distribution networks with power. Table 2.1 includes some of the major hardware located in the transmission domain works together to achieve its goal. This will help us understand this mechanisms' operation. This division allows for increased efficiency and more reliability in individual grids. Microgrids may be included here, which include localized efforts which encompass the generation, transmission, and distribution domains on a smaller scale. Energy travels over the transmission lines as alternating current (AC) with transformers adjusting the current, stepping it up or down as the current moves into separate portions of the transmission network as necessary.

Table 2.1: Common Grid Hardware [2,5]

Transmission Hardware	**Description**
Transmission Lines/Towers	Serves as transmission level energy vehicle
Substations	Transforms, Regulates Voltage
Control Hardware (Switches, Breakers, Loads)	Controls Flow of Electricity
Transformers	"Transforms" energy between voltages
Capacitors	Energy storage
Supervisory Data and Command Acquisition (SCADA)	Monitors and controls industrial process
Phasor Measurement Unit (PMU)	Measure electrical waves
Data Collector	Collects data

A typical power grid is composed of power stations on both the generation stage and between the transmission and distribution stages, power lines which serve as a vehicle for the either distribution or transmission class power, and transformers to step the voltage up or down as necessary. The smart grid will upgrade this infrastructure to support two way communication and flow of energy. Also, equipment is upgraded for advanced sensing and measurement. These items include PMU, SCADA, and Advanced Metering Infrastructure (AMI) [6]. This equipment has the task of providing the key functionality which is established by Federal Energy Regulatory Commission (FERC) in its policy statement including: efficiency and demand response (DR), situational awareness spanning wide areas, storage of energy, PHEV (Plug-in Hybrid Electric Vehicles), communication networks, AMI, and distribution grid management [2].

The distribution network is composed of distribution class power lines which are used to supply consumers with energy of a lower voltage in comparison to the amount observed in the transmission lines. This energy is delivered once it is stepped down by distribution transformers which reduces the voltage to a level which can be utilized in homes and businesses. AMI resides within this domain. The AMI affords the grid and energy consumer DR, load management, real-time pricing, and distribution automation through the network topology visualized in Figure 2.2.

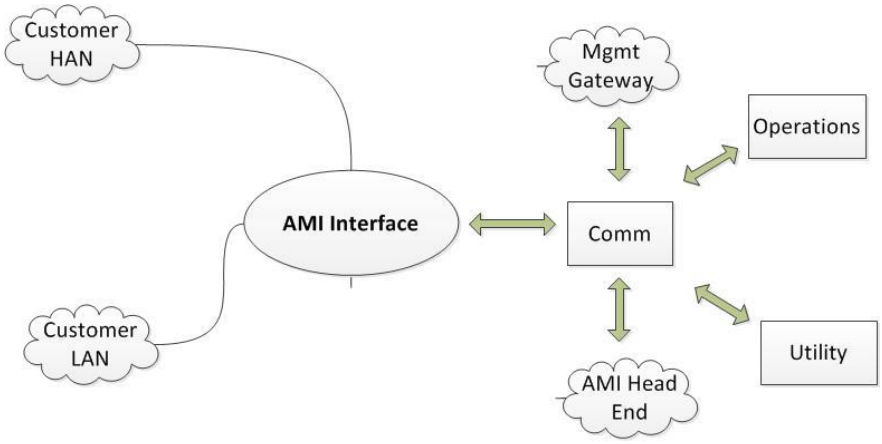

Figure 2.2: Simple AMI Communication Architecture [7]

The endpoints of the AMI normally reside in the customer domain and provide many advanced capabilities due to their proximity and functionality within the customer's network. Intelligent Electronic Devices (IEDs) located in the residential or commercial areas which are connected to the AMI, allow the customers to modulate energy load based on the necessary DR signals or their economic ability or pre-established requirements or preferences. AMI portals are widespread and utilized on a per-vendor basis and allow customers access to their energy usage and pricing information. These interfaces also introduce vulnerability to the smart grid infrastructure.

Other entities important to the grid that span across domains include transportation infrastructure such as roads and bridges. While a great amount of automation is possible in the smart grid, it is still important in some situations to deliver physical service to outlying hardware in the field. Methods to effectively travel to these points in sufficient time to repair equipment are important to grid operation. Buildings and intermediary housing units also play a role in the grid.

2.2. Power Grid Cyber Infrastructure

The cyber layer of the grid is integral as it is where gathering and analysis of real-time data occurs. Consumers, power system operators, ISOs, and producers all utilize this layer of the grid to accomplish various tasks. This data normally contains sensitive information whose availability, integrity, and confidentiality must be retained in order for the proper operation of the grid and its resources. The major parts of the cyber layer of the grid extend from the transmission level down to the distribution level. Figure 2.3 demonstrates this:

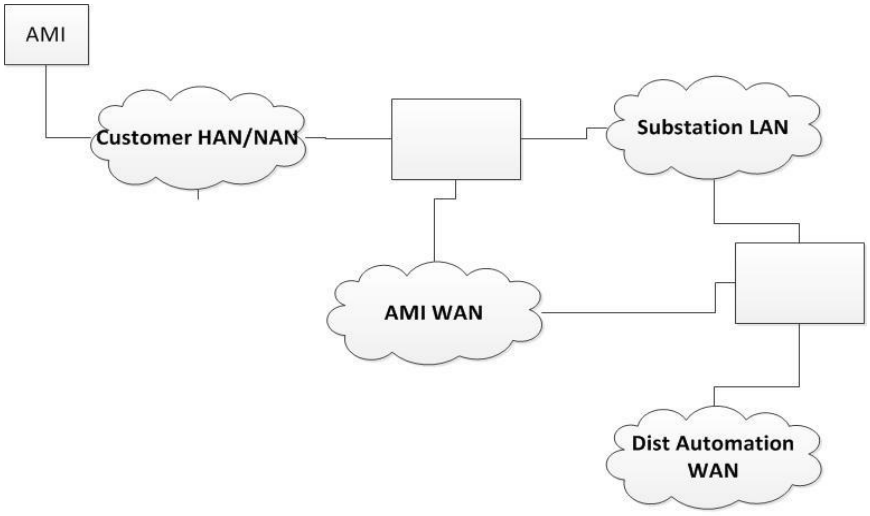

Figure 2.3: Simple Smart Grid Communication Architecture

This layer is composed of several interconnected networks and must communicate across boundaries. As [8] states, many of the connected networks are of a hybrid nature. This means that networks may be composed of differing methods of connectivity such as Wi-Fi communications and satellite. Also, in these integrated networks, there will exist an endless variety of differing requirements, legacy systems, and newer technologies which direct the future trends in the smart

grid systems. This has led to difficulty in establishing a universally adopted set of standards [9, 10-11].

Integration of internet protocol (IP) into grid networks is a major property of the smart grid. IP has become the protocol of choice based on its mature performance, security potential, and reliability [12]. IP will likely be the medium which smart grid devices use to communicate with each other [6]. Successful legacy system activity on the smart grid networks can be accomplished with the implementation of IP [13]. In other words, this protocol allows for encapsulation and many methods which can be used to allow two systems to communicate which normally utilize non-routable communications on a network or with a particular type of connection.

Currently there are many legacy devices still being utilized in grid networks which must communicate and may create vulnerabilities and other difficulties such as bottlenecks. As cost is always a factor, it is very likely that these technologies will continue to exist through the near future.

2.2.1. Monitoring and Visualization

As per the definition of a smart grid, the entity must have monitoring and sensing capabilities spread throughout. These modules acts as the "eyes and ears" of the grid which provide frequent diagnostic data from specific devices which can yield grid state information. Enhanced capabilities in sensing and monitoring allow for detection of anomalies in the grid, which then can be resolved by automation controls in the monitoring device software. Problems that require a more intensive solution are generally resolved by sending crews to physically manage affected devices or strategically re-route power and services.

Sensor technology is also important in the estimation of customer load [14, 15]. AMI technology on the utility side can be used to predict the times during the day that electricity prices will be at

their peak. This gives customers the decision to modify their energy usage during those peak times. Less demand equates to lower peak prices and less energy waste for the whole energy sector.

Functionality provided by SCADA and Remote Telemetry Units (RTUs) allow for controlling and management of the transmission layer devices [16]. Many different types of sensors are currently in use on the smart grid architecture. A list of some of the technologies is located below: regulators, smart voltage sensors, smart capacitors, dissolved gas sensors (transformers), temperature sensors, line condition sensors, and weather sensors [17].

Once measurements are sent to the appropriate entities and verified, the results can be viewed on an Energy Management System (EMS) which may provide an interface to the control capabilities in order to make appropriate modifications to grid operations. Devices such as the PMU sense and relay measurements to control centers where they are aggregated and compared to policy guidelines to determine whether or not action is necessary to ensure proper operation of the grid. This is one portion of the demand-response regulation procedure which keeps utilities from wasting money by having excess power wasted, or brown/black-outs from occurring due to too little power flow. One method of sensing in the smart grid is to establish policy for state in the grid, and the specific bounds which encompass a "good" state, where measurements outside of these ranges signify a fault or intrusion on the grid. These system stability or state recognition readings may be the magnitude or phase angle recorded from a remote PMU which is relayed to a control center or substation for analysis and monitoring.

2.2.2. Analytical Capability

The cyber layer in the transmission and distribution domain is responsible for monitoring and analyzing state variables and preventing or correcting faults or predicted conditions in the grid. Stability analysis is the key in the grid as automation is one of the attributes in the architecture. As

long as actions are defined in the policy which is specified in the grid, there should be no difficulty creating automatic response functions due to state sensing and measurements. The North American Electric Reliability Corporation (NERC) maintains a public list of reliability standards which helps to regulate and standardize cyber requirements in the US electric grid [18].

2.3. Security in the Smart Grid

The modernized grid can be visualized as having two separate layers which will make up a complex cyber-physical system. This manner of description combines the current power grid which is composed of generation, transmission, and distribution [19], and a cyber-communication layer for each of the power grid's domains which maintains integrated connections and measures for useful interoperability. These physical and cyber interfaces to allow for proper communication between devices connected to the grid which depend on mass aggregation of customer and equipment operational data.

Changes to the grid infrastructure not only add intelligence and new communication technology, but also utilize the new interfaces to select power systems and devices from open networks which may be facing the internet [1,20]. While the new technology will drastically increase efficiency and reliability, it also substantially increases the potential for vulnerabilities in a smart grid. Designers of many legacy devices with networking capabilities contained here have been neglecting the need for cyber security, and failed to consider these devices being widely connected. Some of the devices employ embedded web services and mobile interfaces which are becoming increasingly popular among vendors to service customers in providing them with energy information, which makes target environments more vulnerable.

More efficient management of active grid devices can result in sizeable financial savings for the customer, and utilities. Also, this management of energy will allow for more efficient energy

generation and distribution. The widely connected grid is integral to modern society, and generation and consumption must remain mostly balanced as it is produced and consumed. Potential cascading failures and power outages are possibilities if this condition is not met. The integration of previously separate portions of the grid incidentally interconnects legacy devices and software in the grid and implements current technology and smart devices alongside these devices. Some of the more modern equipment employs legacy software such as Windows operating system components as well as vendor created solutions which allow for advanced operations necessary for smart grid operation, but also create vulnerabilities unique to those systems or, in other cases, widely known to the public and which may be exploited in some of the grid environment [26].

With the level of scalability and interoperability that a smart grid maintains, it is important to understand the physical and cyber ramifications that are a possibility with lacking standards and security implementations. Without these, as [27] points out, attacks and other misfortunes on the grid will likely lead to cascading failures and power outages. To convey a context for understanding this necessity, this study gives a review of past attacks and vulnerabilities of the smart grid and also inspects and highlights some areas for additional research which may reveal other weaknesses.

2.4. Accountability in the Smart Grid

Security has most recently been one of the key areas of research in the smart grid landscape. This a very common occurrence in the introduction of new technology. While security is generally a main research topic, accountability serves as a complement to the core principals of information security and the component that allows authorized individuals more robust tracking and auditing history as well as establishing trust and confidence between devices. Currently, accountability in

the distribution end of the smart grid infrastructure only extends to a single residence which aggregates the appropriate data and energy usage amount of all of the devices located therein. This widely utilized method of estimation is minimally sufficient for the currently required duties of billing the customer based on total use of all appliances and devices to be fulfilled. It is also important to note that functions requiring high computational resource loads are discouraged in the smart grid as the devices utilized throughout are normally resource constrained, or given computational and networking resources that are not plentiful enough to handle heavy encryption and simultaneously satisfy the real-time demands of the grid. This also applies to any subset of software functionality included in the grid including accountability measures.

There are several requirements which can contribute to an effective accountable environment or mechanism. These include [28]: decentralization of accountability mechanisms, scalability, minimal impact, data collection, identity management. Inclusion of these elements in any network where accountability is required can be very profitable and will help to cover the accountability requirements. Along with these measures, sufficient and appropriate data must be extracted and archived for review and evaluation. It is imperative to discern the most effective location and type of data to archive and evaluate in each environment. Some devices may require a specific set of data to be analyzed, while others may require a set of data which includes a few of the parameters explicitly required by one, and a few not needed to satisfy the requirements of another. Although in most environments these parameters will be uniform.

Inter-domain identification is also necessary. Normally, devices in the same domain will maintain uniform identification mechanisms which will allow them to distinctly refer to and differentiate between devices on the network. For smart grid applications, the main objective of accountability currently is to maintain record of and assure that a device has acted as it says and/or

is expected to. In terms of the smart grid, a network should not only truthfully report/observe its device's network actions, but also its power usage, and other parameters required at a pre-specified time interval and/or when requested.

Maintaining the previously listed requirements for achieving accountability in a smart grid environment is a huge upgrade to still widely implemented automated meter reading (AMR) infrastructure in which the sum of the power over a certain period is collected from aggregate data of all devices at the customer's residence. Even in the case of AMI, there is still much room for error and we simply cannot expect for the record that the utility manages and what is recorded at the customer's end to be identical. Malicious action, malfunction, miscalculation in estimation, or calibration may be the cause of such differences.

2.5. Energy Consumption in the HAN

Energy sustains life for many people, therefore, domestic usage is behind a large portion of most grids energy consumption. Many devices and methods are being put into place which will give consumers the option of employing more energy efficient options in their homes. Gaining energy efficiency is synonymous with reduction of energy used for a given service or level of activity due to some technological change of an existing infrastructure [29,30]. This is of particular interest, as the majority of consumers prefer to purchase the lower end devices which though cheaper, also tend to provide less in the area of energy efficient components in software and hardware [31].

Many factors are combined to determine household consumption rates. These are highly affected by consumer personal preference and many external conditions such as weather and temperature. Energy consumption here is transient and varies dramatically at specific times. These factors play a large part in the determination of the peak times which are defined by the utility based largely on the overall usage of its customer base and the availability of the generated energy. Peak rates

are normally achieved during specific times of day when many consumers use considerable amounts of energy. While the bulk of energy used in the home is consumed by large appliances, they are normally outnumbered by smaller devices that use considerably less energy. As the number of smaller devices grow, it can be expected for the amount of energy used by the smaller devices to become more comparable to the larger devices. With this type of infrastructure widespread, use of many small devices simultaneously will trigger peak times and rates as easily as a moderate number of higher consumption devices.

2.6. Home Automation

Scheduling in the HAN is a product of home automation. With local generation included, the energy management mechanism in the home can utilize its distributed energy resources (DER) and maximize the net benefits for the end user. An effective scheduling system efficiently distributes various HAN tasks to the capable components in order to implement ubiquitous homes services that efficiently control the devices therein. The scheduling scheme must accommodate several requirements in order to meet smart grid standards, these include [32]: sensing and measurement, context awareness, and service management.

There must be some set of components in the HAN with the responsibility of sensing in the environment. This creates data which is forwarded to a component which is tasked with decision-making. These variables which are sensed and tested in the environment have a known context which the devices in the HAN are aware of. Context in the sense of the smart grid HAN helps devices understand implicit information which can be associated with their responsibilities such as services offered to the consumer in the home where the following offerings should be available and implemented [31]: *Information* – Graphically represented energy usage data, *Automation* – priority setting and scheduling**,** *Advanced Control* – Information and control locally of from third

parties, *Integration* – Use of all previous offerings and forecasting information.

Implementation of the previous offerings allows for a much "smarter" home environment. In these smart homes, many new components are being added in order to complete its objective of minimizing the daily energy costs and reducing the energy consumption at peak times. This is accomplished by scheduling tasks that use energy around specific times of day that most energy customers will be using energy. These times can be can be described as energy prices being at their "peak" due to high utilization and the power companies necessity to add extra generation capabilities to accommodate the extra power demand.

Energy efficiency measures can be more effective when decentralized generation is introduced into the home area. This creates a micro-grid environment which generally has limited resources with some interface to the major servicing power grid. It is still expected that there will be a connection to the conventional power grid maintained in the instance that the local generation capacity is more or less than the residence needs, giving the customer the capability to purchase or sell the excess generated power back to the utility or others in the NAN.

2.7. Attacks and Countermeasures

Security pertaining to smart grid and the components within has been on the forefront of smart grid literature and discussion over recent years. [19] utilizes a custom cyber-security testbed architecture in order to detail attack and mitigation scenarios within that simulated microgrid environment. These scenarios utilize common hacking tools to exploit vulnerabilities while mitigation is attributed to anomaly-based Intrusion Detection Systems (IDS) and firewalls. [33] summarizes some of the requirements and vulnerabilities of the current grid. Many of the protocols and common practices are included here. Vulnerabilities and challenges are detailed well. [9] gives an overview of the relevant cyber security and privacy issues along with some recommendations

proposed by NIST and other recent works. [3] presents a review of the work related to guaranteeing availability in smart grid communications. A common communication topology is detailed in which privacy compromising attributes are discussed. Authors in [34] supply the reader with some attack categories. Some security fundamentals in the areas of access control, authentication, and privacy along with intrusion detection are also discussed. Recent work in this area has, understandably, failed to give detailed descriptions of techniques which exploit these issues and vulnerabilities in the smart grid and its technologies due to the security risks involved. Although, some argue that unveiling vulnerabilities furthers security in industry by forcing security technicians to address these matters.

In order to understand security differences in cyber-physical systems as opposed to traditional Information Technology (IT) systems, we must assess not only at attacks that originate in a given cyber domain, but also those originating in, or propagating through several domains, both cyber and physical [20]. Once those interactions are understood, both cyber and physical means must be used to mitigate the impact of cross domain interactions.

One of the benefits and most integral attributes of the grid is its two-way communication which allows utilities and customers to relay data between each other on a real-time basis, it is imperative for these data transactions to be secured. This level of communication also creates vulnerabilities in grid communication with a broadened surface for cyber-attack and data tampering. Initially the protocols used in communications and the devices which interfacing the gird were proprietary and detached from outside networks. This basically suggests that grid networks employed "security by obscurity" instead of "defense-in-depth". Normally the design of these networks and mechanisms implemented in them were not initially assembled or created with security in mind. As time has progressed, vendors have incorporated security into the device designs, and the protocols in use

on smart grid networks have adapted to the malicious threats and individuals threatening critical infrastructure.

There are some obvious and interesting differences in the priority of security objectives in the smart grid and contemporary IT networks. The security requirements rely heavily on the domain under consideration in the grid. We first look at the CIA Triad and understand that the order of objectives here are different from those in the traditional IT network. This is partially due to the personally identifiable information that is aggregated and communicated back and forth from consumer to utility over public internet channels, and the publically available resources in the field. In addition to these circumstances, functions in the smart grid are normally dependent on strictly timed mechanisms, as its operation is of a real-time nature. When combining this with the fact that many of the devices therein are resource constrained, the smart grid infrastructure is very different from what is found in traditional IT networks. Utility companies collect and store information belonging to the customer including name, address, consumption data, and social security number. Each of the attributes should be kept confidential and away from hackers attempting to affect them or the grid maliciously. While IT security techniques are valid and will be implemented in the smart grid in an effort that likely will satisfy security many requirements, the tradeoff between security cost and performance must be understood to validate specific implementations.

2.8. Confidentiality

Confidentiality in smart grid deals with restricting unauthorized explicit and implicit information dissemination. Exploits may result from unauthorized access to a system or the network that it interfaces, or an insider acquiring data with either malicious or even unauthorized benign intent. Data moving across smart grid networks contains power usage information and other private and sensitive data that can be detrimental to a consumer. Malicious attackers can infer

specific details from energy usage patterns and fashion an attack according to the details acquired from eavesdropping on the smart grid information network. This sensitive information may be sought after by many individuals. For instance, law enforcement could utilize this information to support investigations, not unlike the way cell phone and Global Positioning System (GPS) data is currently used [35].

2.9. Integrity

Integrity in the smart grid refers to modification of devices or data on the grid infrastructure. Normally attacks on integrity in the grid are difficult to accomplish, and require more sophisticated methods to implement. All attacks from network data injection, message replay or masquerading violate integrity on a network. A less exploited vulnerability would be modifying the function of hardware or software on devices before it is shipped from the producer, or modifying images that will be on machines in an operational environment. Malware can be pre-loaded and designed to propagate to other devices on a network. Also, hardware can intentionally be made to falsely read data, and/or malfunction under certain circumstances.

On the consumer's end, where the hardware is much more easily available, a wider range of vulnerabilities exist that can attack integrity. From data injection on a large scale, to AMI cyber-physical tampering, it is important to secure devices and networks on several levels in the cyber and physical layer to ensure integrity on. Normally, due to the operation of the grid, attacks affecting integrity are hard to detect, and in the case of compromising meters and their load information in a coordinated fashion, these are the most prevalent [36-38]. These types of attacks involve stealthy modification of reports intended to inform utilities of resources usages. Changes can be made to deceive the utility into believing that the resident generated an untruthful amount of energy in order to reduce costs of their energy consumption. Whether theft or fraud, these acts

can have devastating effect on the load estimation mechanism in the grid causing too much or too little energy to be produced and eventually failure of select nodes or blackouts/brownouts.

2.10. Availability

Availability can be ensured if smart grid services are protected and accessible to all entities authorized to request them. In the smart grid environment, availability itself is the most important of the immediate security objectives that should be completed in the grid. The critical nature of the grid and its services, along with the necessity of its real-time operation help explain the significance of the requirement of the grids constant availability. Research in availability can be categorized as follows [39]:

- Defense against attacks
- Guarantee of real-time systems
- Communication availability extension

An important part of ensuring availability is understanding the threats posed to an environment. This way, it becomes an easier task to ensure the security of the systems that it is composed of. Once security is ensured, the reliability of the grid is placed solely on the internal function of the hardware and software. The current grid provides a 99% uptime [39]. The near negligible amount of down time is caused by storms, electromechanical arching, and other perturbances that are normally unavoidable. Most of these are physical concerns, but the smart grid upgrade creates vulnerabilities on the cyber side. Malicious control from the cyber side can easily disable systems in the grid and cause widespread downtime and blackouts.

2.11. Varying Consumption Devices

Achieving accountability in the smart grid HAN has rarely been studied in the past. Related areas such as disaggregation and load monitoring [41-43] are useful, but normally estimate device usage based on the aggregate amount from the residence as a whole and the normal consumption

of a device. This type of estimation is more useful when identifying customer behavior patterns and related device malfunctions. Some limited databased appliances identification based on load signature variables has been done with the two load monitoring approaches: non-intrusive load monitoring (NILM), and intrusive load monitoring (ILM). ILM is categorized by its distributed sensing approach where one or more sensors are responsible for sensing each device, and NILM monitors the entire home's power consumption from a single point which is often the smart meter. There is normally a tradeoff in cost, complexity, and precision in choosing between the two of these types of techniques. [44] explores the cost and detail of stand-by power for devices including devices which maintain several states and use varying consumption. Discovering devices and state measurements take principal importance in such studies. [45] categorizes devices based on the type of energy state variations that it may undergo or that are possible in order to identify devices in a network based on their consumption signatures.

2.12. Malicious Network Inspection

Currently for smart grid applications, the main objective of accountability is to maintain record of device power usage and assure that a device acts as it says and/or is expected to. In other words, a device should truthfully report its power usage and other parameters required at pre-specified time intervals and/or when requested. This support is not intrinsic as is evident by [46], which demonstrates that AMI data can be attacked and falsified through several different methods. Studies such as this are important as it displays methods in which the integrity of the data that originates in the HAN can modified maliciously. This makes it obvious that risk is reduced when the nodes in the network are evaluated and inspected from within a distributed mechanism. Even in the case of data reporting, there is still much room for error and we cannot always expect for the record that the utility manages and what is recorded at the customer's end to be identical.

Malicious actions, malfunction, miscalculation in estimation, or calibration may be the cause of such differences. Making the HAN accountable on a more fine-grained level can help alleviate problems such as these and provide us with a means of locating a compromised device which can immediately be disabled or serviced instead of canceling service to the residence until the problem is determined.

The application of accountability has been established in a few works in the NAN in [22,47]. These works provide several linear and tree-based inspection algorithms to address the malicious meter inspection problem (MMI). The work in [23] provides an accountable protocol for use in the HAN, as well as a protocol for the neighborhood area network NAN. The HAN protocol bases its accountability on providing evidences which can discover questionable charges or lack thereof on the final utility bill based on some threshold and detailed logging comparison procedures. Some issues with [23] include the lack of a fine-grained view of accountability which utilizes the aggregate power usage as a comparison factor in it decision mechanism in defining faulty behavior. This may suffer from the same type of vulnerability that distributed false data injection attacks create as falsely reported events will not always be detected as long as the thresholds are not exceeded.

CHAPTER 3

SMART GRID ATTACKS AND COUNTERMEASURES

The development of smart grid brings about an opportunity for advancement in resource utilization and technology optimization, while also creating new areas of concern that have not been evaluated in the current conventional grid. These changes to the power grid infrastructure not only add intelligence and new communication technology, but also create interfaces to select power systems and devices from open networks over the internet [1, 20, 6]. As this new technology will drastically increase efficiency and reliability, it also substantially increases the potential for vulnerability in the grid [19, 20, 6, 9]. Designers of many legacy devices which are currently operating on the grid with networking capabilities have neglected the need for cyber security, and failed to consider that these devices will be widely connected [4,5]. Some of the devices employ embedded Web services and mobile interfaces which are becoming increasingly popular among vendors to service customers in providing energy and pricing information, and this makes target environments more vulnerable.

More efficient management of active grid devices can result in sizeable financial savings for the customers and utilities. Also, this management of energy will allow for more efficient energy generation and distribution. The widely connected grid is integral to modern society, and generation and consumption must remain mostly balanced as it is produced and consumed. Potential cascading failures and power outages are possibilities if this condition is not met. The integration of previously separate portions of the grid incidentally interconnects legacy devices

and software in the grid and implements current technology and smart devices alongside these devices. Some of the more modern equipment employs current software such as Windows operating systems components as well as vendor created solutions which allow for advanced operations necessary for smart grid operation, but also creates vulnerabilities unique to those systems or, in other cases, widely known to the public and which may be exploited in the grid environment [7,48].

With the level of scalability and interoperability that a smart grid maintains, it is important to understand the physical and cyber ramifications that are a possibility with lacking standards and security implementations. Without these, as [49] points out, attacks and other misfortunes on the grid may lead to cascading failures and power outages. To convey a context for understanding this necessity, this chapter will give a review of past attacks and vulnerabilities of the smart grid and also inspect and highlight some areas for additional research which may reveal other weaknesses.

Recent work in this area includes [19], which utilizes a custom cyber-security testbed architecture in order to detail attack and mitigation scenarios within that simulated microgrid environment. These scenarios utilize common hacking tools to exploit vulnerabilities while mitigation is attributed to anomaly-based Intrusion Detection Systems (IDS) and firewalls. The authors in [9] give an overview of the relevant cyber security and privacy issues along with some recommendations proposed by NIST and other recent works. The authors in [50] summarize some of the requirements and vulnerabilities of the current grid including many of the protocols and common practices as well as vulnerabilities and challenges are detailed well. [17] presents a review of the work related to guaranteeing availability in smart grid communications, and a common communication topology is detailed in which privacy compromising attributes are discussed. The authors in [34] provide some attack categories, and some security fundamentals in the areas of

access control, authentication, and privacy along with intrusion detection are also discussed. Recent work in smart grid security has failed to give detailed holistic accounts of techniques which exploit these issues and vulnerabilities in the smart grid and its technologies. Therefore this chapter will cover these malicious actions and their impact on the grid and its components. Countermeasures will also be discussed.

3.1. Security Concerns

The elements of the "CIA Triad" (confidentiality, integrity, availability) generally provide a good baseline for security in major operational systems. These same principals are integral in the context of smart grid security. These automated systems which are also in control of human and equipment safety, help drive the grid to its main objectives. In order to understand security differences in cyber-physical systems as opposed to traditional information technology (IT) systems, both cyber domain attacks, physical domain attacks, and crossing domain attacks should be assessed [51]. Methods from cyber domain, physical domain, and cross domain techniques should be used mitigate exploitation among domains.

One of the benefits of a smart grid is its two-way communication which allow utilities and customers to relay data between each other on a real-time basis. It is imperative for these data transactions to be secured at all costs. This type of communication also creates a broadened surface for cyber-attack and data tampering [52, 53]. Initially, the protocols and the devices used for communication over the smart grid networks were proprietary and detached from outside networks. This suggests and proves that grid networks employed "security by obscurity" instead of "defense-in-depth". Normally the design of these networks and mechanisms implemented in them were not initially assembled or created with security in mind. As time progressed, vendors have incorporated security into the device designs, and the protocols in use on smart grid networks

have adapted to the malicious threats and individuals with access to critical infrastructure which belongs to the grid. A list of popular protocols which these types of devices communicate with is included in Table 3.1.

Table 3.1: Common Grid Communication Protocols [2,8, 54]

Communication Protocol	**Description**
Zigbee 2.0	For use in HAN for device communication
IEC 61107/62056	Smart meter communication protocol
ANSI C12.	Smart meter and HAN device communication protocols
HomePlug	Suite of specifications for communication over home electrical wiring
M-Bus	Protocol for remote metering
Modbus	Standard for communication in industrial devices
OPC Protocols	Open standard specification for publish/subscribe procedure
DNP3	Substation device automation
IEC 60870	Outlines control messages
IEC 61850	Outlines communications between transmission and distribution domains in automation and security

In North America, Distributed Network Protocol 3 (DNP3) is frequently used in process automation for electric utilities. This protocol is built on top of IP and along with IEC 61850 and DNP3 are currently the most widely used protocols [35, 50]. Open Connectivity (OPC) standard is an abstraction layer between components of which implement different and incompatible protocols. Each of these protocols, regardless of popularity have been or will be used in operational settings and should be secured as so.

There are some obvious and interesting differences in the priority of security objectives in the smart grid and contemporary IT networks. The security requirements rely heavily on the domain under consideration in the grid. We first look at the CIA Triad and understand that the order of objectives here are different from those in the traditional IT network. This is partially due to the

sensitive information that is aggregated and communicated between the consumer to utility over public internet channels, and the publically available resources in the field. Utility companies collect and store information belonging to the customer including name, address, consumption data, and social security number. Each of the attributes should be kept confidential and away from hackers attempting to affect them or the grid maliciously. While IT security techniques are valid and will be implemented in the smart grid in an effort that likely will satisfy security requirements, we must understand the tradeoff between security cost and performance to validate specific implementations.

3.1.1. Confidentiality

Confidentiality in the smart grid deals with restricting unauthorized explicit and implicit information dissemination. Breaking confidentiality can be categorized as any unauthorized access to a system or network. Also, any insider acquiring data with either malicious or unauthorized benign intent.

Data moving across smart grid networks generally contains power usage data and other private and sensitive information that can be detrimental to a consumer [48, 52]. Malicious attackers can infer specific details from power usage patterns and fashion attacks according to the details acquired from eavesdropping on the information network. This sensitive information may be sought after by many entities for instance, law enforcement could utilize this information to support investigations, not unlike the way that cell phone and Global Positioning System (GPS) data is currently used [35].

[55] details and expands on work in [56, 57] which describes information flow in environments with multiple security domains. This complicates both the automation processes of devices in a smart grid network and security in these environments. IEC 62351 defines several mechanisms

which are to be used to protect the exchange of information in automation applications used in the smart grid. IEC 62351-3 and 62351-5 provide provisions for confidentiality using Transport Layer Security (TLS) for encryption between devices in the network [46, 58]. Also these protocols adopt a keyed hashing message authentication (HMAC) as specified in IEC 9798-4.

3.1.2. Integrity

Integrity in the smart grid can be discussed in terms of the modification of devices or data on the grid infrastructure. Normally attacks of this nature are more difficult to accomplish, and require more sophisticated methods to implement. All attacks from network data injection, message replay, or masquerading violate integrity on a network. A less exploited vulnerability would be modifying the functions of hardware or software on devices before it is shipped from the producer, or modifying images that will be on machines in an operational environment. Malware can be pre-loaded and designed to propagate to other devices on a network. Also, hardware can intentionally be made to falsely read data, and/or malfunction under certain circumstances.

On the consumer's end, where the hardware is much more easily available, a wider range of vulnerabilities exist that can attack the integrity of the grid components. From data injection on a large scale, to AMI tampering, it is important to secure devices and networks on several levels in the cyber and physical layer to ensure integrity.

Normally, due to the operation of the grid, attacks affecting integrity on a wide scale are difficult to detect, and in the case of compromising meters and their load information in a coordinated fashion, these are the most discussed in literature [36,59,60]. These types of attacks involve stealthy modification of reports intended to inform utilities of resource usage. Changes can be made to deceive the utility into believing that the resident generated an untruthful amount of energy in order to reduce costs of their energy consumption. Whether theft or fraud, these acts can have

devastating effect on the load estimation mechanism in the grid causing too much or too little energy to be produced and eventually failure of select nodes or blackouts.

3.1.3. Availability

Availability is ensured when smart grid services are protected and accessible to all authorized entities requesting them. This attribute is centered on reliability and security of the features providing services. In the smart grid environment, availability itself is the most important of the immediate security objectives. The critical nature of the grid and its services, along with the necessity of its real-time operation help explain the significance of the requirement of the grids necessity of availability. [40] categorizes past research in availability as follows: defence against attacks, guarantee of real-time systems, and communication availability extension.

An important part of ensuring availability is understanding the typical threats that an environment faces. This way it becomes an easier task to ensure the security of the systems that it is composed of. Once security is ensured, the reliability of the grid is placed solely on the internal function of the grid hardware and software barring acts of God. The current grid has provided 99% uptime in recent history [42], and the near negligible amount of down time is caused by storms, electromechanical arching, and other perturbances that are generally unavoidable.

3.2. Hacker's Motives

The heightened level of communications between customers and utilities creates more opportunity for eavesdropping. [42] details motivation for individuals whether malicious or not, to attempt to hack the grid: intellectual stimulation, recognition of peers, power acquisition, terrorism, revenge, penetration testing, curiosity, and monetary gain. The smart grid is not an exclusive attack target for terrorists, there are also individuals with non-malicious aspirations attempting to access and perform acts that may have negative affect on the grid. These efforts can

be carried out with a simple demonstration of power in mind, and end up causing millions of dollars in damage.

3.3. Known Vulnerabilities

While security controls continuously have been making exploitation of obvious and available vulnerabilities more difficult, the devices behind perimeter defences remained un-hardened up to acceptable specifications. Some of the challenges of upgrading the current grid are listed below [61]:

a) Difficulty creating security solutions in complex environment due to propriety nature based on performance and not security,
b) Networking technologies including ModBus, ProfiBus, ICCP, ModBus Plus, and DNP are designed for connectivity and efficiency but not security,
c) Automation systems are composed of legacy systems,
d) Fast addition of new protocols, applications, and requirements are more difficult to make and keep complex systems secure.

SCADA systems are an excellent example of confirmation of these challenges [16]. Older proprietary protocols and software were implemented on these devices rendering them vulnerable to common and easily executable modern attacks. Therefore, it was believed that these obscure devices did not have any threats of note in the past due to its unknown nature and unreachable state. Early versions of SCADA systems hosted vulnerabilities such as allowable default password implementations, missing software patches, and network protocol-based vulnerabilities [62]. These types of vulnerabilities are normally of a vendor-specific nature, and have specially crafted exploit techniques.

Accidental and inadvertent threats are always of concern in any operational environment. These types of events may cause more problems than actual some exploited vulnerabilities by a hacker do to the fallout of insufficient safety procedures, equipment failures, and natural disasters are all of concern.

It is important to consider that legacy systems currently play a large role in smart grid implementations. While observing this fact more often than before, we understand that the smart grid must be defined not only by the new hardware and software, but also by the integration of legacy devices and protocols. Much of the current framework is still comprised of legacy infrastructure and while adding new equipment is necessary, it is generally only upgraded when it is lucrative for the utility or consumers. Typically, these legacy devices maintain inadequate resources and configuration requirements which keep them from implementing sufficient security mechanisms. Several solutions are currently in use, including utilizing secure Virtual Private Networks (VPNs) for remote access, encapsulating the legacy devices, or creating and abstracted layer between the legacy device and the requesting service as an interface to reduce the complexity of actions necessary by the legacy device [62].

3.4. Attack Types

Any infrastructure is vulnerable to attack. Whether the vulnerability is great or small is determined by the exploit mitigation and security techniques implemented around and within it. In the smart grid, specific elements and security requirements are necessary for quality operation. The vulnerabilities which are found within can be described and categorized in many different ways. We can view the weaknesses of the smart grid on a device or entity basis or as a combination of those entities. A list of common entities that have specific vulnerabilities and important purposes on the grid is listed below in Table 3.2:

Table 3.2: Vulnerable Grid Entities [2, 61-64]

Operational Systems	**IT Systems**	**Communication Protocols**	**Endpoints**	**Human Factors**
Generators	PCs	Wifi (IP)	Electric Vehicles	Human Training
Transformers	Servers	Zigbee	Smart Meters	Social Engineering
SCADA	Apps	4G	Mobile Devices	Phishing
PMU	DBs	DNP3	IEDs	Data Transfer
PLC	Web Services	IEC 60870		
Smart Meters		IEC 61850		

Most of the effective attacks which effect the smart grid exploit a combination of several of the vulnerable entities attached to it. Whether the goal is malicious or for testing purposes, normally the exploitation of highly valuable resources employing security mechanisms requires complicated procedures to complete. This normally consists of a coordinated attack carried out in a distributed fashion and utilizing several different types technology and attack vectors.

3.5. Physical Attacks

The smart grids physical footprint is greatly extended to due to the interconnection of consumer home and business networks to traditional smart grid information networks which link to control centers and substations. These newly established connections require equipment to be installed on and near consumer property which will serve as part of the AMI process. This process includes communication of power usage information and other sensitive data between dedicated aggregation points or control centers and customers. Also, sensors and other costly advanced hardware will be placed in publicly accessible areas which are vulnerable to attack.

Physical security is fairly mature and well understood, and while the list of types of physical attacks is relatively short, the possibilities are greatly expanded due to availability. Destruction of equipment and disturbance of availability is the prime objective here and requires a fairly unskilled

individual to accomplish. Malicious physical attacks generally create a type of denial of service (DoS), and multiple DoS attacks create a distributed DoS (DDoS) attack. When implemented in this manner, the attack may cause incorrect data or false sensing and state readings, and ultimately force equipment to malfunction.

Transformers are normally located on substation property and also in the customer domain where they are easily recognizable and reachable. These are large and relatively stationary devices that are normally difficult to relocate and constructed outside of the United States. Also, many smart grid components have a high monetary value which makes them easy and valuable attack targets. Attacks on physical infrastructure in the public domain can have significant effect on the smart grid as a whole. Black-outs and surge related outcomes are frequently the result of damaged equipment, and can result from physical compromise of current managing or directing components of the grid.

3.6. Cyber Attacks

Specifications for cyber security in the smart grid generally are not that legacy techniques are not sufficient in this environment [33]. Compared with IT network, smart grid networks and their devices have more complex objectives and assumptions on what needs to be protected [65]. Taking this into account, it is important to use current cyber security techniques only where they are sufficient, while discovering and implementing new methods elsewhere.

3.6.1. Attacks on Access Control

Access control has been thoroughly researched in environments composed of many systems and networks [66-68]. In any network, access control manages all user's access to information. Access should be controlled for much more than just stored data, devices and networking environments should be included. The stored data may include calculating costs, predictions of

future load, and special case monitoring. Each of these datasets must be sent to specific users while restricting access from un-authenticated users. In a smart grid setting, there are several types of users which require access to grid data. These roles include operators, engineers, technicians, and managers [69]. The policy implemented in the systems must manage multiple domain and network architectures. The interconnection of domains and grids presents difficulties in current access control policies. The policies in question should exemplify good management attributes as explained in [51], including well protected credentials and policies. Neglect in the form of hard-coded credentials is a vulnerability which has been abused often in the past.

Some of the mainstream methods used to protect this information fall under the category of attribute-based encryption (ABE) [70] or role-based access control (RBAC). These schemes can have their user revocation abilities bypassed if one gains the ability to masquerade or tamper with a legitimate user's attributes or communication stream. These schemes have been found insufficient as they generally do not satisfy the requirements of secure authentication across multiple domains and the real-time necessity for communication in a smart grid [71]. Several vulnerabilities have been discovered in typical IT networks which allow for exploiting access control in some capacity, including broken authentication, broken access controls, and information leakage [69,72]. These types of lapses are normally errors in policy implemented in a network. These schemes normally implement key distribution centers (KDC) in their architectures [73]. In the instance that the scheme utilizes a single KDC, this also presents a single point of failure. An attacker has the opportunity to carry out a DoS attack and stop legitimate users from accessing important data stored and accessed on the grid.

[72] introduces HMAC combined with challenge-response method which follows the RBAC scheme. This is another situation which is susceptible to multiple vulnerabilities in the grid. An

information and credential stealing session can provide a hacker with the data to masquerade and gain access to secret of sensitive data. In many instances, proper encryption is not in place in networks vulnerable to man-in-the-middle attacks. Several vulnerabilities have been discovered in equipment from specific vendors which allow for access to backdoors in SCADA systems. These backdoors have included valid credentials being hardcoded into an operational system's software which allows for trivial means of access by a hacker [74, 75].

3.6.2. Attacks on Cryptography

According to [76, 77], the cryptography flavor of choice for the smart grid is that of a public key infrastructure (PKI). This means that each of these networks have well-known vulnerabilities. This method creates a vulnerability in which a single point of failure exists between a key distribution agent or certificate authority (CA) when utilizing a certificate-based system. A successful DoS attack would render all or most encrypted communication invalid or foreign as the receiver would not have the ability to verify the sender's identity. In addition to a single point of failure, vulnerability exists in a hacker's ability to acquire the root key in a PKI which would allow for unfettered malicious communication [78] as modern masquerading techniques are advanced and sufficient [79, 80]. The network administrator is responsible for creating policy which will require a new root key in a sufficient time cycle and have adequate detection systems to mitigate or alert monitoring installations of intrusions or key stealing.

Lack of compatibility with newer standards in legacy equipment is also an issue. Smart grid networks such as SCADA networks interface with many devices new and old. When an un-hardened legacy device is reachable via outside network, it presents liability not only to itself, but to the entire network behind it. In a smart grid system, where the real time nature is critical, all traffic with sensitive data should be encrypted. This creates opportunity for traffic to be analyzed

in order to infer or confirm attributes of a system. With the use of high level encryption techniques, it becomes infeasible to retrieve the actual sensitive data from the raw data packets, but it is possible to intercept timing and frequency information of the messages in order to deduce information from the network which the malicious individual would like to attack. Then the analyzed metadata contained in the message information belonging to the sender can be used to exploit specific inferred vulnerabilities [64].

3.6.3. Attacks on Firmware/Software Policy

A method used with many devices hosting modern software is automatic online updating. This process is utilized to upgrade device firmware or software to the latest version. While this functionality is crucial in AMI and devices in other sub-networks, its implementation may ultimately be the source of malicious acts. Some devices in the smart grid may have a prescheduled window of opportunity for upgrade which the device is hard-coded to adhere to [81]. This can allow a hacker the opportunity to load a malicious version of firmware or software onto the devices and allow for more exploits from the inside.

Field devices with remote firmware/software capabilities may also allow for unrestricted operations during update [82]. In the instance of insufficient authentication measures in the update process, an attacker uploading malicious software to a device may be able to modify functionality of the device or upload malicious software at a later date. In addition to malicious software/firmware uploading, meter cloning and meter migration are also threats [62]. Meter software can be stolen and uploaded into other hardware which would replace an actual meter and be manipulated however the hacker pleases. Malicious data or processes may also be injected into the software before it is installed on the meters in the manufacturing phase. Also, meters may be swapped with neighbouring units which previously have recorded lower energy usage than the

meter designated for the property designated to use the meter being replaced. This will cause an incorrect reading and pass this false data to other smart grid mechanisms.

3.6.4. Attacks on Network Design

Network architectures that implemented in smart grid have generally been modelled after the mesh topology [20, 83,84]. This type of networking system works in tandem with the existing physical power grid to create a cyber-physical infrastructure. The end-users, such as residential and businesses consumers will have their power usage and pricing data communicated to local area utilities which collect and process data from smart meters and PMUs, pass that data on to aggregation points, and finally deliver the data to a substation or back-end network. The design of the network must support the key smart grid services explained earlier whose benefits are targeted for both utilities and customers.

DoS attacks are of great concern here. In the case of natural disaster or malicious physical attack in area which there is lacking redundancy and fault detection. These DoS attacks can be of a distributed nature in which Internet Protocol (IP) addresses are spoofed, flood the victim network, or be a single attacker that attacks a specific service or grid component. This may result in blackouts or rolling brownouts and network overloads [85]. The mesh network topology allows for redundancy and reduces repair costs as the grid is to be resilient in failure and the recovery for most situations should be automated. The designs must support distributed generation and bi-directional energy flow which are both integral attributes of the smart grid.

3.6.5. Software Input Validation

Vulnerabilities in software input validation are identified as those dealing with the underlying software-related architectural concepts of the systems interconnected on the smart grid network. These types of vulnerabilities are not always caused by implementation design flaws, but many

times by a protocol or standard which does not recognize security as a principal design concern. These vulnerabilities created through lack of security consideration in the past have also been a product of web application operation with automated functionality providing remote or internal access into the smart grid network. These types of attacks include buffer overflows and java/web interface exploits [13]. A buffer overflow occurs when a program writing to a buffer in memory and writes more data than the size of the buffer and completes its writing in adjacent memory. In an environment in which this is allowed policy does not require for all input to be checked, such as customer data, grid component data, etc. An attacker can create false data and send this data to the substations as if it were a valid and authenticated entity. With a specially crafted message that takes advantage of a lack of standardization for instance, is larger than the typical message size and writes pass the buffer end on the receiving machine. At this point the attacker can execute arbitrary commands.

In a smart grid system input will require resources constantly. This input must be handled properly to avoid catastrophic consequences. Invalid operations or arbitrary execution of malicious code can be devastating. Even improper handling of valid and safe input or code can cause unexpected results. Many of these vulnerabilities including most Structured Query Language (SQL) injection and a significant number of cross-site scripting vulnerabilities can be prevented with sufficient input validation [86]. The objective of most of these attacks is to create malformed or specially crafted messages to a specific node or server which contains the targeted vulnerability. From this point, the attacker can make use of a buffer overflow or an unprotected operation which can help in escalating privileges of their own malicious processes. Assumptions that the data received will be of a correct message format, while instead, received malicious messages are

malformed or exploit a known vulnerability which may trigger exceptions and arbitrary code execution.

An SQL injections is a type of attack that is fairly easy to avoid in most environments, but it is a vulnerability that is exceedingly more common in utilities which choose to utilize web-based interfaces. They are still prevalent in today's computing society due to the many avenues of usefulness of the attack which system administrators leave unsecured, and the type of data stored on targeted servers. These attacks normally exploit web applications or service interfaces by inputting specially crafted SQL queries into available forms belonging to these websites. Vulnerabilities such as incorrectly filtered data or inadequate typing can cause these maliciously crafted statements to be executed [87, 88].

Cross-site scripting (XSS) and cross-site request forgery (XSRF) are also a vulnerability inhabited by many web applications. These vulnerabilities allow the attacker to inject their own malicious scripts into a web site and simply wait for the victim system to navigate to the malicious webpage. JavaScript has been the most prevalent of the scripting used, but it also extends to ActiveX, HTML, Java, VBScript, and Flash scripting [89, 90]. Vulnerable systems normally do not sanitize the results of the HTTP query parameters and process or execute the commands in their malicious state. Also, the permissions granted the sites that the malicious scripts are downloaded from grant these scripts the same elevated rights.

XSRF allows for arbitrary requests to be sent on the victim's behalf. These requests can be maliciously executed by scripting or simply web browsing [91]. These scripts or actions like XSS are granted the permissions of the site from which they are accessed or downloaded from. A simple example would be for a user to browse the web while he/she has a valid online energy services session open. Upon browsing to a specific website which has a XSRF vulnerability and a malicious

image posted which references the action of withdrawing money from the victim's banking website. Therefore, these attacks use cookies or authentication which was previously established to forward requests to the unsuspecting victim. In some instances, devices interconnected in smart grid networks employ legacy operating systems that are no longer receiving support which introduces vulnerabilities unique to that software. Also, cloud/utility computing introduced into the grid creates vulnerabilities which must be of concern.

False data injections [38] are used to input manipulated measurements of specific state variables from demand-side or supply-side devices on the smart grid network. Attacks such as these provide state estimation systems with data which will create abnormalities in a power system and may result in the compromise of supervisory or power controlling devices on the grid. Also, these types of load altering attacks modify actual load at specific locations in order to disturb the balance between supply and demand or to allow the customer to relieve himself of a portion of his power bill. This is achieved by maliciously modifying one of the following: energy that demand-nodes demand, energy that supply nodes can supply, and states of the energy links. Manipulation of data sources in communication with systems in the grid, especially SCADA systems, can cause them to change state in accordance with the data relayed. In an environment where automation is prevalent and necessary, automatic operation based on data input is generally the standard.

3.6.6. Other Attacks

Masquerading or piggybacking open connections such as Wi-Fi in these networks is an example of an attack which exploits availability called network barge-in [90]. In the HAN or NAN, specific devices communicate with each other to relay energy usage information. A malicious attacker can gain access to the network and piggyback on the connection which is established between a smart appliance and a smart meter or aggregation point. With input of malicious or

misleading data, the smart appliance may falsify data or be taken over completely, not only risking secure authentication data of the user, but giving the attacker a valid entry point into the grid networks. A man-in-the-middle attack is also an option for an attacker in this environment. With access to a HAN or NAN in the smart grid, the attacker can intercept communications and relay with or without modifying its contents. A list of possible attacks to mechanisms that may be vulnerable is listed below in Table 3.3.

3.7. Countermeasures

Countermeasures are imperative in today's integrated infrastructure where IP is commonly used to simplify integration of the many parts of the grid and makes communication more standardized. Also, new security mechanisms, such as PMUs should be implemented here. Also there are several phases of securing advanced cyber-physical infrastructures. [107] presents three key services that need to be in place to have a secure smart grid system: prevention, detection, and response.

Prevention in a secured infrastructure should be composed of access control authentication in order to prevent unauthorized access. Detection should serve the purpose of flagging specified actions or signatures and monitoring the system as a whole. Response should include signature forensics, decision analysis, and contingency procedures [107].

Table 3.3: Attacks of Vulnerabilities in a Smart Grid

Attack Type	**Description**	**Devices Affected**	**Defense**
Buffer Overflow [13]	An operation which writes data and overwrites adjacent memory.	Devices employing software vulnerable to write exploitation (Networked Devices)*	Bound checking, safe coding procedures, ASLR

Race Cond [81]	Programming flaw in which the result of the output is dependent on sequence of events.	Devices employing software with improper input validation and Quality of Service (QoS)*	Increase integrity checks, strategic checkpoints
SQL Injection[81,92]	Submitting malicious SQL statements in a web form to a SQL database.	Databases	Query sanitization (based on DB)
Cross-site Scripting [90, 93]	Injection of client-side script into web pages exploiting web browsers or web applications.	Servers using scripting languages	Disallowing untrusted data in HTML pages, Sanitization,
Cross-site Request Forgery [89, 91]	A session hijacking technique in which a hacker masquerades as a trusted user.	Servers using scripting languages	Cookie Security, Authenticate per request, "NoScript" declaration
OS Injection	Executing commands via a web interface on a remote server.	Devices employing software vulnerable to injection	Proper coding practices
DoS [94-98]	Utilizing machine resources or making resources unavailable for other users	Devices Providing resources: SCADA, EMS, AMI, PLC	QoS, Distributed Servers, ACLs
Phishing [99-100]	Using methods to masquerade as a trusted party to gain information from a user.	Devices operated by users	Web Browser Extensions, Training Programs
Malicious Rem Media [2]	Devices containing malicious software	Devices operated by users	Employee Training Programs
Backdoor Admin Cred[64]	Unauthorized user using admin credentials to gain access to hardware.	Mainly SCADA	Vendor selection, Access controls

Attack Type	Description	Devices Affected	Defense
Fuzzing [102]	Inputting data to a remote networked entity which is monitored for undefined results.	Networked devices serving as servers: HMI	Address Randomization, Stack protection, buffer length checking
Crypto Key Flash Extraction [10, 85, 104]	Accessing device hardware directly with specific tools to extract data	AMI	Physical Protection, Data Encryption
Flash Image Manipulation [10, 103, 104]	Modifying software images before installment	AMI	Physical Protection, Data Encryption
Meter Bypass [10, 103, 104]	Masquerading or hijacking a communication session stream	AMI	Physical Protection, Data Encryption, Authentication
Meter Measurement Modification [10, 103, 104]	Modifying AMI to report incorrect measurements	AMI	Physical Protection
Extract RAM [10, 103, 104]	Accessing the device hardware directly with specific tools to extract RAM.	AMI	Physical Protection, Data Encryption
Extract Firmware [81]	Accessing the device hardware directly with specific tools to extract firmware in memory.	AMI	Physical Protection, Data Encryption, Update Signing
Watering Hole [105]	Injecting malicious code into a web page which a target victim is likely to visit	Devices operated by users	Web Browser Extensions, Training Programs
False Data Injection [38, 106]	Manipulating power systems states or readings by injecting false load data via AMI/sensors	SCADA, PMU, Transformers, AMI, EMS	Temporal/Spatial-based anomaly detection, Sensor Protection
Spoofing [79]	Adding an end system to the grid network and falsely using a legitimate identity	AMI	Integrity Checking, Physical deterrent,

Attack Type	Description	Devices Affected	Defense
Worms/Malware	Executing malicious or self-propagating software on the grid network	Potentially all devices*	IDS, IPS, AV

Physical security should include several measures which include considerations in these areas [108]: electronic access control, response to emergency situations, video surveillance and monitoring, geographical location, and tamper detection and reporting. Access control in a smart grid environment serves the same purpose of strict and specific authorization as in any other cyber network or physical premises. Access control in this setting should build upon currently available technologies and also define relationships between entities and authorized domains in a manner which they can be identified across multiple domains, while assuring real-time access [69].

Well-rehearsed policy should be in place in order to avoid incidents from escalating from small to detrimental. Employee training and sensing devices can assure this. Monitoring and logging equipment should be implemented in any secure infrastructure, with routine evaluation and response actions. In addition to these, more sophisticated and likely expensive measure can be taken, such as burying distribution equipment underground, enhancing security technology to create a more robust physical infrastructure, or a physical location which is less vulnerable to attack or incident. Hiring personnel to guard the premises of critical infrastructure is instrumental in fortifying physical defense. Tamper proofing field devices and implementing protocols such as invalidating keys when evidence of tampering on is detected should also be implemented on these smart grid systems [109].

[94-96] detail DoS and DDoS attacks. DoS security mechanisms include preventive methods which will allow a victim to endure the attack or remove the attack vector altogether. This can involve a type of QoS identification or a access control which only lets specific users access to

necessary resources [38, 94]. The difficulty of finding a solution to DDoS attacks is that a most effective method is distributed. This means that there must be a coordinated response in place which will be deployed from many different points on the internet [85]. The first and least likely of solutions would be to make arbitrary systems secure from outward attack. This would reduce the ability of an attacker to create a botnet [110], and effectively remove the distributed attack surface of the malicious individual. Another method of prevention is to avoid protocol functions that are expensive for server entities and cheap for the client which are frequently used for DoS attacks [85]. This can be handled by assuring that resources are committed to a client only after proper authentication [111], utilization of proxy servers with sufficient resources [112], protocol scrubbing (to remove protocol uncertainties which can be misused for attacks) [112], and methods to detect spoofing downstream which utilized outside sources such as ISPs of governmental services.

An approach in which resources are served from a distributed architecture may also mitigate DoS attacks [113]. This allows service to be re-routed in the case of failure at a specific location on a network instead of incurring a loss of connectivity. [112] proposes a solution based on data fusion. Where local detection techniques are employed and data is relayed to aggregation points where it is analyzed and action is designated. The number of nodes involved in the data fusion is determined by the detection sensitivity of an attack or a more traditional method of detection which incorporates all nodes on the network in the data fusion and analysis procedure.

Sufficient network resiliency provided by protocols, standards, and architecture may improve mitigation of such DoS attacks. The various network topology possibilities available all have their shortcomings, and there is no universal solution which removes all threats. Geography and utility preference and capability play a large role in the selection of a service topology. For AMI

specifications, a meshed network topology, which is the topology of choice for the smart grid, provides quality resilience, and several other requirements [114]. [115] proposes several requirements which help ensure resiliency in smart grids: AMI functionality, flexibility in DR, management of grid incidents, and asset security.

The advent of remote metering allows for the utilities or other control entities to read and control electricity delivery and usage at the consumer endpoint. This allows for automatic route modification in case of line disruption to allow for continued delivery in the case of an emergency in a specific location, and even isolation of portions of the network in the instant of malicious intrusion. DR allows for generation to better match the consumption. In better regulating the generation as closely to demand as possible, excess generation and underproduction can be avoided. This will reduce brownouts and blackouts.

The expected resiliency, when considering its real-time operation, of grid operations can be described as having a certain threshold relative to the latency requirements of the data, and operational requirements of the devices. Therefore, specific measures must be taken to deliver data expected above a lower bound that would disrupt the operation of the grid due to insufficient or incorrect data. These control mechanisms help ensure this attribute.

Race conditions in the smart grid may be deterred by utilizing one or more of several methods. These include multiple checks which distinguish the validity and integrity of the data, while moving the checkpoints closer to the source of origination. Also, immutable binding will provide for exclusive use of resources [20]. There is the possibility of race conditions outside of specific smart grid operational data. Examples of this can be seen in race conditions found in widely used universal protocols such as Dynamic Host Configuration Protocol (DHCP). Many race conditions may occur on the software side which is a result of poor programming. Any implementation of

protocol or procedure on any network hosted on the smart grid should be secured in such a way that resolves these race conditions appropriately. This may require removing or securing common protocols, or ample testing for software which may contain these types of errors.

SQL injections have been used maliciously in web applications to extract data in an unauthorized manner. Attackers can take advantage of attacking through many potential vulnerabilities (user input, cookies, server variables, etc. [88]), with possibility of revealing or compromising a network in several ways. This type of attack becomes easier as utilities become more reliant on web interfaces to provide consumers with services. These services and interfaces which the utility may host or utilize through an external cloud can create more vulnerabilities. Mitigation techniques include appropriately stripping away characters or strings used in SQL queries that can be used maliciously. This would be a process specific to the DB, allowing only strings relevant to the search [87]. [88] presents several other mitigation techniques: black box testing, penetration testing, and monitoring based on known patterns (including static code checking), methods for type correctness checking (including query development paradigms), replacing unregulated query binding to a type-checked API (including IDS and instruction set randomizing), and replaces normal SQL keywords with a randomized set.

Static code checking is very valuable in that the form of SQL queries is known, and limiting queries to a specific standard is essential. For example, strictly limiting a query to a single command, while checking the type of command and the authorization level of the user, can help prevent ambiguous requests. Query development paradigms and instruction set randomizing require the programmer to develop a subset of commands in which the DB engine will qualify as valid. These commands should be limited to the set of valid commands relative to the user's privilege level and remove the ability of unauthorized users to modify records or access data

outside of their authorization. An IDS implementation can be used to detect SQL injection via an anomaly-based or signature-based method [116]. An ideal location for this IDS would be in front of the DB in the network in question and would specifically evaluate SQL statements being forwarded to the server. A signature for an IDS in this context can be as simple as a specific query or a sequence of SQL keywords, while an anomaly is anything that creates or is equivalent to abnormal system function [116].

Cross-site scripting can be mitigated in the design of a web page by disallowing untrusted data in specific elements of an HTML document and escaping vulnerable and untrusted texts before allowing them in the body of the document [87, 93]. An HTML policy engine should be used to validate or clean user created HTML in an outbound way [93]. Valid cookie security is imperative as well as script disabling. While these mitigation techniques are executed on the web page side, Cross-site request forgery can be mitigated from the user side by carefully implementing a privacy/security plan which includes avoiding malicious links and cached data presented at login pages. According to [89, 91], the main method of mitigating this attack is to constrain input and encode output. Some areas of concern that can help prevent or eliminate request forgeries are listed below: cookie session life, user specific authentication in order to submit a form, and mechanism to verify request headers on web page redirects.

[89] details the synchronizer token pattern usage which should be implemented in the sensitive operation request process of the user. This process is a mechanism which requires the user to input a token into the HTML form in order for that specific step in the process to be valid. This process is initiated at several different stages in the operation completion process [89]. This token requirement process may utilize any client identification attributes including a type of Personal Identification Number (PIN) and is normally referred to as a challenge token.

A privacy/security plan which trains workstation users on the smart grid network, or corporate networks connected to it to identify phishing attempts helps mitigate multiple types of these attacks, along with browser extensions which disallow phishing efforts [102].

File fuzzing is normally conducted to search for buffer overflow, DoS, SQL injection, Format String bugs etc. This simple method of inputting large amounts of possibly random data into a system or network can greatly benefit programmers and administrators in finding errors that may be overlooked. Stack protection and buffer length checking are also novel tools [102].

Bad data is detected and identified after the estimation process by the analyzing measurement residuals. False injection attacks can be detected through either spatial or temporal-based methods. Unobservable attacks cannot be expected to always originate from physical locations in close proximity. Therefore, methods should be designed to detect large unobservable attacks which occur and modify loads in a much faster or abnormal rate [88]. Also, protective measures should be taken in order to secure the sensing mechanisms to mitigate these attacks [38, 106].

In protecting against false data, is important to consider preventative and reactive approaches. Firstly, pricing and command signals should be protected using authorized encryption techniques. A sufficient public or private key encryption algorithm together with an authentication mechanism should protect integrity and confidentiality. Also, protection of AMI devices such as the smart meter is integral. Once a malicious individual gains access to a single smart meter, they have the platform to legitimately introduce false values into the grid.

Unobservable coordinated injection attacks can be detected by placing PMUs in strategic positions along a specific bus which will calculate voltage and phase details along that bus [88]. This PMU measurement data can be submitted over the NaspiNet which implements more techniques for secure transmission of data than standard networks, therefore less subject to attacks

[96]. Analyzing PMU data as a security technique uses an anomaly-based algorithm which learns the normal load of a specific portion of the network and alerts the correct authority upon deviation. This also alerts command of the exact perpetrator whose load is compromised. Traffic analysis takes advantage of the availability of data and infers specific details which will allow the attacker to generalize and develop attacks which may exploit vulnerabilities which are assumed from analyzing this data. NIST announced in 2001 FIPS 197 which is the Advanced Encryption Standard (AES). [56] suggests this standard for use in the smart grid for encryption. Triple DES has also been approved, but unlike AES, the computational strength and method of encryption are estimated to only be secure until around 2030. NIST, along with FERC, also recommends the IEC family of protocols for establishing smart grid interoperability [56, 117]. Several of these protocols are listed below in Table 3.4. Meter security is one of the foremost areas of security research in the smart grid [6, 21-23,46,56]. Software/firmware attacks require reliable authentication methods to ensure secure data transfer.

Table 3.4: IEC Standards Recommended for the Smart Grid [64]

IEC 61970 & **IEC 61968**: present a Common Information Model (CIM) for data exchanges between devices and networks, while **IEC 61970** is for transmission and **IEC 61968** is for distribution
IEC 61850: provides help for substation automation, communication, and interoperability using a often-used data format.
IEC 60870-6: provides help for information exchanges between control centers.
IEC 62351: is for the cyber security of the communication protocols in the above IEC standards.

Secure boot loaders and cryptographic validation is integral when upgrading software [109]. Security in these devices is more or less a tricky matter as resources are limited in these fairly mobile devices. This means that conventional IDS implementations and computation heavy encryption algorithms should not be utilized on these devices. Physical security measures or

tamper-proofing should be enabled on a per device basis to remove the ability of an attacker to physically access the meters memory which may contain consumption data or encryption keys. Serial ports and optical ports must be secured physically and required to have authenticated measures.

To truly evaluate the integrity of a system, evaluating entities must be aware of the recentness of measurements and be able to analyze their results while understanding the context in which they were extracted. In a system of systems as diverse and widely interconnected as a smart grid, measurements and characteristics must be analyzed at a very large scale for various software and devices [113, 70].

3.8. Publicized Attacks

The most infamous of the malware which targets industrial operating or control equipment is Stuxnet [102]. This worm's attack vector includes the Windows operating system which was employed on Seimens industrial equipment and software. Several variants of Stuxnet targeted five Iranian organizations [118]. Seimens SCADA systems and PLCs were targeted in these organizations with speculation that the US and Israel played a part in the engineering and distribution of the worm [118, 119].

Very recently, Telvent's network and accessed project files of a control systems used in the electrical grid were breached by hackers. Attackers installed malicious software in order to access the files via a system which was interconnected with a utility's corporate network. This system was as an intermediary between legacy devices used on either side of the device [120].

Another type of event which deserves consideration is acts of nature. In recent events, Hurricane Irene blacked out over 4 million customers in the eastern US. Also, in June, 2011, 5 million

customer in six states lost power for up to a week. Also, in the summer of 2012, hurricane Sandy caused more than 70 billion dollars in damage [121].

In 2008, Tom Donahue, of the CIA, with no knowledge of the perpetrators, explained that there were several distributed attacks on power equipment in several regions outside of the U.S. These attacks were followed by extortion demands and caused disruptions in services [120].

On a lighter note, On Dec. 29, 2008, an individual hacked into the Ozarks Electric Cooperative Corporation's reporting and outage management system in order to upload a custom voice message stating [121], "All of Ozarks Electric's employees have gone home. Call someone who cares."

2003 hosted the Slammer worm. This malware made its way into a private computer network at Ohio's Davis-Besse nuclear power plant in January and removed monitoring equipment for an estimated five hours [122].

In 2005, the National Nuclear Security Administration computers were hacked in order to steal sensitive information on over 1500 contractors and employees, and went unreported upon initial observation of observation [123].

In Baxley Georgia in 2008, a cyber-threat caused a 48 hour emergency shutdown due to a malware injection attack. An unsigned firmware update was attempted and an attacker uploaded a malicious version of firmware which modified data and caused safety systems to be triggered [124]. Several reports of “watering hole” sites which attempt to infect traffic visiting the site which will allow for an attack from inside the network.

Vendor MacAfee reported that a series of relatively unsophisticated attacks, such as SQL injection, over a term of likely four years by Chinese hacker which stole intellectual property from U.S. energy companies [125]. Several companies were attacked through public facing web sites via cyber methods mixed in with social engineering. Once compromising web servers in the

Netherlands for attacks several other countries, malicious software with remote administration tools was uploaded to browse areas such as Active Directory. This operation was labeled Night Dragon [125].

Duqu, discovered in 2011 is a worm with a likeness to Stuxnet, while serving a completely different purpose. This worm recorded keystrokes on remote systems which allowed the hackers to create attacks based on information inferred from the data gathered [125].

3.9. Conclusion

Since the natures of the systems in a smart grid environment are complex and critical to the current state of technology and human well-being, they require quality and sufficient security mechanisms and solutions. This must equate to a holistic approach where all threats and vulnerabilities are considered, including future hazards. In the coming years, standards should be enforced in a manner which will alleviate the responsibility of choosing from the numerous security options on the market that the utilities and device manufacturers. The bulk of the current attacks on the smart grid infrastructure are composed of DoS, traffic analysis, AMI vandalism, and higher level application attacks. Exploits of vulnerabilities found in the grid infrastructure have been detailed along with an overview of current countermeasures, which will afford us some insight into securing the grid.

Securing the smart grid will require utilities and all other participating parties to take both short-term and long-term views. Also, utilities and vendors should begin preparing for a much more standards-based future. These industry standards and protocols should address the necessity for a requirements-based level of consistent and interoperable performance. Finally, a near-future look into smart grid progress will likely yield more functionality in processing and beneficial action on the data accumulated by smart grid AMI and sensing processes.

This domain is the most vulnerable to attack due to customer defined specifications and unregulated operations. HANs are normally more easily compromised due to the lack of cybersecurity knowledge of most customers and the interfaces with other devices and networks in the grid. While most devices in this domain should have security mechanisms in place, there are often not enough to mitigate many attacks from prototypical hackers, as vendors have to weigh financial responsibilities against a standards-based evaluation of their product.

CHAPTER 4

MALICIOUS DEVICE INSPECTION IN THE SMART GRID HOME AREA NETWORK

4.1. Introduction

Inaccuracy in estimation and malicious devices are two of the problems that continue to plague many smart grid installations. Even throughout the networks in the home, it is well-known that these networks generally contain devices with legacy software which can be actively targeted as entry points into a network. After a successful exploit, some malicious individual or application can freely take advantage of vulnerabilities on any of the devices resident on the network, including devices which interface other smart grid networks. These entities can take advantage of AMI which allows for automated measurement and communication of the metering data from the consumer to the utility. With the implementation of AMI, there must be some form of trust between two entities. In addition to trust, data being communicated should be truthful and correct. This can be provided upon adding sufficient accountability into networks which reside on the smart grid or connect to it, and more importantly from a consumer perspective, the HAN.

Since metering and accountability data are generated on the consumer side, a more fine-grained process must be implemented to assure accountability as well as a technique to efficiently discover the devices in the HAN which are behaving in a manner which is outside of their expected and correct requirements. Little work in accountability of devices in the smart grid HAN has been done. The HAN normally interfaces other critical networks in the grid and is most influenced by the consumer who normally has little knowledge in hardening hardware and software in a manner that is sufficient for grid purposes. Therefore, research and requirements in this area should be one of much interest in the smart grid landscape. Within this deficiency resides the lack of a mechanism

for inspecting devices in the HAN at a fine-grained level, which will further establish accountability in this domain.

The objective of this chapter is to introduce an accountable method which inspects the status of the devices connected to the HAN in order to find which, if any, are performing actions that are undesired or malicious in the network. A minimal inspection cost while maximizing efficiency is of extreme importance. Our contributions here are two-fold:

- *HAN Device Grouping* creates witness-target relationships between devices in the HAN in such a manner that they can effectively monitor and report required activities.
- The *Inspection Algorithm* is used to effectively pinpoint malicious or malfunctioning devices. This portion of the method utilizes the group structure created in the grouping stage to efficiently manage the device inspection.

In addition to these contributions, we present analysis of the device inspection method and the grouping algorithm.

The rest of the chapter is organized as follows. Section 4.2 provides some background in smart grid and accountability, Section 4.3 will give an appropriate problem definition, while Section 4.4 begins the discussion of the HAN inspection method. Section 4.5 details the HAN grouping process for the method, and Section 4.6 provides evaluations and analysis of the method through simulations. Section 4.7 concludes this chapter.

4.2. Background

The importance of the security of data which originates to and from the HAN must take precedence in the organization of security and accountability. Making these devices secure and accountable to their actions will reveal many potential problems in the grid and allow these malicious actions to be isolated and resolved. Related estimation tools such as disaggregation and

load monitoring [26,42,43] are useful in certain situations where there are few or no devices with unknown attributes, but normally estimate usage based on the aggregate amount from the residence as a whole and the normal consumption of a device cannot always be determined sufficiently well enough for the smart grid. This type of estimation is more useful when identifying behavioral patterns instead of a more fine-grained approach and discovering malicious and malfunctioning devices.

Security has been one of the key areas of research in the smart grid landscape. Accountability can be viewed as a complement to the core principals of information security and the component that allows authorized individuals robust tracking and auditing history as well as establishing trust and confidence within the HAN among devices. Current accountability in the smart grid does not extend far beyond a single consumer (household, business, etc.) reporting energy usage to the utility. This is not a sufficient method for smart grid operation as the lack of accountability in the HAN allows for false reporting and data creation from inside the HAN before or during the process in which consumers send data to the utility.

There are several requirements which can contribute to an effective accountable environment or mechanism. These include [28]: decentralization of accountability mechanisms, scalability, minimal impact, data collection, and identity management. Inclusion of these elements in the accountable scheme can be very useful and will help to cover the accountability requirements.

Currently for smart grid applications, the main objective of accountability is to maintain record of device power usage and assure that a device behaves as it says and/or is expected to. In other words, a device should truthfully report its power usage and other parameters required at a pre-specified time intervals and/or when requested. This support is not implanted as is evident by [46], which demonstrates that AMI and other HAN devices data can be attacked and falsified from

multiple angles. Even in the case of data reporting, there is still much room for error and we cannot always expect for the record that the utility manages and what is recorded at the customer's end to be identical. Malicious actions, malfunction, miscalculation in estimation, or calibration may be the cause of such differences. Making the HAN accountable on a more fine-grained level can help alleviate problems such as these and provide us with a means of pinpointing compromised devices which can immediately be disabled or serviced instead of canceling service to the residence until the problem is determined.

The application of accountability has been established in a few works in the neighborhood area network (NAN) in [22,23]. These works provide several linear and tree-based inspection algorithms to address the malicious meter inspection problem (MMI). [21] provides an accountable protocol for use in the HAN, as well as a protocol for the neighborhood area network NAN. The HAN protocol bases its accountability on providing evidences which can discover questionable monetary charges or lack thereof on the utility bill based on some threshold and detailed logging comparison procedures. Some issues with [21] include the lack of a fine-grained view of accountability. This may suffer from the same type of vulnerability that distributed false data injection attacks create as falsely reported events will not always be detected as long as the thresholds are not exceeded. When carried out over a long period of time, the customer suffers a significant amount of loss and the malicious actions may remain undetected.

In this chapter we will assume that the model HAN is composed of many devices. For power calculation purposes, disaggregation techniques have been well studied. This is insufficient for entities inside of the HAN as observation and troubleshooting at a more fine-grained level is necessary, as well as location of devices affected by malware and physical abnormalities.

4.2.1. HAN in the Smart Grid

The smart grid HAN can be described as a grid subsystem which is dedicated to demand-side management through energy efficiency and quality demand-response implementation. It can be further described as a dedicated network of devices which will inevitably become “smart”. These devices range from load and control to typical household appliances, built with some form of software applications which allow the consumer to control these devices at a detailed level. With the application of smart grid concepts, the home area will be transformed into intelligent nodes in the grid network where some amount of the energy that it uses is produced locally by generators (likely photovoltaic generation) and renewable energy.

The works in [132, 133] give several categories of technology that are normally found in smart homes. Intelligent management devices are the first type of devices found here. These devices include the control and monitoring capabilities which are locally required. They manage and utilize the data created inside of the HAN as well as external data generated from the utility of other intelligent nodes connected to the grid networks that work in tandem with the HAN. A simple example of how this data can be used is precise and efficient management of energy usage and discovering local producers and consumers. Management controls not only higher level functions, but may also control and manage individual devices. Scheduling and peak usage avoidance are keys in maintaining an optimum demand and supply relationship.

Other technologies include remote control capable and measurement devices [132, 133] and devices which interface the HAN with the utility and other domains. These have commonly been added to the HAN in the form of mobile devices which add capability and allow real-time information exchange and connect to their respective utilities.

Although there are many purposes for devices inside and outwardly connected to the HAN, many which reside therein simply desire to consume energy and do not provide any type of control or management capabilities are also play an integral role. These devices normally communicate through internet-based technologies using Zigbee, WiFi, HomePlug, etc [133]. The majority of devices in current homes will need to be completely redesigned with several features included in order to take advantage of the envisioned behaviors and capabilities in the smart grid. Many devices currently given the "smart" moniker are not able to deliver many of the communication requirements necessary to fulfill the vision of the smart grid. Therefore, we name smart devices ones which have the capabilities to modify their operation to positively achieve certain goals, while connected devices do not, although they may monitor and report details about the operation and environment.

4.3. Problem Definition

The following sections detail a discussion of the proposed accountable method for inspection of devices in the smart grid HAN and the elements of security elements it will address.

4.3.1. Problem Details

There are many components that go into assuring accountability in a network such as the smart grid HAN. With implicit knowledge of the environment, the status of a network or devices can be proved with a few other details such as an audit trail to observe prior actions. Currently the smart grid landscape requires little accountability, and even less in the HAN and distribution domain. This means that locating malfunctioning or malicious devices in the HAN can be very difficult, and all but impossible for entities outside of the network to verify. The dispensation of data from one node of a smart grid network to another, which is generally unregulated, is a major vulnerability, but the legal repercussions of monitors encroaching on civil liberties and privacy of

a consumer are also of concern [134]. The enforcement of privacy laws keeps the utility from performing accountable observation inside of a HAN connected to the smart grid, therefore, this accountable evaluation must be completed from within the network.

Given the dynamic nature of devices in these types of networks, the solution must be scheduled to run at a specific time interval which it will be most effective, or triggered by some action and inherently granted visibility to the devices residing on the network. In many instances, protocols have been proposed which resolve issues in the smart grid HAN while making many assumptions about the composition of the network and actions therein. The uncertainty of the actions within the HAN may be contained by some thresholds when estimations are made, but normally no requirements are made for fine-grained observances or activity.

4.3.2. Threat Model

To define a threat model, we can detail the some properties for a quality accountable inspection service:

- *Completeness*: Holistic visibility of each device on the network by those entities required to review/monitor such actions. Also, complete visibility for the inspection process.
- *Authenticity and non-repudiation*: Devices which report activity be authenticated by the device which cannot deny its participation in the report.
- *Freshness*: Due to the dynamic nature of devices in the HAN, maintaining a most recent record of the devices located therein is of the utmost importance.

Therefore, false reporting of status is not the only worry that must be addressed. A faulty device could violate any of the above properties in an attempt to maliciously affect the network inspection process, or these actions could be taken by devices which are malfunctioning due to hardware or software error. An example of such an action could be a device accepting status reports from a non-authentic source, or reporting false entities resident on the network. While the proposed method not only prevents errant reports, it also prevents false accusations.

4.3.3. Assumptions

In the proposed accountable environment, we define the HAN model to include a home or a single building composed of *n* devices and a single smart meter. We will assume that each device has a set of witnesses (W_n). The objective of the inspection is to efficiently search the active devices which are connected to the network in order to find malicious or malfunctioning devices. In the initial model, the smart meter resident in the HAN will be responsible for accountability management and maintaining a record of devices and their witnesses. As the presence of network devices will likely change constantly due to mobile devices moving in and out of the network. Smart devices can effortlessly broadcast their presence on a network and the management device can simply observe the network for traffic from new hosts.

Another goal of the proposed method is to be easily implemented over any device that is considered to be smart. Therefore, use on the principal communications protocol for the foreseeable future is easily possible. Evaluation parameters are based upon the number and ratio of total devices that must be utilized in the inspection process. This number is directly responsible for the efficiency of the inspection method. The process overhead will also give us a baseline for the efficiency of the method.

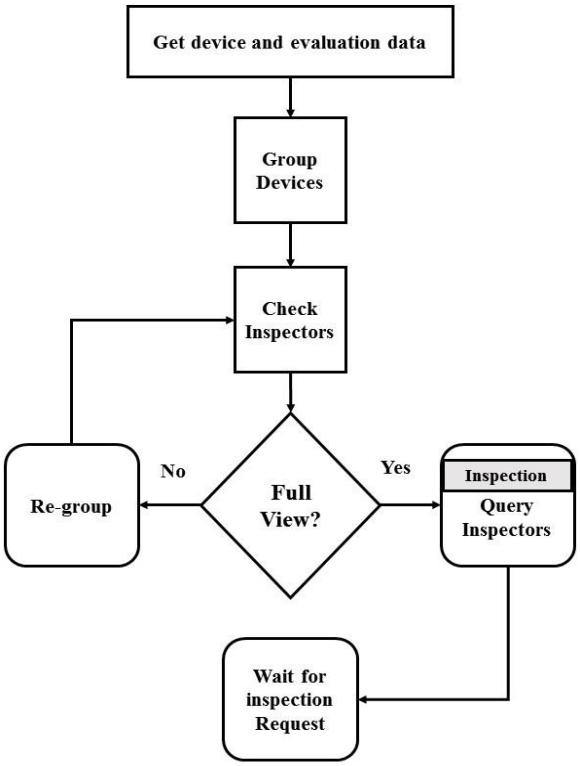

Figure 4.1: HAN Inspection Process

4.4. HAN Inspection Method

The aim of the inspection algorithm is to locate malicious or malfunctioning devices, and in doing so, increase the accountability of networked actions. Many actions that a device can take may not be explicitly labeled as malicious, and therefore, we define a malicious action as one which is not allowed by the scanning procedure that the witness uses. Scanning procedure can range from passive network overhearing to an intrusive virus scan. All of which will work under the proposed accountability method's structure. Any such act that causes adverse effect on the network can create a situation in which the offending device will be categorized as faulty or malicious. In instances that a device may innocently malfunction or falsify data, there may be allowances for these types of devices to be labeled as suspect and inspected further. Once these actions are discovered, there must be a method to, without a doubt, deduce which device

participated in the wrongdoing, isolate it, and resolve the issues. The overall process flow of the method can be viewed in Figure 4.1. The method begins by acquiring the identity of

Input: (I) Inspecting Devices
Output: (*Q)* The set of possibly malicious nodes
Initial: $Q = \{\}$
1. **procedure**: Detect(*I*)
2. if (*I* is empty)
3. return Q;
4. // retrieve the witness data *D* from the set of witnesses;
5. **while** (faulty or suspected dev(s) are reported)
6. **for each** (dev ∈ $D.s_0 \cap D.s_1 \cap D.s_2 \cap \ldots D.s_n \cap$)
7. **if** (dev != "clean")
8. I := I – {dev}
Q := Q ∪ {dev}
9. **if** (all devs in *D* == "clean")
return *Q*;
else go to step 5;
10. **end for**
11. **end procedure**

Figure 4.2: HAN Device Inspection

each of the devices on the network. The method of evaluation is also necessary for the inspections process. From here, all devices in the network are grouped and the witness-target relationships are formed. Each of the grouping process steps will be detailed thoroughly in section 4.5. The inspection will then take place.

In the proposed method, the set of inspecting devices is partially defined by the number of devices resident in the HAN and the variable witness requirement of the accountable scheme. We can define the set of malicious devices as *Q* and the set of inspecting devices as *I*. I is the set of devices which will participate in the selective scanning routine which the eventual final status verdict for each device in the network is derived from. The inspector devices are taken from the set of witnesses *W*. While $I \in W$, the inverse is not true, as only a small subset of *W* is needed to have the necessary witnesses for each of the devices in the complete set of devices *D* in the home. Once *I* is established, it must only be changed when a device in the set leaves the network for

efficiency considerations. The inspection algorithm is given in Figure 4.2.

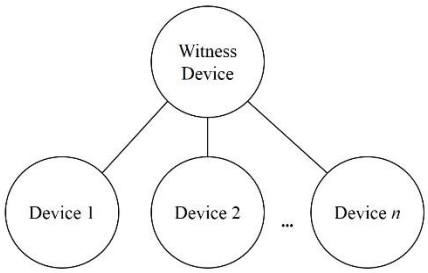

Figure 4.3: Witness-Target Structure

Figure 4.3 shows the view from a single witness device down. In this manner, the root node will only have to request status indications from the single witness device shown to find any possibilities of ill-reported or malicious data from any of the witness device's targets.

This approach is basically a selective scanning procedure similar to the D-scanning method in [23] for utilizing the multiple witness scheme. In other words, we take advantage of the fact that each device has several witnesses, the inspector set can be reduced to a significantly small percentage of the complete set of devices in the home *D*, in order to have a complete view of each device on the network.

Inspection frequency will be established based on the policy of the network and each instance of inspection will be completed in a single sweep based on the report from each of the inspectors. Since the devices in *I* are already contained in a device's witness set, there is no need to further monitor the inspectors. This means that the completion of the inspection will require the inspecting devices to only scan the devices in *I* to gain a full view of the entire network. Errors or suspect reports propagate up the chain and will reach each respective device in *I* which is witnessing the faulty/suspect device in question. In a tree-based scheme with many levels, there is an inherent trust requirement in the devices which are at the lower levels. With the use of a common one-by-one scanning method where there is only a single witness of a device, either device may be malicious and that data may not be propagated as it should due to the malicious device which the

data travels through or is produced by. In the proposed scheme, there will always be multiple devices witnessing a single target, and the witness devices in turn will always be witnessed by multiple devices. The nature of the smart grid HAN is such that devices may turn malicious and/or faulty at any time. Therefore, to address this, there is accountability on many levels which is necessary in such environments.

4.4.1. Static Inspection

We consider static inspection to be some inspection where many of the devices in in the home remain active on the network for a longer period of time. Although the internal makeup of the network may remain the same, it is untrue that the status of the devices will be static. We can also assume that over a long period of time, it is infeasible to expect for the network to remain unchanged with no devices being added or leaving the network, but this behavior will be expected to take place for longer periods of time than in a typical HAN for this type of inspection.

There are two options which would be suitable for this type of situation. Both the proposed method and a complete scan of each of the devices on the network are a possibility. A complete scan is maximally inefficient in the first of the two extreme cases where only a single device in n is faulty or malicious, although the inverse would represent the opposite of this trend. Therefore, as the number of faulty devices increases the more efficient static inspection by sequential scan may become. In an instance which we utilize this type of method, each device would be inspected individually by some dedicated inspection device. This is equivalent to a brute force scan. The authors in [23] proposes a similar scan by implementing a tree structure whose depth is determined by the number of nodes which represents the meters in the NAN. The inspector has access to each of its subtrees and has the ability to investigate the device details from its level down.

Due to the dynamic nature of the smart grid HAN a static inspection technique is not ideal. Though mobile devices are especially prevalent in these networks, many high usage devices permanently reside in the home. Lighting, space heating and cooling, water heating, ventilation and refrigeration normally represent about 70% of the usage in the HAN [135,136], so these devices can be expected to remain present. While taking these devices into account, the average home has about 25-35 electronic devices residing in it regularly, therefore, efficiency will normally suffer with a complete static inspection of every device.

4.4.2. Static Approach

The proposed method behaves optimally under the conditions of a predominantly static network. Although we can add some stipulations for increased efficiency. Considering the current conventional makeup of the smart grid home, there are certain devices that are common found therein. Devices such as washer/dryer, oven, heating ventilation and cooling (HVAC), etc. generally can be expected to be permanent fixtures and constantly capable of communication on the network. Devices with this property will be given priority to become witnesses of other devices in the network. Even if the network becomes more dynamic, the device grouping method will not need to be completely reinitiated as a large portion of the witness devices will already have been established and in the worst case will simply need to have a few of the parameters changed.

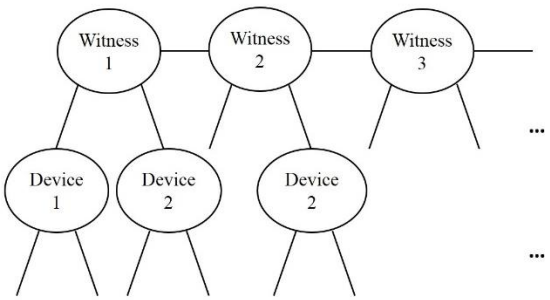

Figure 4.4: Static Witnesses

Figure 4.4 represents the static set of witnesses on the network. With a static set of witnesses on the network some of the cost of the grouping method will be reduced as well as the communication overhead as a result. This is due to the static devices constantly being part of the inspector set, therefore, no re-configuration of the witness-target relationships are required. Also, priority in witness request response is given to the static devices, and therefore, less overhead is accumulated.

4.4.3. Devices with Irregular Smart Operation

In the discussion of accountability and inspection, devices whose actions do not fit the predefined expectations of the prototypical HAN's decision mechanisms must be included appropriately. In many instances, legacy devices are and will be utilized in smart homes. These types of devices normally cannot communicate as expected to participate in the witnessing portion of the accountable method in the HAN. This problem is solved in the fact that the proposed scheme does not need each device to act as a witness. Devices considered as witnesses, of course, will be devices which meet several requirements, one having the ability to communicate and log their own actions and the actions of their targets in the network. With precision, the legacy devices and all other devices will maintain the minimum required number of witnesses which will log their actions and verify that they are within their expectations. Moving forward into the expected smart home environment where there are a typical number of smart devices, the use of legacy devices that are completely incapable of participating in network communications will generally be minimal, and the impact on the accountable scheme will be nonexistent or negligible.

Another class of devices in the HAN that has irregular activity and is responsible for much inconsistency in reporting is the class of devices with varying consumption. These devices normally have several operating modes or levels which consume different amounts of energy. These modes are triggered by specific events which are expected to occur during the day. Some of

the devices included in this group are air conditioners, washing machines, water heaters, and refrigerators. Each of these devices must be dealt with appropriately. We propose a method which enforces accountability in such devices in [137]. This is done by utilizing the multiple witnessing scheme similar to that of the algorithm proposed in this work. Therefore, the accountability of varying consumption (VC) devices is increased. The work in [137] uses general usage grades for specific types of devices to better estimate and validate their energy usage, making the consumption calculation in the HAN more fine-grained, and in doing so, more accountable. Once this is done, the task of inspection will also become more correct, yielding less fewer positives.

4.4.4. Logging and Auditing

Auditing is an important addition to any accountable environment. First we list the actions in need of logging.

- Network entry and departure
- Device grouping communications/actions
- Inspection participation/actions
- Status changes

Challenges can also force a device to cryptographically provide some proof of its identity and actions during communication. The challenges also help to protect against attacks on freshness. The environment for logging actions pertaining to any of some device's (Device 1) behavior is demonstrated in Figure 4.5.

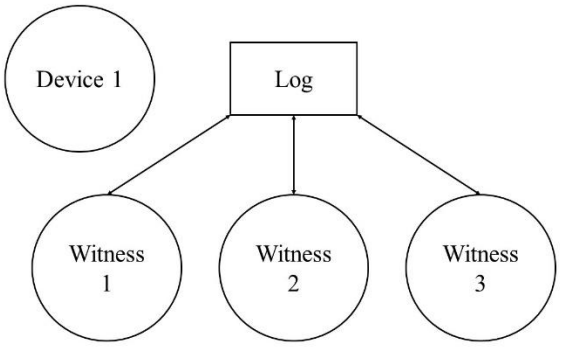

Figure 4.5: Logging Environment [138]

The witnesses of a device have the ability to audit and challenge the target device as often as necessary in order to produce valid and correct results. This is carried out by accessing the environment log. A witness is entitled to go as far as auditing a recent sequence of actions to ensure the target device's validity.

The idea for the overall framework is similar to [130]. While auditing and logging are very important in the assurance of accountability, the resources of the devices must be taken into account as to not overwhelm their computational and memory limitations. The network administrator may select a specific degree of auditing and logging which is efficient in assuring accountability in a sufficient manner while maintaining the responsibilities of the included devices and network operation.

4.4.5. Limitations

The issue of accountable storage has yet to be completely addressed. Some faulty or malicious storage device can be placed on a network with a considerable amount of energy stored. Even if the entry is authenticated, the device may communicate some incorrect amount of local storage, and with this, confuse devices of the origin of their energy and disrupt overall energy usage readings. Also, if the majority of the networked devices are incapable of network communications

in such a manner that there are insufficient devices capable of being an inspector, the method cannot function properly.

4.5. HAN Device Grouping

The second step of the inspection solution as viewed in Figure 4.1 is to find a way to establish relationship between the devices in the HAN. The works in [23,140,141] present similar problems in which they implement some type of grouping in order to solve their issues. The authors in [23] presents a binary tree structure with a single root node for inspection of smart meters based on proximity, while [141] divides a large population into groups based on efficiency and cost effectiveness for inspection. In [141] the key differences are the existence of groups and the variability of the status of the observed sample at any given time. The proposed method allows for a variable number of witness devices and readily takes into account the fact that any device's status in the house may change to malicious or fail at any time. The target selection process is also unique.

4.5.1. Device Grouping

Each of the devices in the network will have a special "witness" attribute which keeps track of the details of each of its targets, as well as the number of devices witnessing itself. Each device will need to have a minimum number of witnesses in order to satisfy the accountability requirements of the network. This is accomplished by each device querying the network for witnesses in the case that it does not meet the network required amount. The smart meter manages the record of the device relationship bindings and each device can access this information as Figure 4.6 displays.

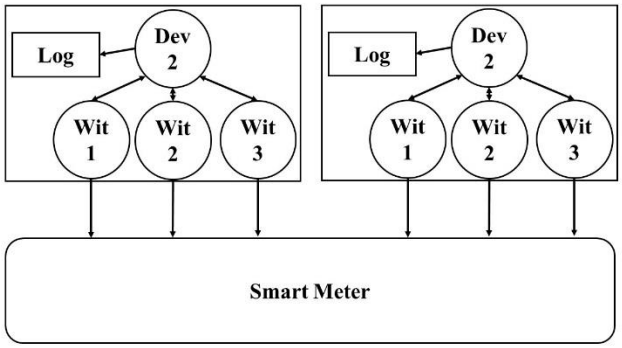

Figure 4.6: Accessing Relationships Bindings

The devices communicate with each other in order to find eligible witnesses, while the smart meter manages final decisions.

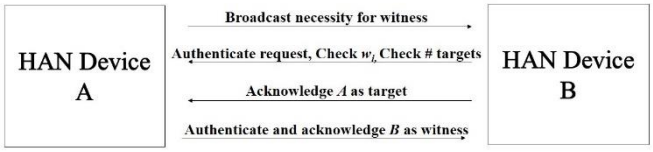

Figure 4.7: Request for Witness

Figure 4.7 shows that device *A* requests device *B* as witness. The request for a witness must first be authenticated and then the fielding device must verify that the requestor has not already reached the number of required witnesses in the network by reviewing the smart meter managed record. If this number of witnesses has been met, the fielding device will explore other options in the network before agreeing to witness device *A*. This is done by reference to the smart meter's record in order to maintain efficiency of device monitoring in the network by keeping the number of witness devices in the network at the minimum. This will also create a basis for a more efficient scanning procedure. For an organized grouped witness-target network representation, we review Figure 4.8.

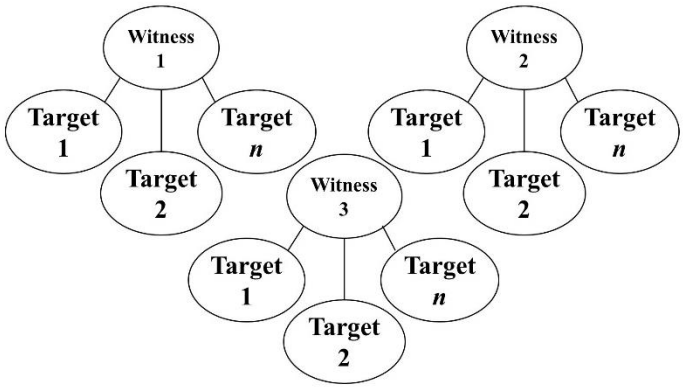

Figure 4.8: Witness-Target Network

From a management perspective this is the suitable view, as all inquiry about the status of the targets only need to be directed to the set of witnesses which have the responsibility of maintaining a status judgment of their target. A more comprehensive view of the network is represented in Figure 4.9.

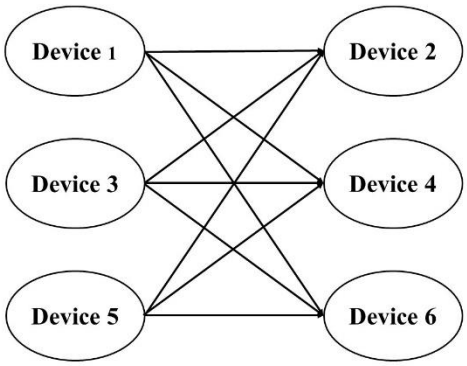

Figure 4.9: Detailed Network Relationships

This representation shows the devices 1, 3, and 5, targets (devices 2, 4, and 6) for simplicity, the connectors for all of the device's targets are not shown. These relationships stay in place until some device is unresponsive, or properly leaves the network. The device relationship can in certain instances be completely random. In theory, it is best to introduce a delay in the responsiveness of the devices that presently have targets once a new request for a witness is presented to the network.

Doing this will allow for the witnessing responsibilities to be assumed by a smaller number of devices as the devices with witnesses will respond to new requests first. The benefit here is that the number of devices with witness responsibilities will be smaller.

The detailed algorithm for the selection process is given in Figure 4.10.

Input: A device dev_i and its targets (targets(dev_i));
Begin at dev_0 (smart meter)
1. **procedure**: groupDevs(dev_i; targets(dev_i); $\forall_{devj} \in$ targets(dev_j))
2. (β, newWitness) = receive(); // Read target/witness data
3. Establish witness connection
4. **while** (newWitness != NULL) do //pool on witness request
5. **if** (!witnessMax(newWitness)) then
6. newWitness = getNewWitness(targets(dev_i))).
7. **end if**
8. **end while**
9. **if** (!targetReq(newTarget)) then
10. newTarget= getNewTarget(targets(dev_i))).
11. **end if**
12. **end procedure**

Figure 4.10: Selection Algorithm

The selection algorithm accomplishes a very necessary task which is maintaining ideal and required target and witnesses for each device. Understanding that mobile devices will be constantly moving in and out of the network, as well as powering on and off, means that the witness and target attributes must be maintained and verified instead of simply established and ignored. Devices which do not meet these requirements cannot be fully trusted in their actions as witness devices.

The witness-based monitoring helps to mitigate false alarms by not simply accusing devices unilaterally, but instead incorporating multiple and unanimous accusations from the device's witnesses into the decision-making. Upon the detection of any protocol misconduct by one of the witnesses, the nature of the problem is noted, and subsequently, the SM will query all other witnesses of the behavior of the target device.

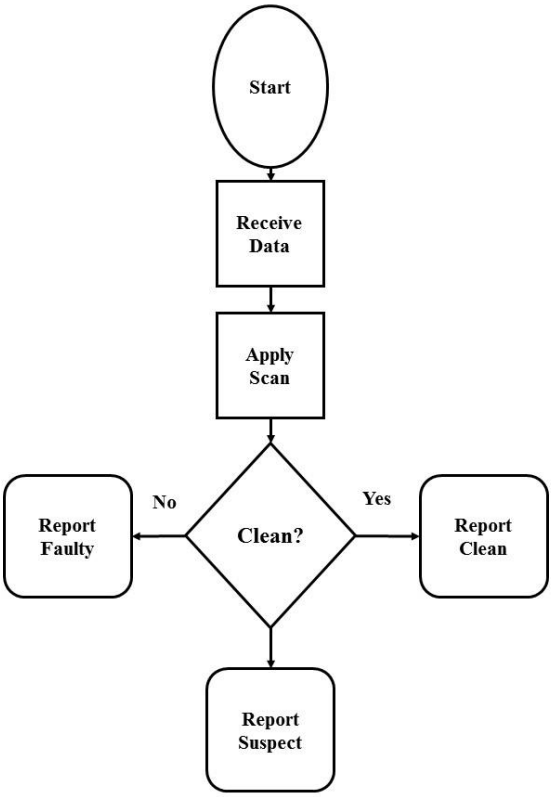

Figure 4.11: Witness Monitoring Process

If those witnesses observe malicious activity or outcomes of targets actions are above some tolerable threshold, they will report against the device. A consensus ruling will generate a label being assigned to the target device. The evaluation routine for witness monitoring is displayed in Figure 4.11.

4.5.2. Grouping Adaptability

In order to construct and maintain a network structure which will adhere to the method requirements of the witness-target structure and a valid inspector set with full view of the entire network, the grouping method must be run at least when any devices leaves or enters the network. The adaptability of the network is described as the ability of the network tom maintain or re-establish the complete state whenever any changes occur to the witness-target structure. Leaving the network can be denoted as powering off/unplugging a device or the device leaving the range

of the wireless signal provided by the access point. We can measure the adaptability of the network by the amount of effort it takes to re-establish a complete state after some device/s becomes inactive. A complete network has the immediate capability of a full inspection of each of the networked devices. The complete state must be observed for short period to assume that the network is in a complete condition. Generally incomplete network states are caused by two actions: (1) One or more members of the current inspector set become inactive. (2) The current number of targets per each device in the inspector set becomes inefficient.

In the instance that a device becomes inactive, the distribution of device monitoring must be reviewed and optimized if necessary. Three conditions may occur once a device becomes inactive. Either the device that exits is part of the inspector set and has the maximum number of device targets allowable based on the size of the network, the device monitors other devices and is not part of the inspector set, or the device is solely being monitored by its multiple its witnesses. The third would likely be the case for any legacy devices participating the network. With the second condition, some ample requirements would be in place in the network which may require some devices to maintain supplemental witnesses while not requiring these devices to be a part of the inspector set. The smart meter's record of device relationships must be queried in order to find the devices in need of additional witnesses based on network requirements. Once this is done, the task of adding witnesses to these devices is of the utmost importance. This can be accomplished by running the selection algorithm in such a way that only witnesses are requested for the device/s in need of replacements due to one or more devices leaving the network. Figure 4.12 demonstrates the regrouping of the inspector set. At all times the inspector set must maintain full view of the network. Therefore, whenever the network is not complete this process must be run. It is composed of checking the number of targets per device in the network as a whole.

```
Input: Inspector set I and all devices D;
Begin at dev0 (smart meter)
1.  procedure: findInspectors(inspector set I)
2.  (β, data) = receive(); // Read target/witness data
4.  while (targets!= NULL) do //pool on witness request
5.      if (targets(target not in I)) then
6.          Add device to I.
7.      end if
8.  end while
9.  if (sufficientTargets()) then
10.     groupDevs()
11. end if
12. end procedure
```

Figure 4.12: Inspector Set Regrouping

One way to expedite this process is to review the inspector set for the device/s that have changed or left, and assume that their set of targeted devices remains in the same state that it was before the most recent event of device/s leaving. After evaluating the targets the number of targets in the inspector set must allow for full view of the network. This can be achieved either by adding more targets to the current devices in the set or adding more devices that have the capacity to monitor additional devices and participate in the inspector reporting activities.

Figure 4.13a displays the relationship between devices in a network in which the devices have been assigned identifiers 0-19 based on the time the devices became active on the network. The devices are required to have 3 witnesses at all times. These devices have been assigned witnesses based on the same principal, meaning that in this situation the devices with lower identifiers basically have priority when gaining a witness as they were active in the network before their latter counterparts. Figure 4.13b displays the same network of devices with the first device (Dev 0) removed. We can gather from observation of the Figure 4.13b when reviewing the witnesses-target relationships of the devices the only acceptable inspector set which gains full view of the with three witnesses per devices in the network contains devices 0-15. As mentioned earlier, there are

three conditions which are caused by a device becoming inactive in the network. The first, being removal of a device contained in the inspector set is displayed in Figure 4.13. Here the inspector set must be evaluated and modified to satisfy the network inspection requirements. We see through observation, the new inspector set contains devices 1-15, with the recently inactive Dev 0 not eligible for inspector set consideration any longer. In the second case in which the inactive device monitors one or more devices but is not included in the inspector set, the only task to complete would be to find another witness for the device/s that this device was previously witnessing. The third, which includes a device which has no witnessing responsibility, and is solely being monitored would require for additional actions to take place aside from the removal targeting record to be removed from the inactive device's previous witness(es).

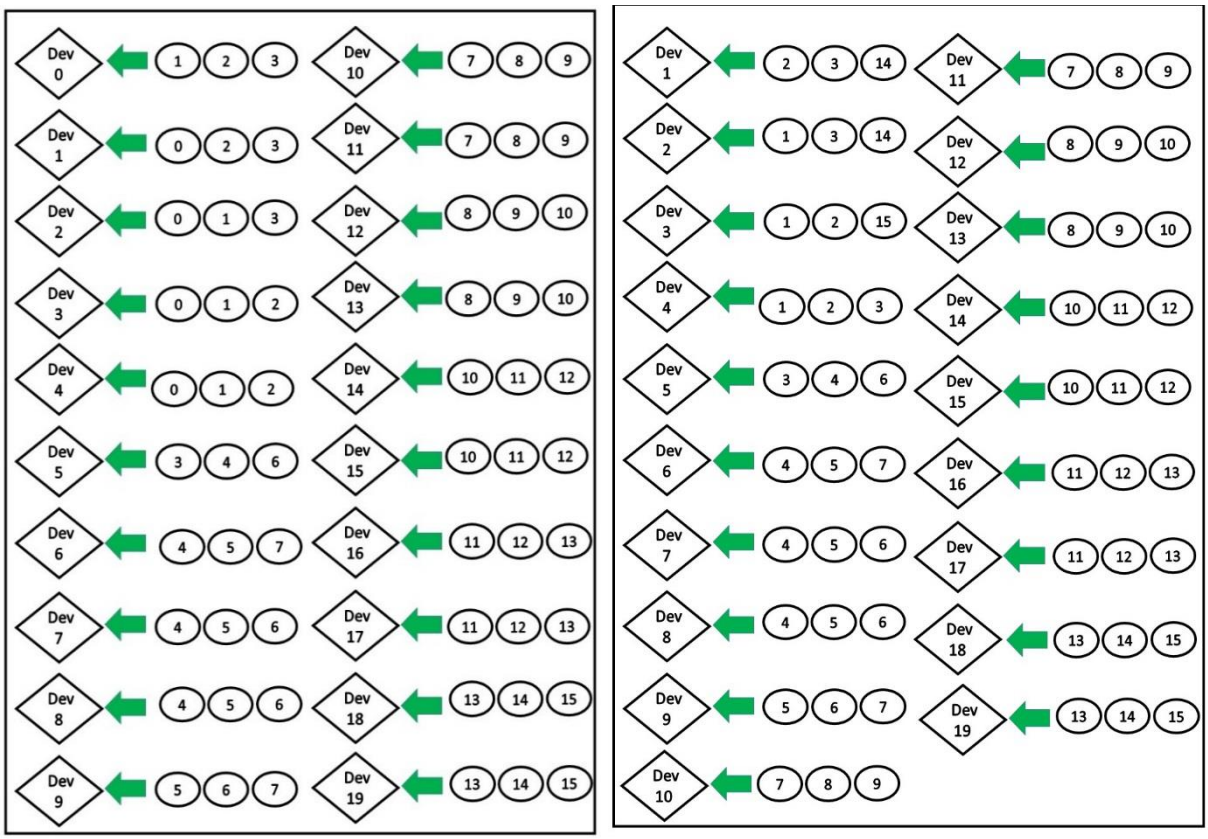

Figure 4.13: Device witness-target relationships (A), Device witness-target relationships with Dev 0 removed (B)

4.6. Inspection Method Evaluation

The number of overall appliances can be expected to be about three of four times more when accounting for the requirements of smart homes which are expected to host many more devices than current homes do [42]. In a smart grid where all devices communicate over a network, each of these devices should be expected to participate in accountability processes and report their actions as the network or scheme requires.

The evaluation of a method can be carried out with the discussions of several key components. [198]:

Effectiveness: this metric can most simply be measured by the accuracy of the detection of malicious or malfunctioning devices. This is then combined with the false alarm rate, in which the false alarm rate is composed of the false positives and false negatives. False positive, in this instance, signifies any event where a device report categorizes a device as malicious or malfunctioning while the device is actually operating properly. In the inverse, a false negative signifies an event where a report categorizes a device as clean while the implicated device is acting maliciously. Also, any lack of a report results in a false negative.

Resource consumption: Many of the devices utilized in a HAN of the smart grid are categorized as resource constrained. This means that in comparison to PC-class devices, these devices, in many cases, lack comparable computational and memory resources to process the load required by its normal operation and sophisticated software. In many cases, the fewer resources the software uses, the more resources can be allocated to monitoring or dedicated to other actions. While many devices are extremely resources constrained, this is not always the case. Therefore, it must be assumed that all devices operate with a minimal amount of resources in order for the method to perform adequately on a wide range of devices.

In evaluating the method, two approaches are generally accepted. The first uses measurements of the system, while the second is based on representations of system behavior via a model. Measurement techniques mostly are utilized when the environment or a prototype of the environment is available to create an actual realistic scenario. Then this technique can be applied to the system. Creating a real HAN testbed for some specific scenario can be very expensive and limited in terms of working scenarios without utilizing all necessary components. Also, measurements and results are generally non-repeatable. Taking this into consideration, device mobility patterns, scalability, and protocol usage, are all difficult to implement in a real testbed. Therefore, utilizing simulations or analytical models allows for an increased spectrum of working scenarios and variations of parameters.

The selection process is either selective or automatically inclusive of all of the devices in the HAN, in the case of the most trivial scanning technique, which is the complete scanning of the entire set of devices *D.* The algorithms proposed and described earlier are each simulated through software. The data is created based on a number of devices ranging from the common number of devices found in consumer homes and medium size businesses, to 200, which can be viewed as a theoretical home or business. Figure 4.14 shows the number of devices required for scanning in the proposed algorithm for a ranging number of devices as utilized in the simulations. The results in Figure 4.14 require three witnesses per connected device which will be input into the selection algorithm from Figure 4.10. We observe that the set of inspectors *I* is roughly half of the complete set of HAN devices. If we require only two witnesses, we do not observe much change in these numbers as shown in Figure 4.15.

This factor is more pronounced when the number of witnesses is increased. Also, the number of targets that a specific device is allowed to witness is a major factor.

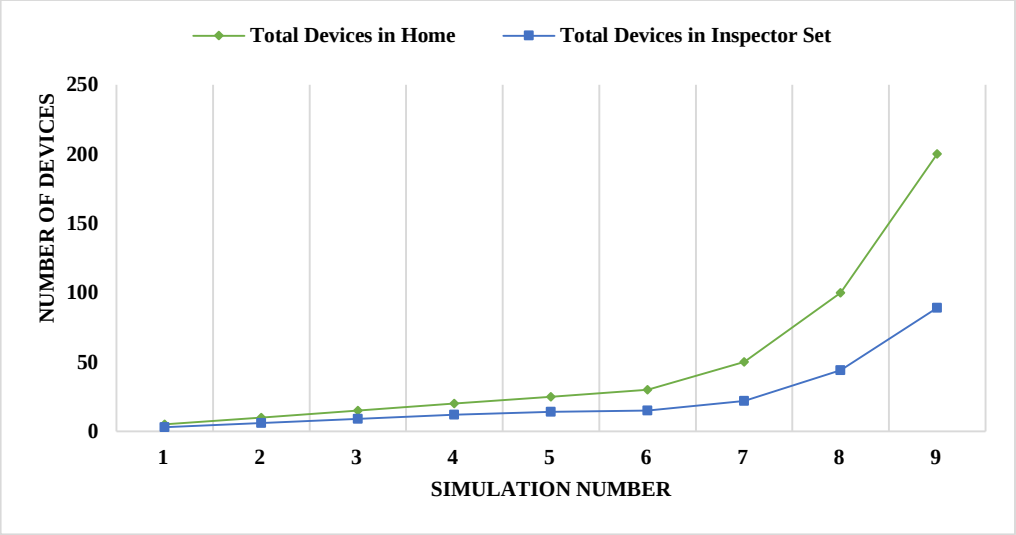

Figure 4.14: Inspector Efficiency with 3 Witnesses

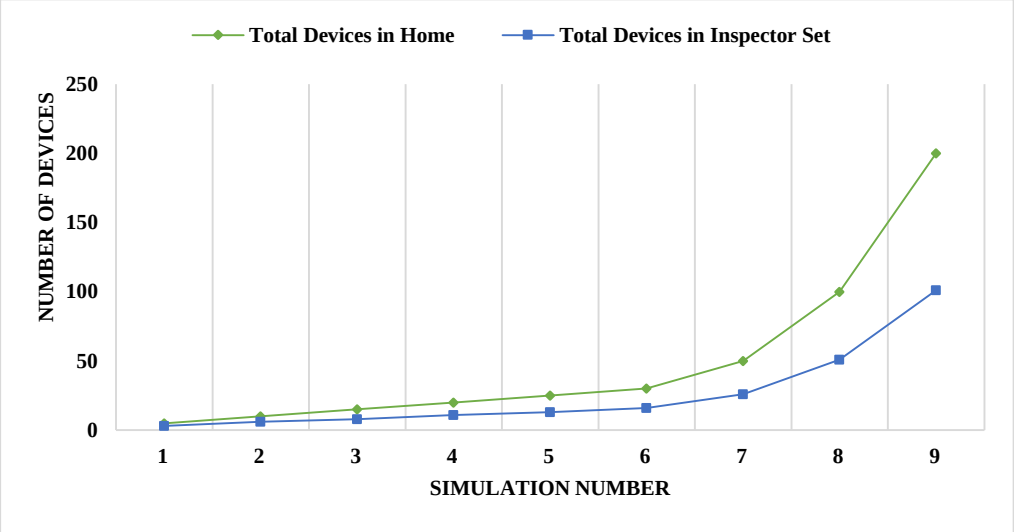

Figure 4.15: Inspector Efficiency with 2 Witnesses

We will limit this to 4 devices in order to maintain a lower level of computational and networking overhead as increasing the number of witnesses or targets creates more work for devices with witnessing responsibility. This method of scanning is obviously more efficient than a one-by-one method of scanning which must include all device in *D*, which includes all devices in the network.

The authors in [23] proposes a method for dynamic inspection of devices in the NAN. This method makes the assumption that the malicious devices, once discovered, will be removed from the tree-based structure which is being scanned and then proceeds with its scanning in a round-by-

round fashion and queries a global monitor to check results. The problem with tree-based approaches is that in an extreme case it will repetitively scan the same set of nodes. In a scanning approach, it is normally assumed that devices with children nodes continue to infect or report false data at the scan time. Another pitfall can be that the child nodes continuously report false data during scan time. The premise here is that the higher level nodes must be trusted inherently as the child nodes may not participate in the accountability of their parent nodes. This in essence makes networks such as this fully trusted from the view of child nodes looking up to the parents.

4.6.1. Grouping Analysis

The establishment of witnesses maintains the structural basis of the proposed method. Therefore, the number of witnesses is very important. Fixing *w* is a tradeoff problem, where increasing the number of witnesses reduces false positives and reduces the efficiency of the inspection process. While having a high number is important to be as accurate as possible in detection, the inverse of the positives are also true. A lower number of witnesses increase the efficiency as there will be fewer inquiries of targets required, but the possibility of false positives will normally increase.

The purpose of arranging the devices in trees with a depth of 2 and a variable number of leaf nodes is for inspection efficiency. One of the challenges of the grouping mechanism is reformulating the grouped structure while devices are constantly entering and departing from the network. In order to calculate cost for the proposed grouping method, we can view the amount of devices required to participate in the grouping as the minimal number of devices which will need to maintain witnesses. With this, the ratio of the number of devices required in the proposed method, by the number of devices required in a one-by-one scanning technique will yield the overall relative cost [141].

Table 4.1 and Table 4.2 show the significant efficiency improvements provided from the proposed method in contrast to the complete scanning technique. This is due to the manner in which the device are grouped and the fact that each devices does not need to be inspected individually in order to acquire full view of the devices of the network.

An important question for an implementation of this method lies in the number of witnesses that are optimal for the method to be most efficient. As observed in the grouping statistics in Table 4.1 and Table 4.2, there initially is a slight increase in the relative testing cost in situations the number of witnesses increases. This is due to the minimum witness requirement in the method stipulations. Therefore, there is a necessity for more inspectors to fulfill this requirement.

Table 4.1: Relative Costs for Grouping with 2 witnesses

Number of Devices	**Relative Testing Cost**	**Efficiency percentage gain**
5	60	40
10	60	40
15	60	40
20	60	40
25	56	44
30	50	50
50	44	56
100	44	56
200	45	55

Table 4.2: Relative Costs for Grouping with 3 witnesses

Number of Devices	**Relative Testing Cost**	**Efficiency percentage gain**
5	60	40
10	60	40
15	53	47
20	55	45
25	52	48
30	53	47
50	52	48
100	51	49
200	50	50

4.6.2. Communication Overhead

In this subsection we will explore the implications of choosing a policy for response to some devices entering the network and requesting witnesses, more specifically whether unicasting or broadcasting replies to messages is most beneficial. Report messages policy will also be discussed. Since any broadcast request can lead to significant and possibly an excessive amount of replies, some delay or suppression mechanism should be in place to assure that the network bandwidth and device network capabilities are not overwhelmed. The options of discussion are listed below:

1. *Unsuppressed Broadcast* – All nodes reply with no suppression.
2. *Delayed Broadcast* – Specific nodes have delays in order to grant priority of witness responsibility to a group.
3. *Dynamic Delayed Broadcast* – All nodes choose some random interval for delay, snoop the channel and reply based on the network traffic after the delay.
4. *Unicast* - Only a single device replies to and request, whether the request is uncast of broadcast.

Theoretically, the most efficient of the methods presented previously is the dynamic delayed broadcast algorithm when the interval is large [143]. The others are only optimal under certain conditions and provide for a tradeoff in terms of complexity and efficiency. Option 1 maintains the least efficient of the 4 methods in terms of network activity and computational load. Option 3 makes an effort to increase the efficiency by implementing some estimation function based on network or environment parameters. Beneficial parameters to use in the estimation function could be packet loss, network size, or device locality.

The broadcast response policy that would be most efficient for use with the proposed method is be the delayed dynamic option. With this option in place, the response policy will take into consideration the congestion and loss probability of the network and each device will calculate an

optimal random delay for use in responding to newly connected networked devices or the request for target reports.

The delayed broadcast is optimal for the static inspection method. Within this framework, the devices which are determined to not be "permanent", would receive the delays in response to the witness requests. Report messages will also be handled in the same manner under this framework. Upon smart meter request of a target report, at any time, the device will need to exhaust its delay before it responds to the request. This way, the devices which most likely have multiple witnesses will report their measurements first.

4.6.3. Re-Grouping Analysis

Measuring the effectiveness and efficiency of the regrouping algorithm can be done by observing the work which is done when one or more devices become inactive or leave in the network. This work is the result of regaining the completeness of the network in the form of modification of witness-target relationships. Since the primary motive of grouping is efficiency of inspection, it is most beneficial to evaluate the make-up of the inspector set. For the least complex case of a single device leaving the network, we examine three cases:

- The device that exits is part of the inspector set and has *t* targets
- The device monitors other devices and is not part of the inspector set
- The device is solely being monitored by its' witnesses.

In this evaluation we assign no work to the action of modifying the targeting attribute of a device. In the case of device departure, the first and third cases in which the device has no targets will require no work due to the lack of witnesses and having no need for witness replacement. The second case in which the device previously had witnesses and is not in the inspector set requires w_d work. The witnesses which that device was previously being monitored by must be replaced,

each of which requires one unit of work. The modification of the device's targets requires no work. On the other end of the spectrum resides the complete inspector set becoming inactive or the entire network shutting down. The latter brings about a unique problem in which there are no devices in need of monitoring, and therefore the work required is also zero. Table 4.3 displays the work required for regrouping with a varying number of witness requirement. In any instance in which there are no witnesses required or the number of witnesses equals the number of targets, the amount of work required will be zero. When the witnesses and target numbers are equal, all devices included in the network must be included in the inspector set to satisfy this requirement.

Table 4.3: Required Work for Varying Witnesses (with 4 targets)

Network Size	**No Witnesses**	**2 Witnesses**	**3 Witnesses**	**4 Witnesses**
20	0	18	12	0
40	0	38	27	0
50	0	48	30	0
100	0	98	72	0

As per Table 4.3, the amount of work done increases as the network has more devices. This type of increase is typical of any network which implements methods in which the devices participate in network activities. Also, when comparing the differences between the 2 witness and 3 witness data, it can be observed that as the number of devices increases the amount of work per device is lessened. This means that the ratio of efficiency per number of devices trends up as the number of devices increases especially when working with a higher witness requirement.

4.6.4. False Positives/Negatives

In this subsection we evaluate and analyze performance of the inspection method by finding the probability of false positives and negatives. The probability of a correct inspection can be determined by a set of three factors: the number of witnesses per device, and the probability of detection p_d and the detection accuracy p_a. The second parameter (p_d) can be described as the

probability that the intrusion detection system utilized has enough information to accurately detect and diagnose the malicious device's actions (positive or negative). To maintain simplicity, transmission and overhearing which is required for the witnessing process both experience equivalent interference from environment variables and are included in p_d. p_a represents the accuracy of the detection mechanism which is expressed as a ratio. Using the parameters above, we can model the probability of detecting a faulty device *d* as:

$$\boldsymbol{Pr_d = p_d * p_a} \qquad (4.1)$$

False positives can be defined as any report event in which a clean device on the network falsely submits a status report of some other device as *faulty* or *suspect* while the device is *clean*. On the other end of the spectrum, a **false negative** occurs when a clean device submits a status report of one of its target devices as *clean* while the device is either *faulty* or *suspect*.

Each of device *d's* witnesses gives a status indication for *d*. The management device which is likely the smart meter, never trusts any device on the network, therefore any device serving as *d's* witness will also be untrusted. The information regarding device *d*'s status is like all other information, untrusted at the time it is received.

False positive probability (FPP) and false negative probability (FNP) will be used as accuracy metrics. Table 4.4 represents the conditions necessary for false positive and false negative identification. FPP is the probability that status reporting of device *d* is not consistent with its actual status if it *d* is actually clean and is reported as faulty given that none of its witnesses are compromised.

To find the false negative probability, we first understand that there are three events that can cause a false negative:

- Device *d* has one or more compromised witnesses which report it as faulty

- Device *d* maintains consistent false data which is reported by witnesses
- Proper reporting of device *d* fails in route to smart meter

With no witnesses, we can observe the FNP as a single device providing consistent false data which misleads any witness device that makes a report. Since the proposed method will always utilize witnesses we can model the probability of the FNP as:

$$FNP_d = p_d(1 - p_a) \tag{4.2}$$

Table 4.4: False Alarm Decision Model

SM's evidence about *d*	**SM's decision**	***d*'s actual state**	
		Compromised	**Uncompromised**
All evidence is consistent	Uncompromised	False Negative	True Negative
	Compromised	True Positive	False Positive
All evidence is not consistent	Uncompromised	False Positive	True Negative
	Compromised	True Positive	False Positive
Evidence not complete	Suspect	Suspect	Suspect

Where both parameters used represent collaborative probability variables determined by the network and the detection mechanism. We can see that the probability of a single device providing a false report without consistent evidence against its target device without collaboration from another of the device's witnesses is very small. Thus, in the case that there is no collaboration, for simplicity $FNP_d = 0$. For simplicity, since $\boldsymbol{p_d}$ and $\boldsymbol{p_a}$ make up the majority of the FNP and FPP, we combine these two to find the false alarm rate which is composed of all false alarms FNP and FPP.

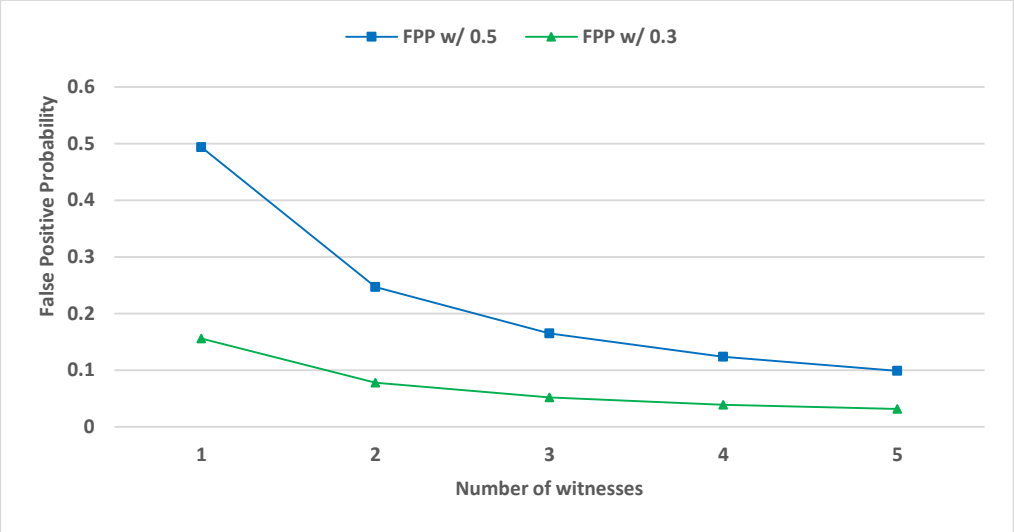

Figure 4.16: False Alarm Probability with 0.5 and 0.3 Accuracy

Figure 4.16 shows the trend of fewer false alarms as the number of witnesses grows which displays the value of utilizing a witness-based approach. Assuming that each of the witnesses is uncompromised, we understand that the packet loss is normally very low in the typical HAN. Also, only in the case of a high loss rate does the trend shown in Figure 4.16 not hold.

4.6.5. Inspection Analysis

We begin with the strategy of scanning all devices in the network, which is accomplished by receiving a status indication of all devices in the network D. If the number of malicious devices in the network is much less than the total number of devices, the efficiency will suffer due to unnecessary operations. The extreme cases being $D_s = 1$ and $D_n = n$, the complexity of such scanning is bounded by the number of devices in D although the set of malicious devices, Q, is unknown. Especially in environments such as the HAN where Q is likely to be constantly changing, there is little benefit to acquiring status indications of only a select few devices and not the entire set due to the possibility of devices becoming malicious during method run time. The proposed protocol solves this problem through the select scanning method of the inspector set I.

The inspector selection process is viewed as finding a Borel set of all singleton node sets of the nodes in set *D*. This produces a minimal set of nodes that contains all nodes in *D*. Each element in *D* will be represented by their target nodes data as opposed to their own data. We can define the generating of the Borel set by iterating through the *D* as equation 4.3 shows which performs all countable intersections and all countable unions possible with the subsets in *D*:

$$D \rightarrow D\delta\sigma \qquad (4.3)$$

It is now necessary to remove the subsets which are non-singletons. This is achieved in Equation 4.4:

$$D\delta\sigma \rightarrow I \; only \; if \; |D\delta\sigma| = 1 \qquad (4.4)$$

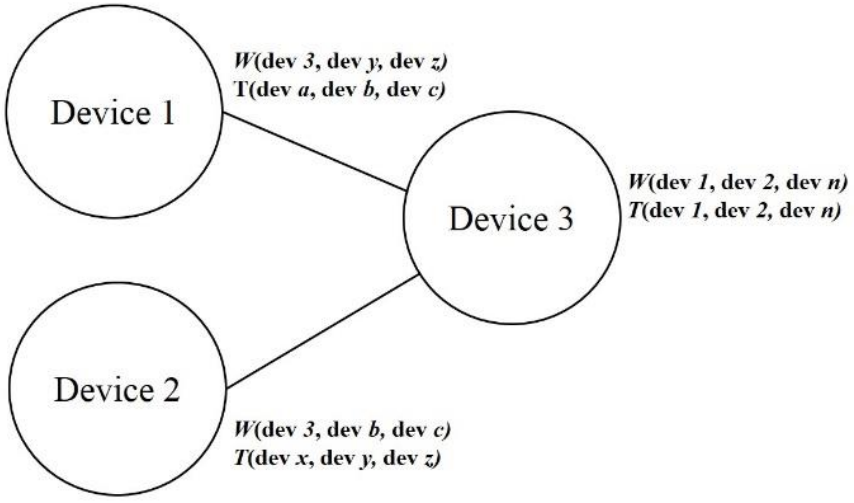

Figure 4.17: Node Witness-Target Data

This set of inspectors is essentially minimal while maintaining full view of the entire set *D* which allows a single sweep of *I* to determine the reported status of each device.

As the devices in *I* maintain the reported statuses of all devices in the network, the upper bound and lower bound of necessary scanning of the size of *I* remains the same while *D* does not change. Upon any change in *D*, devices affected in the network will make the necessary changes to their

witness-target relationships due to network requirements. This shows that performance remains the same in either of the extreme cases of malicious node existence where $n = 1$, or $n = n\text{-}1$.

An accountable environment has been researched and developed in [21-23] while making some assumptions such as activity patterns of varying consumption devices, generation, and storage devices. The authors in [21-23] adopt the multiple witness concept for the HAN, and the work in [23] adopts the inspection procedure in the NAN, while the HAN and the NAN are quite different networks. The HAN is mostly defined by the appliances/devices in each home, while the NAN is defined mainly by the AMI in a neighborhood or service area. In the proposed algorithms, we use the multiple witness concept and the inspection procedure in the HAN which are similar to those used in [21-23] though with key differences. The proposed witness selection eliminates the inherent trust requirements of higher level nodes that tree-based methods maintain, as the trust of witnessing nodes is necessary. Our method leaves no nodes without witnesses that will monitor their actions.

4.7. Conclusion

This chapter has proposed algorithms to efficiently provide accountability in the smart grid HAN through multiple witness-based monitoring and inspection of the devices therein. An inspector selection algorithm is proposed as well. The algorithms provided show their validity in environments of a dynamic nature, where complete device inclusion is required and there is always a possibility of changing malicious statuses. The analysis and simulations in the study show that the proposed algorithms are effective in creating an accountable environment in a smart grid HAN.

CHAPTER 5

HOME AREA NETWORK ACCOUNTABILITY WITH VARYING CONSUMPTION DEVICES

5.1. Introduction

A difficult problem in the HAN lies not only in the concept of estimating power usage, but establishing accountability in this domain. Accountable environments in smart grid have been researched in [21,22,47] while making some assumptions such as activity patterns of varying consumption devices, generation, and storage devices, which may or may not lead to sufficiently accurate estimations in the HAN.

This chapter will detail a method for more intricately estimating and monitoring usage of varying consumption devices in order to create a more fully accountable and accurate environment in the HAN. The "witness" concept is used to provide a solution to the assurance problem between normally trusting devices and the SM. Each device will be assigned $w > 2$ witnesses based on the network size and policy which will allow for multiple usage reports on a single device to ensure this device is accountable for its actions. Aside from the overall method, contributions include:

- the *proposed method, called VC (varying consumer) algorithm* which establishes the energy related category so that each specific device will belong to and continuously converge on a range most suitable for estimating energy usage;
- *usage state infrastructure* which provides a baseline for further establishment of energy categorizing and thresholding, and allows for more accurate recognition of a device's expected usage while in a certain "mode";

- and a *threshold selection* method which utilizes recurrence quantification analysis to identify and converge on common usage amounts within a usage state.

The rest of the chapter is organized as follows. Section 5.2 provides some background. Section 5.3 describes the problem statement. Section 5.4 details the proposed method. Section 5.5 presents the evaluation. Finally, the chapter is concluded in Section 5.6.

5.2. Background

The smart grid is an increasingly expanding network of networks and system of systems. It is integral to have simple knowledge of the grid to understand how the consumption of energy and its accurate estimation in the HAN plays a major role in every domain.

AMI plays a large role in the consumer domain with two-way communications from the consumers to the system operators [147]. From the data, the consumer can receive pricing information, and schedule/modify their power usage according to their preference, or some peak rate avoidance scheme.

Sensing and measurement are constantly occurring and reported in the smart grid. Once the data are analyzed, tendencies can be created and major and catastrophic events can be predicted and avoided based on past measurements. This type of wide situational awareness plays a large role in demand-response. When catastrophic events are avoided, price spikes will decrease. The same action and consequence are often replicated in the HAN. If energy usage can be more accurately predicted and identified, peak prices will not be as high or occur as often.

Achieving accountability in the HAN has rarely been studied in the past. Related areas such as disaggregation and load monitoring [26,42,43], are useful, but normally estimate device usage based on the aggregate amount from the residence as a whole and the normal consumption of a device. This type of estimation is more useful when identifying consumer behavior patterns and

device malfunctions instead of a more fine-grained approach of estimating and assuring that each device is accountable.

5.2.1. Accountability

Security has been one of the key areas of research in the smart grid landscape as new technology generally introduces new vulnerabilities. Accountability serves as a complement to the core principals of information security and the component that allows authorized individuals more robust tracking and auditing 8history as well as establishing trust and confidence within the HAN between devices [138,148]. Currently, accountability in the distribution end of the grid only extends to a single residence which aggregates the appropriate data of all of the devices located therein. This is sufficient for the currently required duties of billing the consumer based on total use of all appliances to be fulfilled, but in order for demand-response to be optimized on both sides of the equation, a more fine-grained approach must be utilized.

There are several requirements which can contribute to an effective accountable environment or mechanism. These include [28]: decentralization of accountability mechanisms, scalability, minimal impact, data collection, identity management. Inclusion of these elements in the accountable scheme can be very profitable and will help to cover the accountability requirements.

Lightweight functions are imperative in the smart grid as the devices utilized throughout are normally resource constrained, or given computational and networking resources that are not plentiful enough to handle heavy encryption and simultaneously satisfy the real-time demands of the grid. This also applies to any subset of software functionality included in the grid including accountability measures**.**

Sufficient and appropriate data must be extracted and archived for review and evaluation. It is imperative to discern the most effective location and type of data to archive and evaluate in each

environment. Some devices may require a specific set of data to be analyzed, while others may require a set of data which includes a few of the parameters explicitly required by one, and a few not needed to satisfy the requirements of another. Although in most environments these parameters will be uniform.

Inter-domain identification is also necessary. We assume that devices in the same domain will maintain uniform identification mechanisms which will allow them to distinctly refer to and differentiate between devices on the network. For smart grid applications, the main objective of accountability currently is to maintain record of and assure that a device acts as it says and/or is expected to. In other words, a device should truthfully report its power usage and other parameters required at a pre-specified time interval and/or when requested.

Maintaining the previously listed requirements for achieving accountability in a smart grid environment is a huge upgrade to still widely implemented AMR methods in which the sum of the power over a certain period is collected from aggregate data of all devices at the consumer's residence. Even in the case of AMI, there is still much room for error and we cannot always expect for the record that the utility manages and what is recorded at the consumer's end to be identical. Malicious action, malfunction, miscalculation in estimation, or calibration may be the cause of such differences. Making the HAN accountable on a more fine-grained level can help alleviate problems such as these and provide us with a means of locating a compromised device which can immediately be disabled or serviced instead of canceling service to the residence indefinitely.

5.2.2. Energy Consumption in the HAN

Energy sustains life for many people, and rightfully so domestic usage is behind a large portion of most grids' electric power consumption. Many devices and methods are being put into place which will give consumers the option of employing more energy efficient options in their homes.

Energy efficiency means that there is a reduction in energy used for a given service or level of activity due to some technological change of an existing infrastructure [149,150]. This is of particular interest, as the majority of consumers prefer to purchase lower end devices which though cheaper, also generally provide less energy efficiency of energy use [151].

Many factors are combined to determine household consumption rates. These are highly affected by environment conditions and consumer personal preference. This energy consumption is transient and varies dramatically at specific times. These factors play a large part in the determination of the peak rate times which are determined by the utility based on large overall usage by its consumer base. Peak rates are normally achieved during specific times of day when many consumers use considerable amounts of power. Though many devices in the home use small amounts of energy, when large amounts are powered on simultaneously, peak times and rates can be heavily influenced by this.

5.3. Problem Definition

In the currently implemented power grid, the only accountability required in the distribution domain is the periodic reading of the power meter which records aggregate energy usage at each user location. The frequency of readings is dependent on the utility and is generally limited to a few times per month. Inside the HAN, security measures can be put in place to introduce some level of networking accountability through a specific entity such an IDS, or the ESI, but in an environment such as the HAN where the number of devices will greatly increase over time, it is a good practice is to make the accountability mechanism distributed. This is also important as the resources many devices maintain are constrained in the HAN and additional computationally expensive software is difficult to run while maintaining its primary responsibilities.

Disaggregation techniques are wide ranging and have been well researched. The three major

techniques include [152]: survey, single point sensing, and distributed direct sensing. These techniques alone are simply not sufficient as more smart devices are being added to homes that are programmable. This means that the threat of malicious and/or malfunctioning devices is greater than ever and still increasing, and brings about the need for a more fine-grained model for accountability in the HAN.

In addition to creating an environment where the devices are accountable for their energy usage, the devices should also be made accountable for all of their actions with a scheme implemented in a distributed fashion. If a device takes an action that causes an unexpected amount of energy use, that action and the energy should be verified and the device accountable for it.

HAN devices' energy consumptions patterns are not necessarily static in the sense that though operation may be scheduled, they may use varying amounts of energy at any given time. These devices may also have a non-constant power capacity factor at any given time while it is active. Some examples of these types of devices include water heaters, boilers, even coffee makers. It is of great importance to implement a mechanism which can correctly assure accountability in environments utilizing such devices as well as detect any events that can be problematic. Once the events have been discovered in a timely manner, it should be categorized so that the appropriate actions can be taken to resolve the issue.

We consider a modern house with full smart grid capabilities and numerous smart devices in the home. Current technology requires the inclusion of some legacy devices, which are also included in the home and can not necessarily communicate using required protocols to maintain accountability in the scheme which will be proposed later. The home will have at least one smart meter which will measure the usage and serve as the "trusted" entity and will normally

communicate with the utility and other authorities outside of the home premises along with the ESI which the consumer will utilize.

5.3.1. Architecture

The HAN will serve as the basic communication infrastructure for management of energy in a smart grid. Normally, it is composed of a smart meter, many smart and connected devices, and alternate private energy sources and devices which are involved with storing energy. There is a general understanding that there are two basic architectures for the HAN and its interconnection to the smart grid [153]. Figure 5.1 and Figure 5.2 show two kinds of smart grid HAN architecture. Figure 5.1 allows for the utility to have direct control of the HAN devices for those who have for instance, opted into policy which allows the utility to modify device operation at specific times to minimize peak times and rates. Figure 5.2 splits the device operation adjustment responsibility between the consumer and the utility, or per the consumer's desire, solely on the consumer.

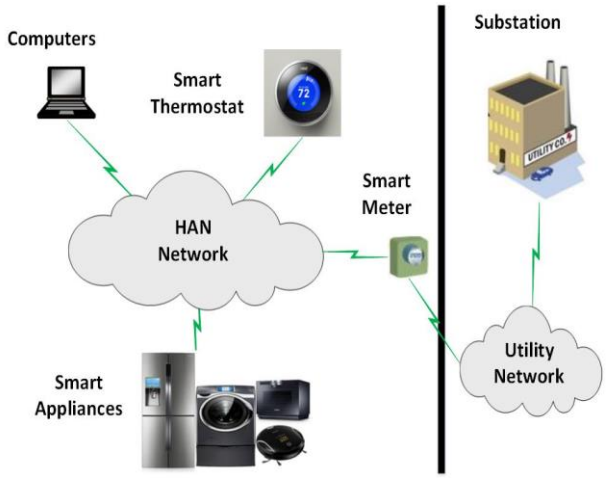

Figure 5.1: Version 1 of a Smart Grid HAN

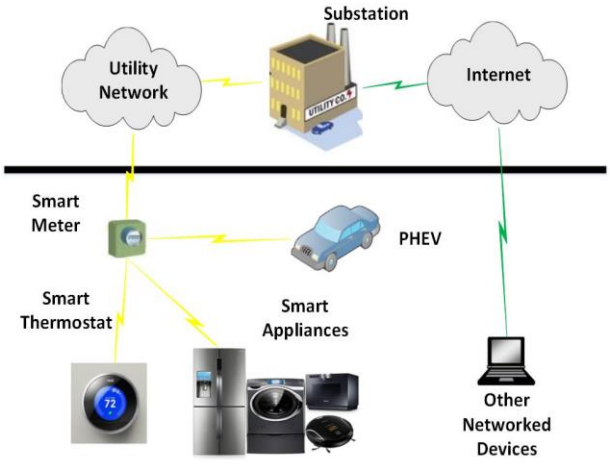

Figure 5.2 Version 2 of a Smart Grid HAN

Here, the smart meter, in either approach, is responsible for collecting consumption and generation of the aggregate of these devices in real-time over one of the many popular wireless

technologies. The devices can be divided into three categories. These include smart devices, connected devices, and legacy devices. In the context here, smart devices are fully qualified devices which maintain software and hardware capabilities to communicate over the protocols implemented on the network which it is connected to. These devices can also participate on the required schemes and algorithms being used therein. Smart devices also have the ability to modify their operation to better achieve objectives which benefit the network or operator of the device.

Connected devices are many times mistakenly categorized as smart devices, but lack the capabilities to modify their operation to positively achieve certain goals. While maintaining the hardware and software capabilities to communicate over the network, these devices only have the ability to report and/or observe their surroundings.

Legacy devices may lack networking completely, or simply may not be able to utilize certain protocols, and while still smart or connected, are rendered useless in the context of the HAN and its communication. Devices can also be categorized as schedulable and non-schedulable. This means that for scheduled devices, we will likely have more insight into the specific times in which the target device will be using power.

5.3.2. Varying Energy Consumption in the HAN

There are hundreds of millions of devices which have flexibility or varying consumption in the HAN. Much of this flexibility can be attributed to the time flexibility of the device usage due to management, or the upper and lower bounds of flexible energy usage amounts. In addition to this inherent variability which may or may not be induced by user interaction, many devices also host a range of energy consumption settings and the actual amount of energy consumption depends on the setting at that time. [154] describes the aggregation and disaggregation of these flexible devices and their flexible timing constraints. Though the aim of this chapter is accountability and accuracy

in the HAN, aggregation and disaggregation is out of the scope and of small benefit in this discussion.

Energy consumption is considered to generally be constant in most devices when estimating power consumption. This means that there will normally be some overuse or/and underuse. Therefore, for many reasons, including the previous, the measurement and estimation techniques are threshold-based. Scheduling helps to manage and estimate energy use to a certain extent, but the details of a varying consumer are normally partially defined by the habits of the user and cannot be sufficiently estimated unless sample testing and forecasting is in place along with high level control of the "varying consumer" (VC) devices introduced later.

5.3.3. Problem Statement

Accountability in the HAN is at best the minimal in that only readings of aggregate consumption are estimated daily. Disaggregation techniques cannot provide the fine-grained accountability required for the smart grid. The objective here is to verify and report device's actions inside of the HAN. A unique problem provided in the HAN is the accountability in energy usage of devices that have a varying power capacity factor and requirements.

Our goal is to provide an accountable environment in the HAN so that devices will be held accountable, while the devices' power consumptions are not constant, but varying over time. Therefore, we will propose a solution, i.e., a mechanism to achieve accountability for devices with varying power consumptions over time. We will also conduct some evaluations of the proposed method in terms of observing the amount of work required by the proposed method in comparison to a typical method, and device usage accuracy and estimation efficiency utilized as a metric.

5.4. Accountable Method

The proposed method utilizes group witnessing such as that which is proposed in [21]. This

discussion will detail the status reporting and inspection mechanism that is required to create an accountable environment in the HAN. The premise of the protocol is that devices called witnesses are used to monitor other devices in order to verify their actions. When multiple witnesses are utilized to monitor a single target, the target device will be held accountable by multiple entities as opposed to a single device which authorities would be solely forced to trust with the reporting of its target's actions.

The target-witness structure gains its validity and accuracy partially through a single device w_1 which serves as a witness to its target device *t*. w_1 utilizes readings from the sampling unit which is monitoring *t*, and together with two other witnesses (w_2, w_3) of which the latter two use NILM algorithms to estimate the usage of *t*, create an accountable witness target structure for each device in the network.

Once the reports are gathered the inspector must discover and report inconsistencies in the witness reports given by devices in the network which will be monitoring and reporting the actions of their target devices including energy consumption. A single pass through the set of inspectors *I* can determine the state of the network and each device therein to evaluate the network with a single inspector it takes at least *n* tests to evaluate a network with *n* operational devices in a one-by-one testing scheme. In order to reduce the number of work required for a full inspection two options are possible: reduce the number of witnesses per device and utilize a better method.

To identify any device as a "varying consumer" (VC), the consumption patterns must be identified. Some details may also be inferred from the devices rated power usage even though this amount will likely not be constantly consumed during the duration of the devices active phases. A probability distribution of the device's energy consumption must be built to estimate the usage. To complete this, each device will communicate with each of its witnesses which entails the minimum

and maximum power consumptions. With this and some additional information, we can construct a probability distribution table (PDT) which is explained in the following section.

5.4.1. Probability Distribution Table (PDT)

The proposed method utilizes a PDT to help create a higher level of accountability. The PDT, whose operation is defined in this section, allows for some levels of forecasting based on previously observed energy usage. The initial communication between two devices which are establishing a witness-target relationship will contain several pieces of information which are integral for the witness devices to perform their duties in the accountable scheme. These include minimum and maximum power ratings of the potential target device. These values will be used for the potential witness device to define which usage group the target device will be in and in turn, to estimate the energy usage of the device at certain times more accurately.

Table 5.1: Example PDT

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
12-1am	…	…	…	…	…	2	3
1am-2am	…	…	…	…	…	1	2
2am-3am	…	…	…	…	3	2	3
…							
4am-5am	…	…	…	…	1	…	…
7am-8am	1	3	2	1	3	4	4
8am-9am	1	3	2	1	3	4	3
…							
3pm-4pm	4	2	3	4	3	…	…
4pm-5pm	4	3	4	3	2	…	…
6pm-7pm	4	4	4	3	4	3	3
…							

Once initial information is acquired, in order to obtain the probability distribution of the target device, the “on” status probability must first be determined. In the initial phases of interaction after the contract between the witness and target, the active usage patterns including the patterns of device activation are observed. From this information, the table of usage probability is created.

Upon multiple observations of the target device, its' habits over specific time lengths can be determined. The continuation of these observations will allow for corrections and a more complete analysis of the device's actions. Table 5.1 shows an example PDT which is specific to the day and time of the week.

Management of data in the PDT and the access thereof will be monitored and controlled by policy. This policy will ensure that the accountability is not solely ensured by sampling capability, but in more of a non-intrusive manner. There is normally a fairly high amount of uncertainty in dealing with usage forecasting and therefore a model for each period of a half-hour is established. Similar procedures can be found in the following works [151,155,156]. In each half-hour interval, we establish the logarithmic or raw demand model as:

$$\log(y_t, p) = h_p(t) + f_p(w_{1,t}) + a_p(y_t, p) + n_t \quad (2)$$

where *y* is the demand and *p* is the one half-hour measurement period; *hp(t)* is the calendar effects including seasonal patterns and holidays; $f_p(w_{1,t})$ represents temperature effects with *w* representing the past temperature at the location; $a_p(y_{t,p})$ represents recent past energy usage observations; *nt* denotes error at a specific time *t*.

With this equation we can calculate values for the PDT at various times for devices which we have some energy usage data for. The PDT with these values will be used in the proposed method for furthering the accountability of the devices in the HAN. The values calculated here can be used as a measure to compare actual usage or usage estimated by some NILM method to in an attempt to establish a devices status.

In order to lessen what would be difficult computational requirements in the face of calculating much historical forecasting and environment data, a more streamlined bootstrap process is

designed similar to [43]: retrieve and utilize forecasting data and model, calculate load forecasts using temperature and calendar forecasts, block bootstrapping for the forecasting residuals, and update model through observations and historical data.

Many devices in the home will be able to even further streamline this process, as many of the effects due to calendar and temperature variability will be negligible. After sufficient observation and/or categorization, the model can be reduced further. This will also make concessions for the devices which are resource constrained.

5.4.2. Device Power Sampling

Power sampling plays a large role in the proposed method. Each of the devices in the home is assumed to be fitted with a sampling device for frequent sampling of the devices' energy usage. This section details some background of power sampling for appliances similar to the ones found in the HAN.

For a high level of accuracy, it is mostly agreed that monitoring devices must examine many features of the electric signals including the microscopic and macroscopic attributes. Microscopic here means harmonics and signal waveforms, while macroscopic means power state changes [43]. According to the Nyquist sampling theorem, it is necessary to sample at more than two times the frequency of the signal in order to capture the highest harmonic [157]. This detail is important as the real-time demands of the smart grid require for the data to be processed and forwarded very quickly. With sampling rates above 2.0 kHz, it may be generally difficult to overcome some of the inherent transmission and storage requirements for generally lower end data in the HAN. It is more realistic to envision mechanisms which record voltage around 1 Hz. Devices with this type of capability are normally more inexpensive and sufficient where the period is either 1/60 or 1/50 seconds [43].

Two feasible methods for sampling are described here. Considering the current state of technology and the direction in which it is headed, we can assume that most homes do not currently have advanced current flow detection mechanisms built into the internal circuitry of the A/C port which can acquire the voltage and current signals. With this understanding we can add these types of mechanisms to our definition of a "smart home". This will provide the witness devices access to sample readings of their target's current usage.

The second method relies on appliances and other devices with advanced hardware and sampling units fitted onto them. This will also provide the witness devices the ability to sample their target's usage. With sampling units fitted onto devices, or incorporated into the home wiring, the computational complexities and requirements can be offloaded from a central point. This will prevent from possible computational bottlenecks. These external devices can be the sampling units, or the devices which they reside on. Another method of maintaining efficiency is to only relay and store specific information about the devices load and events. Load changes and other events are not necessary to successfully verify the load reported by a device, therefore, there is no need to store or communicate all information.

5.4.3. VC Algorithm

During the initial phases of activation, witness devices observe the VC and build a table according to its tendencies over a specific time length. Observations of target device's state and energy usage are recorded over a period of time. These measurements can be scheduled or initiated when certain conditions are met e.g., high resource availability, the status of device being turned on. Once observed, this data may be used to challenge the accountability of the device. With the values in the PDT generated, one can assume and estimate the power usage at a certain time or phase of operation for a specific device. This makes testing for accuracy less error-prone, as

without knowledge of how much energy a device uses at a specific time, it is nearly impossible to create a threshold delta in which the device will be within at any stage of normal operation. The sampling and table construction are continued until the table is filled, and then passes are periodically made to verify and update the data to account for device behavioral changes (which are normally caused by the user).

Each device $\boldsymbol{i_n}$ in the network to a specific grade of rated power usage. Each of these devices possesses a certain number of attributes ***attr*** defined by the environment as {$\boldsymbol{attr}_{i,1}$, $\boldsymbol{attr}_{i,2}$, $\boldsymbol{attr}_{i,3}$, …, $\boldsymbol{attr}_{i,n}$}. Once the attributes of the device are combined, we find the rated power usage grade of that specific device, $Gp \mid p \in \rho$, where ρ denotes the number of grades in the HAN. Calculating the grade of the i^{th} device can be completed using Equation 2:

$$\boldsymbol{n^i = \sum_{k=0}^{n} w_{i,k}, attr_{i,k}} \qquad \textbf{(3)}$$

where, $w_{i,k}$ denotes the weight of the attribute represented in the summation while n^i will be assigned to one of the power usage grades by the following:

$$\boldsymbol{if\ (Gmin < ni < Gmax), ni \in Gp} \qquad \textbf{(4)}$$

G_{min} and G_{max} denote the lower and upper limits of the specific usage grade G_p, respectively. The value of n^i depends heavily on the environment and the attributes considered with the device. With the usage grade of a specific device known, the range of its power consumption can more effectively be estimated. The VC algorithm is defined in Table 5.2.

1. **Function Group** (*witness_devs*, *target_dev*)
2. //target_dev reports max possible power usage
3. discover_VC_tendencies(*target_dev*) // samples usage, or infer from target's broadcasted energy capabilities
4. **REPEAT UNTIL** usage_group(target_dev) // G_p is discovered
5 IF G_p is correct | $G_p \in$*GROUP(i)*
7. usage_group(target_dev) = *GROUP(i)*
8. **ELSE** redo group test for *GROUP(i+1)*
9. **END REPEAT**
10. Verify usage_group(target_dev) with sampled power usage
11. Build PDT with usage and time data
12. **REPEAT** discover_VC_tendencies(*target_dev*)
13. **IF** sampling data and PDT are differing above Δ*, mark target_dev "suspect" or "faulty"*
14. **ELSE** *update or confirm PDT based on newly acquired data*
15. **RETURN** PDT
16. **END REPEAT**

Figure 5.3: VC Algorithm

5.4.4. Multiple Status Reporting

Any status report made by a witness device, whether requested or scheduled, will contain the target device's usage state. Instead of defining this with only two values (on/off), we have at least 4 states for the target report. With these various reporting states, we can more closely estimate the power usage of the current device without sampling it. This is necessary for the witnesses of some target that do not have access to the sampling unit on the target device. How these states are defined is based on the reported consumption capability amounts of the target device. While the power usage grade is known, we can more precisely estimate the device's energy usage at a specific time by having multiple states (levels) within that devices usage grade which are relative to the device.

As G_p has an explicit minimum and maximum, we can further divide the state into 4 power ranges. The power consumption can be even more accurately estimated as future power sampling observes energy usage and consistently finds more specific readings within a state that is constantly sensed. With this information, the witness can assume that the target device uses a

specific amount of power (which has been consistently observed) while the target device reports the recently reported state.

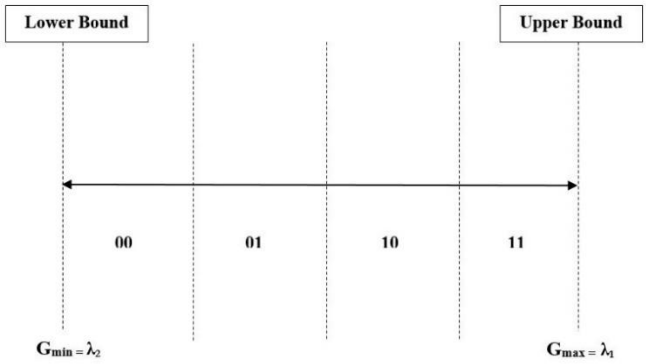

Figure 5.4: Usage States

Figure 5.3 shows the upper and lower bounds of a target device's consumption range. This range is further divided into several smaller ranges with sub-thresholds (ST) at the lower and upper bound of each. The four ranges will initially be equal in width with the ST values are chosen as:

$$ST = \begin{cases} \lambda_2 + D \\ \lambda_2 + 2D \\ \lambda_2 + 3D \\ \lambda_2 + 4D \end{cases} \quad (5)$$

$$D = \frac{(G_{max} - G_{min})}{No.of\ usage\ state} = \frac{(\lambda_1 - \lambda_2)}{4} \quad (6)$$

$$M = \begin{cases} 00, & \lambda_2 < X \leq (\lambda_2 + D) \\ 01, & (\lambda_2 + D) < X \leq (\lambda_2 + 2D) \\ 10, & (\lambda_2 + 2D) < X \leq (\lambda_2 + 3D) \\ 11, & (\lambda_2 + 3D) < X \leq \lambda_1 \end{cases} \quad (7)$$

λ1 is defined by the Gmin while λ2 takes the value Gmax which represents the complete consumption range of the device in question. For each M, which can be defined as the quantization

decision, there is a corresponding decimal value that will be associated with it based on the usage state the device is observed to be in according to its consumption range given by Equation 6.

$$m = \begin{cases} 01, & \lambda_2 < X < \lambda_1 \\ 00, & X < \lambda_1 \\ 00, & X > \lambda_2 \end{cases} \quad (8)$$

$$n = \begin{cases} M, & \lambda_1 < X < \lambda_2 \\ 0, & otherwise \end{cases} \quad (8)$$

$$y = (m + n) \quad (9)$$

where m and n are local decision variables which are defined by the current usage observed by the witness device. If the observed values fall within or outside of λ1 and λ2, it generates values as described in Equation (7) and Equation (8).

The decision model can be created as shown in Figure 5.4 utilizing the equations (7) and (8):

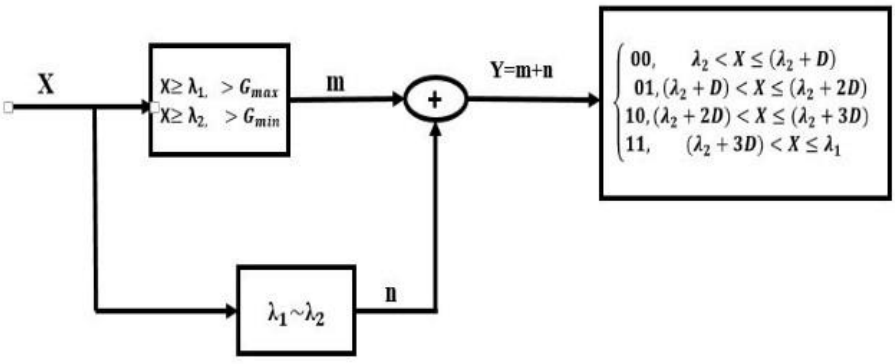

Figure 5.5: Usage State Flow

This decision model combines *m* and *n* with the addition operator '+' and outputs the usage state of the device for the witnessing device that is observing the targeting device which is using the energy.

5.4.5. Estimating Power Usage

In order to calculate the power usage of any device or to closely estimate it, the operational capacity P_i and the state of the device must be known [144]. In the case of VC devices, the energy

usage is not necessarily known at any time. This means that outside of random/scheduled sampling of the target device's power usage, there is no definite way of knowing exactly how much power a single device is using outside of inferring through deduction if the usages of the other devices in the HAN are available. There is also the threat that the device malfunctions or is behaving with malicious intent. Here lies our problem, and our solution lies within the estimation and accountability measures.

With the knowledge of the power usage grade G_p, and the status communicated from the target device, we can more accurately estimate the power usage at time t_i for any device *d*. with one of the witness devices (w_1) in question having the ability to sample the target device's power consumption through the sampling unit attached to its target, which is carried out regularly. We understand that we can derive the power usage P_d of a particular device *d* as displayed in Equation (10):

$$P_d = \int_{t_b}^{t_a} p(t) \cdot R_{d(t)} dt \qquad (10)$$

where *p* is the expected power consumption at time *t* and *R* is the running state that the device is in at time *t*. Understanding the rated power usage amount is not sufficient for the VC device, as the amount of power that this device uses is not necessarily constant. Therefore, in the previous discussion we introduced the premise of a power usage status for a specific devices, in this case *d*, ST_d which is partially determined by the power usage group G_p. These values are used to more accurately estimate the power usage at a specific time. It is understood that if $d \in Gp$ then at any time $p_d < max(G_p)$. In other words, the power usage for device d will never be greater than the upper bound on the range or the group that it resides among. If this anomaly data does occur the

device which reports this reading will be considered suspect or faulty and marked for further evaluation.

5.4.6. Varying Consumption Device Reporting

With the usage grade and the device power level status known, we can effectively construct a table for quick reference, or calculate the estimated amount on-board the witness device at the necessary time. The scheme for building accountability into varying consumption devices is presented in the following steps.

- The potential VC device is connected to the network. Recommended scheduling is verified as well as device attributes.
- The potential VC device informs proper authorities (e.g., witnesses, smart meter) of the minimum and maximum power usage/requirement. This value will be used to assign the VC into a usage grade G_p.
- The VC device informs proper authorities of its initial usage state (level 0-4) while witness w_1 samples the VC device's power consumption. Witnessing devices calculate the expected power usage (from the usage grade and the status report) and create a status report. If the reported usage states differ between witnesses, label the device faulty.
- Witness devices build PDT while continuing scheduled sampling of the target's (VC device) power consumption. This information is used to update the PDT as well as challenge the target's accountability.

At any time that a device's reported status, or time constraints are found to be incorrect or suspect, that device is labeled as suspect or faulty.

5.4.7. Legacy Devices

Although legacy devices participate in the accountability protocol, they most likely will not have the software and hardware components to communicate over a network with the required protocols. The proposed algorithm allows us to estimate their power usage more accurately. With this more accurate approximation, we can patrol even legacy devices with static energy consumption and derive whether or not the device is behaving correctly. The difficulty here is that the legacy device cannot serve as a witness. As the proposed method allows for efficiency in such a way that all devices are not required to serve as witnesses, legacy devices will exclusively serve as targets and be evaluated in the say way that non-legacy devices are.

5.4.8. Threshold Detection

Determining faulty devices can be accomplished by comparing the current usage with the expected or reported usage at a singularly specific time. If these two numbers do not maintain proximity within a certain delta, the target device will be labeled according to the event management policy. This delta will be the threshold with which detection and comparison will either earn the device in question a faulty or clean labeling.

The comparison of the energy usage and the threshold is trivial, however, the process of establishing an acceptable threshold is most important and normally device attribute dependent. As stated earlier, many VC devices have modes of operation, which means that the energy usage amounts for each of those modes will likely be very much similar whenever the device is operating in that specific mode. In the case that this usage amount is not within its specific threshold level, witness devices can more accurately estimate the usage when the device is operating in an expected mode. VC devices that do not have defined operation modes generally operate on a sliding scale which is influenced by external conditions or an interval-based time schedule. A water heater for

example maintains and heats the temperature of water and uses energy according to the temperature of the water which is in turn influenced by external temperatures among other variables. Determining the amount of energy these types of devices will use is very difficult as current policy attempts to estimate based on forecasted conditions and other events. Operation in this capacity is more likely to produce energy usage which is close to the thresholds, and in some instances will produce conditions that will likely be further away from acceptable than desired.

5.4.8.1. Threshold Analysis

A recurrence quantification analysis (RQA) can be used to generalize the usage of a generic device, and from this, establish the necessary thresholds based on its habits. With use of the analysis, densities of recurring energy usage amounts can be identified and used to establish quality thresholds. Recurrence analyses, in the past have been used to locate recurring patterns and structural changes in dynamical systems [158], and with data from one of the VC devices based on a univariate time series which is of some n-dimensional model, the systems behavior detailed in the time-delay statistics can be constructed be constructed into phase space vectors and then to a topologically equivalent multidimensional plot [159]. This recurrence plot (RP) is simply a visualization of the recurrence matrix (RM) *R* in which we can define the entries in this matrix, R_{jk}, at row *j* and column *k* using the equations below [160]:

$$R_{jk} = H(\lambda - d_{jk}) \tag{11}$$

$$d_{jk} = \left\|\vec{V_j} - \vec{V_k}\right\|_2, j, k = \overline{1, N} \tag{12}$$

Here, *H* is the Heaviside step function which is assigned value relative to zero, as is denoted in Equation 13:

$$H(x) = \begin{cases} 0, & x < 0 \\ 1, & x \geq 0 \end{cases} \tag{13}$$

- $\overrightarrow{V_j}$ and $\overrightarrow{V_k}$ are the row and column vectors created by the n-tuple of energy measurements in R
- λ represents the acceptable standard deviation from the initial time series of energy measurement of the entry
- d_{jk} represents distance between the two vectors $\overrightarrow{V_j}$ and $\overrightarrow{V_k}$. [159] allows us to reconstruct the phase space vectors as specified by Taken's time delay embedding theorem with n samples from a device yielding:

$$\overrightarrow{V_j} = i_j + i_{j+t}, \dots i_{j+(m-1)t} \quad (14)$$

In Equation 14 m is the embedding dimension function and t represents the time delay while j is the time index. To observe the time series from a non-linear system the embedding dimension or n-dimensional Euclidean space for reconstruction must be determined. In the case of VC devices and this RQA, the embedding dimension will always be 2. From here, the can be RP is generated from the phase trajectories similar to the method in [160]. Once the RP is created, the densities therein can be analyzed for a more reliable threshold parameter through adjusting the threshold boundaries of the usage state to more properly enclose the densest areas of the RP.

5.4.8.2. Threshold Selection

Throughout the history of fixed threshold selection methods, many types have been used including graphical and diagnostic approaches in order to assess a model for threshold choice beforehand. Several of these include stability plots, mean life residual plots, and general distribution plots, to name a few [161-166]. In certain cases, graphical approaches can be difficult to interpret and uncertainty of the threshold is not well accounted for [167]. Although, many studies maintain such a hindrance, some informal remedies have been proposed in the form of resampling-based approaches [168-170].

There have been several general guidelines suggested for the selection of a desirable threshold [171]. These values should be represented within a small percentage of the phase space diameter.

In terms of device energy usage, the phase space diameter can be defined as $G_{p,}$ or the entire possible energy usage range. Also, threshold uncertainty should be incorporated into the analysis as well as removing the necessity of subjective selection of parameters of the threshold. In order to ensure effective threshold selection, the method proposed in this work incorporates some components of the Bayesian mixture model which helps to find values based on a certain criteria from some overall set of values. RQA will be utilized in the refining of the thresholds to create a more accurate environment.

The phase space of a VC device encompasses all usage states possible for the device, or in other words, the complete consumption range. The consumption range properties can be characterized based on a partitioning $\{S_1 \ldots S_n\}$ of the device's phase space into *n* disjoint sets [172]. As explained earlier, each one of these sets represents a usage state.

There must be at least two stages of the threshold defining method. The first will provide for defining threshold for devices where there is minimal or no usage correlation data, while the second will provide devices which have sufficient usage data available for analysis. For the first method, the initial phase space partitioning is described in section 5.4.4 by equally distributing the consumption range of the device among the usage states. The upper and lower thresholds will be initially among the more extreme percentages of the usage states amounts in the case of devices with insufficient observable data.

Upon further observation while the device is active, the RQA can be used to reveal the bounded areas of the highest concentrations of usage amounts. With such an analysis, the thresholds can be placed at values which are most effective in categorizing the usage states efficiently by ensuring that the thresholds are placed in areas of little to no recurrence density through normal operations.

From here, [173, 174] demonstrate a method to generalize the extreme values given previous observations, X_1, X_2, $X_3 \ldots X_n$. This can be done through utilization of distribution function F(x), under conditions $F(x|\lambda) = P(X_i \leq \lambda + x | X_i > \lambda)$ can approximate these values by a general Pareto distribution (GPD) with a density function defined in Equation 14 [175,163]:

$$H(x;\sigma,k) = 1 - \left(1 - \frac{kx}{\sigma}\right)^{1/k} \quad (14)$$

$$\text{while, } \begin{cases} 0 < x \leq \infty, & k \leq 0 \\ 0 < x \leq \sigma/k, & k > 0 \end{cases} \quad (15)$$

- k is the shape
- σ is the scale
- x is a random variable with a standard exponential distribution

With estimates from the initial graphically established threshold, the GPD has an interpretation as a limiting distribution in such a way that we can use this to generalize extreme values within the current usage state based on the observations. This will allow us to modify the threshold in such a way that the majority of points in the RP occur well within the usage state in question. This will increase efficiency and maintain the threshold and the usage state in its entirety at the optimum placement.

5.4.8.3. Pitfalls and Limitations

Any method of detection or estimation has some type of performance limitation. These types of drawbacks can easily result in the producing of false positives and/or false negatives. Consideration of analytical variability can help to resolve conflicts arising from inaccuracy of estimation or measurement [176]. Instilling a system where multiple entities concurrently verify the accountability of each other may also help to pre-empt inaccurate measurements which may lead to malicious or damaging activity which is the objective of this study.

Many household appliances and devices are composed of sophisticated circuitry and many components and circuits. This creates possibilities for electrical interference of many types which can lead to inaccuracies in measurements or the improper calculation of a device's usage. Often these inaccuracies are caused by some defect or failure while in other situations, devices constantly produce interference as a byproduct of their operation [177]. It is well to note that manufacturers are generally required to follow standards provided to them by various entities when designing and manufacturing their products in order to avoid excessive electrical interference [178]. Even with these considerations, there are still certain families of devices typically used in the home which are not under the jurisdiction of these regulations, and can interfere with other devices if certain precautions are not taken.

Under normal conditions, when a device acts as a source of interference to another, the device itself is susceptible to interference of the same type. The most frequent offenders in the home tend to be lighting fixtures and halogen light bulbs, also, touch and air conditioner controls. The framework used in the distribution and transmission line systems are also causes for heavy interference over areas as large as the typical neighborhood [179]. Figure 5.5 displays the flow of the threshold management process.

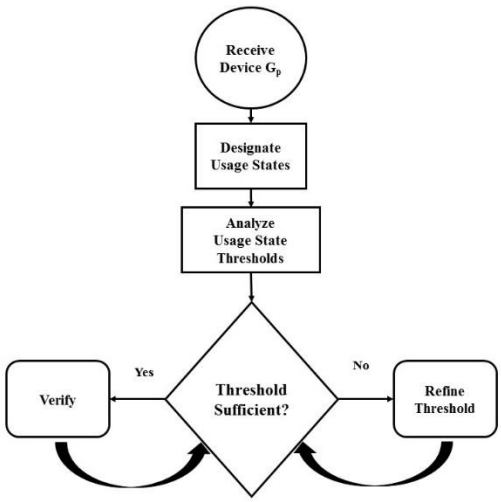

Figure 5.6: Threshold Process Flow

5.5. Evaluation

This section will analyze the proposed method detailed in the earlier sections. It must be understood that the purpose of this effort is to contribute to and enhance accountability in smart grid networks. Most publications in today's smart grid HAN energy academic area focus on optimizing load scheduling in the consumer domain. Establishing accountability is also an extremely important feature that the grid must enhance, which the proposed algorithm helps to accomplish. This accountability is furthered on a per-device basis which differs from other studies in accountability which focus on multi-user households [180], and understanding users and how to motivate savings [181].

5.5.1. False Positives/Negatives

We can model probability of the behavior of devices using two parameters: probability of detection, (p_d) and the ratio of false alarms (p_{fa}). p_d represents the probability that a witness device has sufficient information about its target device to evaluate and generate a sufficient and effective status report. This report labels the target device faulty, suspect, or clean. In either case, there is a probability that this event result can be false. False or incorrect labeling of a device can be categorized into two types: false positives or p_{fp} result in a device falsely being labeled as "faulty" or "suspect". Since each device in the network participates in the inspection and has the authority to implicate other devices to malicious intent in the network, namely its targets, each device is always untrusted by default. Therefore we can observe false positives as a case that clean device falsely labels a clean target device as faulty and a clean device falsely labels a clean target device as suspect. On the other end of the spectrum, false negatives or p_{fn} can be defined as a witness device incorrectly labeling its' target device as clean in the instance that it is actually suspect or faulty: a clean device falsely labels a faulty target device as clean.

There may be several reasons for which a false alarm may occur. Device *d* provides some indication of its target *t's* status after some information either gathered from the sampling unit or from estimation with some NILM mechanisms. There is a possibility that device *d* may become compromised and is intentionally committing malicious acts such as providing false reports of device *t* on the network. The method assumes that not all witnesses of a single device are compromised at the same time, and therefore during regular operation, device *d* observes its target device *t* and evaluates the details of its energy usage. With this information reported, a status indication for *t* is developed and communicated to the management unit which will normally be the smart meter, and the appropriate actions will be taken to have the device properly serviced based on its condition.

In the instance that *d* is compromised, it may report false information which forces an issuance of a "faulty" status to *t*. Similar to [182,183], all information that is observed from and originates at *d* is unforgeable, only in the case of dropped messages or lack of measurements can the false positives of this type be generated and communicated as long as there is at least a single correct witness. Any other false positives may be due to malicious action or faulty estimation/reading.

While assuming that the number of witnesses per device is fixed, we can display several important properties. Evaluating a correct device and producing a correct report can be accomplished with a probability of p_d. p_d is dependent on the sampling unit or the NILM mechanism used to gather data about device *t'*s energy usage. The probability of false reports and the events creating these are used to come to a final ruling on device *t* and assign a status for further action.

We must review the load disaggregation algorithms which may be utilized in the estimation of the energy usage of the devices in the HAN. Current literature generally uses recognition accuracy

as the main metric for measuring the effectiveness of NILM research. Although much of the work here provides accuracy metrics, it is difficult to draw meaningful comparisons and conclusion from the metrics provided by differing algorithms. [195] suggests 3 accuracy measures for performance evaluation: detection accuracy, disaggregation accuracy, and overall accuracy. Taking this into consideration, Table 5.3 displays several popular types of disaggregation techniques and their typical overall accuracy rates.

Table 5.2: Load Disaggregation Algorithm Comparison [197]

Algorithm	**Features**	**Accuracy**
SVM [184-186]	SS & Tr	75-98
Bayes [186,187]	SS	80-99
HMM [188-190]	SS	75-95
Neural Networks [62, 66, 67]	SS & Tr	80-97
KNN [185, 189, 190]	SS & Tr	70-90
Optimization [194-196]	SS	60-97

Steady State (SS), Transient State (Tr)

We can describe the accuracy rates as the acceptable and common percentages experienced when utilizing these methods. Upon observing Figure 5.6, we can understand how the false alarm rate is affected by NILM accuracy.

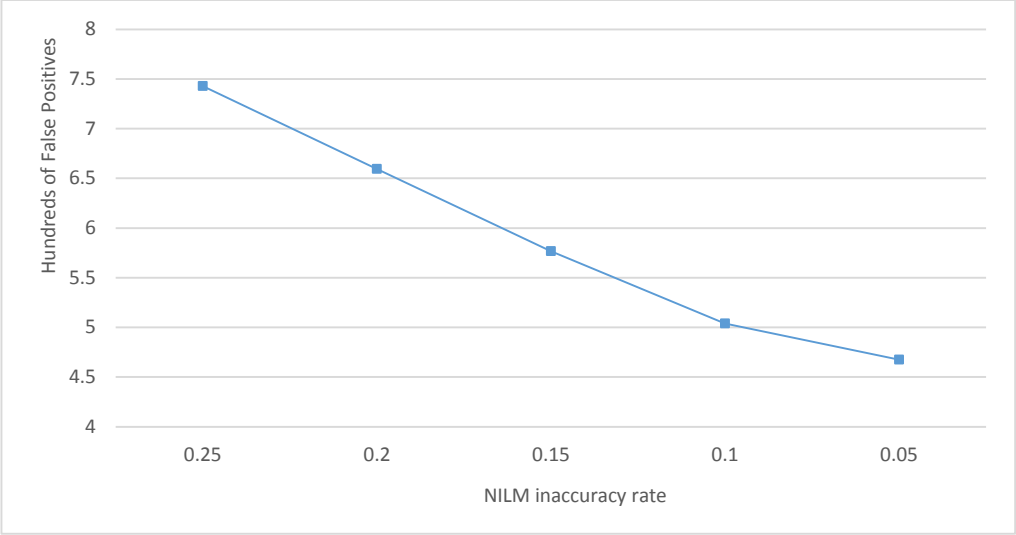

Figure 5.7: False alarms as Affected by NILM Accuracy

As shown in Figure 5.6, the number of false alarms is affected greatly by the NILM accuracy at a linear rate. With 20 devices in the simulation and 200 comparisons of energy use per device, we have a false alarm rate of .19 when using a disaggregation algorithm which has 85% overall accuracy, and when using an algorithm with 95% accuracy we have a false alarm rate of .12. These percentages are observed in the initial usage states with no training time required. After proper usage state training, the usage states will be more closely fitted to the typical amounts of energy used in its state, which will create a situation where fewer false alarms are signaled during the method's operation.

The accuracy is heavily dependent on the original source estimation (NILM) of energy usage as the proposed method looks to assure accountability in the energy usage of these devices. The false alarms are detected whenever one of the usage amounts produced by a target device has two reports which do not match each other. The sampling unit on each device must maintain a high detection accuracy to justify the initial error of the NILM. These efforts together can provide a significantly acceptable accuracy for usage accountability.

5.5.2. Energy Usage

The following will discuss the performance of the proposed method. In the considered smart grid HAN, the simulation will encompass the devices connected in the network which is also interconnected digitally and electrically with the smart grid. We assume that each device in the HAN is complete with an energy sampling unit in order to verify attributes and actions of peer devices in the network. This is a responsibility of each device which, in working together, will work to create a trusted and accountable environment. There are n=40 devices in each home, and a single home represented in each simulation. Attributes of each of the devices are all extracted from the Appliance Consumption Signature Database (ACS-F1) database for appliance consumption signatures [182]. The ACS-F1 appliance signature database contains device consumption signatures which were acquired by plug-based sensors. Acquisition was performed with device in the database undergoing two acquisition sessions of an hour in which specific details about the device's consumption was recorded. For simplicity, the data utilized spans a single hour of the 2 hour acquisition phase which is carried out on each device.

We assume that witness devices are able to discover the operational time of each device, as well as its power requirement information. This functionality can be programmed into the specific device so that this information is broadcasted upon connection. Also, assumptions can be made of legacy devices and verified with the sampling unit and/or NILM technique. Flexibility in operational time should be available, but as discussed earlier, load management and estimation of future energy usage are not of concern in the assurance of HAN accountability.

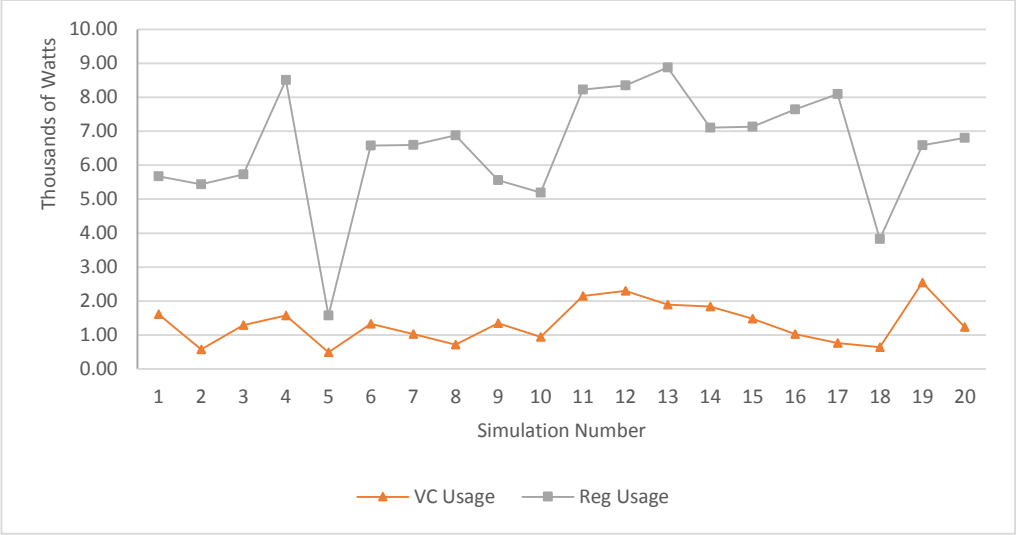

Figure 5.8: Total Power Usage

Figure 5.7 shows the results of energy usage in the HAN comprised of VC devices that use a presumably non-static amount of energy in kW-h format. Presented here is the total energy usage of each device throughout the 20 simulations. The measurements are carried out under the same per device load signatures which are found in the ACS-F1 database, and the energy data is represented for one hour of each device's acquisition period. The amount of energy usage difference here is fairly significant when evaluating a single hour of device powered on activity. The most important observation from Figure 5.7 is the disparity between the VC and regular usage for each device. The regular usage is represented as the maximum amount that the device would use at any time, but for the simulation, in order to stay in the bounds of the ASC-F1 database, we utilize the maximum amount recorded in the device record. The VC usage in Figure 5.7 is the total amount that the VC device's used over the acquisition period. The most important observation from Figure 5.7 is the disparity between the VC and regular usage for each device. This shows that any estimation using a device's maximum consumption over its' active time would be significantly over the actual usage amount. Generally utilities use methods which can more accurately estimate

usage than the disparity displayed on Figure 5.7, but this is giving us an extreme baseline for measurements and evaluation.

Figure 5.8 gives us insight into the increased usage estimation created through usage state utilization for the VC devices

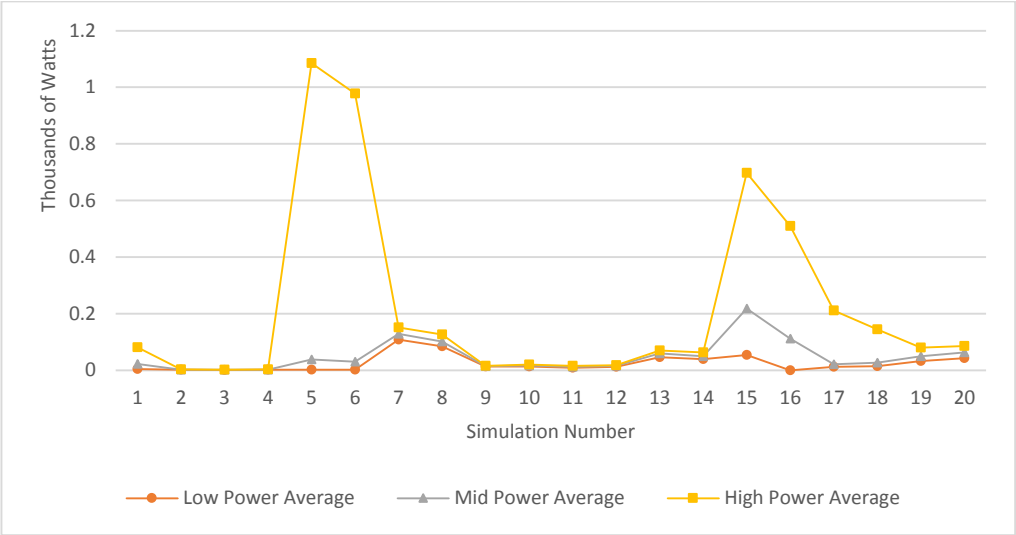

Figure 5.9 Usage State Amounts

For simplicity, each of the devices is limited to only three usage states. In the typical HAN, this could affect the accuracy for devices which use a much broader range of energy during their operation. Such devices as HVAC which maintains a very wide possible consumption range, which would likely need several more usage states to make estimation as efficient as possible. Figure 5.8 details how, on average, much power the devices used in the simulation in each of the three usage states. We can see that once again there is a disparity between the lower and higher usage amounts. Generally, according to Figures 5.7 and 5.8, we see that these types of appliances' usage have been most often near the upper or lower ends of their consumption ranges. With this type of usage, assumptions along with usage states can very easily be implemented to understand energy usage of a device for accountability purposes without implementing a full NILM mechanism. Even in instances where the usage range is very small (simulations 2-4, 9-12) the majority of the usage

remains near the extreme upper or lower usage amounts. Therefore, the usage state has a more accurate labeling on the amount of energy used whenever usage is in its' range.

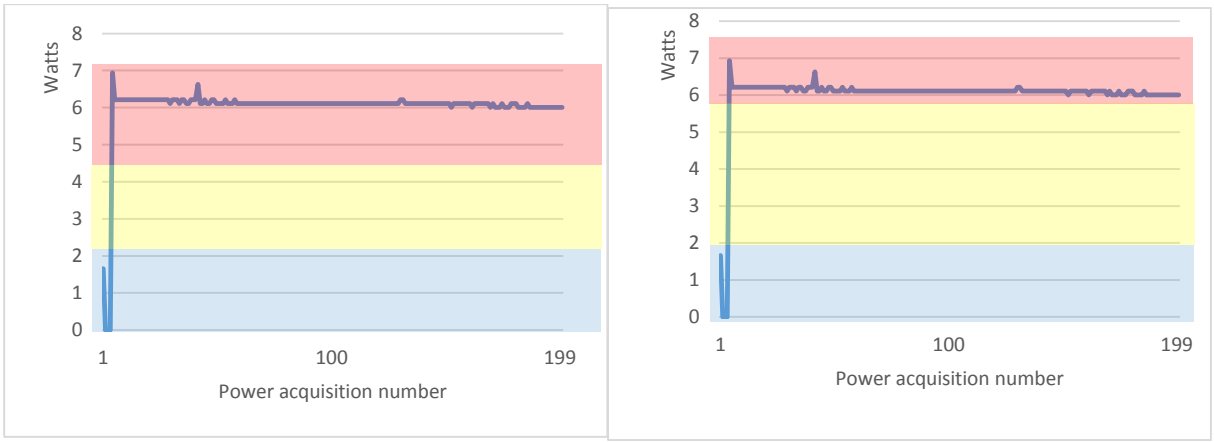

Figure 5.10: iphone 4 Usage States (before and after One hour of usage)

In the instance that a device has a small usage range such as the iphone 4 in Figure 5.9, we can see that among the rises and falls of usage amounts, the most time is spent at either end of the highest or lowest usage state. Also, the amounts of energy usage are fairly constant which provides a level of confidence in efficient procedure of the usage state estimation algorithm.

The VC method evaluates the power usage of a device with a threshold-based algorithm and categorizes the amount in one of several categories. For simplicity, the usage states are broken down into three (high, medium, and low). The basic method does not take this into account, and although any checks and balances of systems are also threshold based, they do not take into account VC devices, and therefore a larger deviation from what is estimated may occur. This can lead to an increase in the number of false positives or negatives. We can also see that from Figure 5.9 that the distance can be fairly dramatic relative to the usage space between the high and low states. This usage amount difference must be accounted for even if the devices are in those phases for a short time in order to make estimation and efficiency more effective.

It is also necessary to understand and analyze the time that the devices are operating in these states as its importance cannot be understated. Figure 5.10 gives us insights into these measurements.

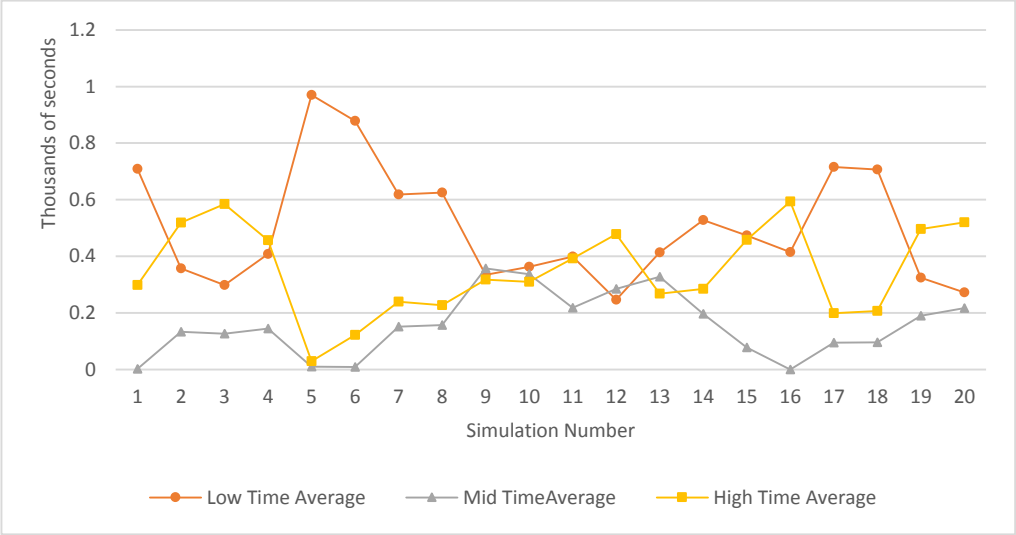

Figure 5.11: Usage State Time

As shown in Figure 5.10, much time is spent outside of the middle power usage states with the VC devices. In instances where more middle usage state time is observed, this happens in instances which devices make many state transitions, or when the device has a small consumption range. The thresholding method will modify the usage states accordingly in order to avoid increasing false positives. With this taken into consideration, we see that the variation in energy usage which normally makes estimation without lengthy training very difficult, is accomplished with adequate accuracy.

5.5.3. Varying Consumption Performance

This VC accountability method requires certain amount of parameters to be set prior to its execution. The usage state details pertaining to the separation of state space is required. Increasing the number of usage states will not degrade the performance of the algorithms, instead will allow witness devices to more accurately determine the current usage of its target device. Also, the details

of the power capacity of each device will need to be known. In the process of estimation of the energy usage of a target device, the witness device does not always sample the target's usage, the PDT and/or knowledge of the current usage state will in most instances suffice for estimation purposes. Another important detail is understanding that devices with differing operational modes or phases normally use similar amounts of energy while residing in a specific state. With some knowledge of the usage states we can sufficiently know estimate how much energy is being used. Table 5.4 displays the variances in recurring usage state values and their actual values which were recorded during the simulation. As shown in Table 5.4, there is definitely a discernable difference in the accuracy which is created by understanding the usage in a specific usage state as opposed accepting the maximum usage amount for each device whenever in an "on" state or not. Through the simulations, the average difference in measurements is 21.90%. It is important to state here that the method proposed is not to rely on the sampling units for measurements, but to ensure accountability through multiple witnessing, with this, most of the estimation can be done through simply have knowledge of usage states and accessing the PDT for prior usage information. In modern estimation and load monitoring, nearly 90% accuracy is acceptable, especially in non-intrusive load monitoring scenarios [182,183].

Table 5.3: Total Usage Amounts (watts)

VC Usage	**Regular Usage**	**Usage Difference**	**Difference Percentage**
1615.79	5672.32	4056.53	28%
571.62	5433.51	4861.88	11%
1292.64	5730.30	4437.65	23%
1573.79	8506.18	6932.38	19%
491.35	1572.07	1080.72	31%
1326.46	6581.45	5254.99	20%
1028.96	6599.65	5570.69	16%
721.01	6876.50	6155.49	10%
1345.66	5561.11	4215.46	24%

939.12	5191.61	4252.50	18%
2148.35	8225.62	6077.27	26%
2298.73	8345.76	6047.04	28%
1895.60	8877.86	6982.26	21%
1833.84	7104.06	5270.22	26%
1478.75	7134.92	5656.18	21%
1029.22	7638.08	6608.86	13%
764.86	8090.58	7325.72	9%
644.63	3826.21	3181.58	17%
2546.18	6585.76	4039.58	39%
1230.98	6798.86	5567.88	18%

5.5.4. Message Overhead

In order to analyze the message overhead of the accountable method, we adopt the analysis method used in [6,55]. *d* represents any device on the network while *w* represents some witness on the network. The assumptions apply specifically to any device *w* which has a witness target relationship with device *d*. *M* represents the smart meter. We present the accountability goals:

G1: *M* CanProve (*d* is faulty or correct for all *D*)

G2: *w* CanProve (*d* is faulty or correct)

We assume that public key infrastructure (PKI) is being implemented on the network in the communications taking place in the fashion described below. Only signed messages are considered after target-witness establishment.

Message 1: *w* Recieves (t_a, $\{Gmax_d\}$ Signed with K_x^{-1})

Message 2: *M* Recieves (t_a, $\{Gmax_d\}$ Signed with K_x^{-1})

Message 3: *M* Recieves (t_b, $\{Acc_d\}$ Signed with K_w^{-1})

Assumptions required for accurate analysis of the communication flow are:

A1: All *d* CanProve *M* is trusted (by default and PKI implementation)

A2: *w* Recieves (t_a, $\{Gmax_d\}$ Signed with K_x^{-1}) , Therefore, (*w* CanProve *d* is trusted) due to the PKI implementation.

Message 1: When *w* receives message A1, integrity and non-repudiation can be verified based on the unique signature. With *w* serving as device *d*'s witness, it can calculate *d*'s power usage at any time *t* either by querying *d*'s usage monitor or by utilizing the NILM scheme. This satisfies G1.

Message 2: *M* receives message 2 at the same time as *w* receives message 1 and can also prove that device *d* is trusted.

Message 3: *M* receives message 3 and by comparison of the accusations from all device *d*'s witnesses, can come to a conclusion about device *d*. This satisfies G2.

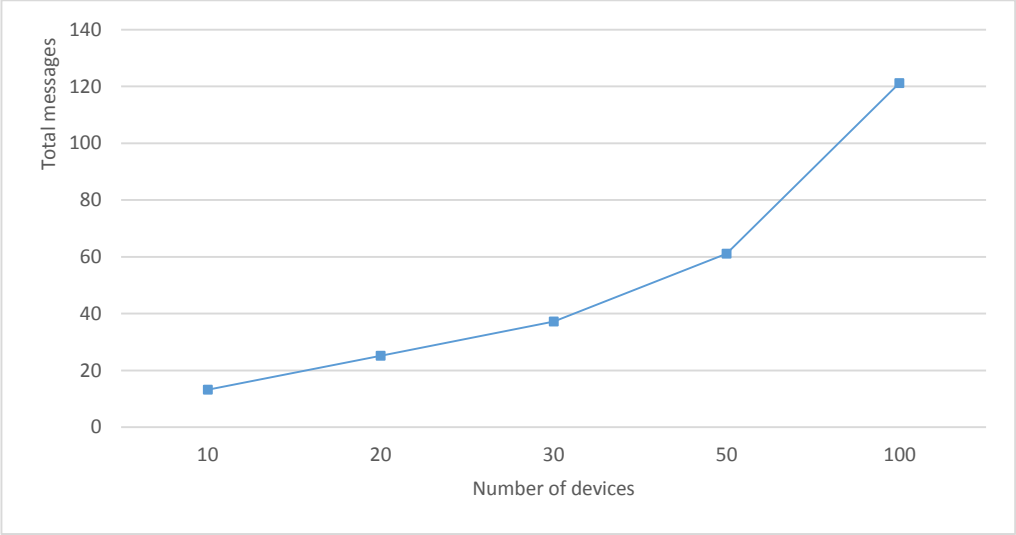

Figure 5.12: Message Overhead

Figure 5.11 shows the network overhead experienced in the method process. The results are gained after a series of 200 simulations of the witness-target status relationship handshake process for each device and a single inspection procedure. The growth rate is almost linear while the curve is produced due to the variable amount of extra witness request response messages that are sent to

devices requesting witnesses upon initial connection to the network (or upon losing a witness due to inactivity/departure).

5.6. Conclusions

The state of smart grid capabilities will continue to evolve as time passes. This means that technology and all other necessary components will continuously advance. Without accountability in the HAN, many deficiencies in security and accuracy can be exacerbated. This chapter highlights the modern state of accountability in the HAN and typical home energy usage. The proposed VC energy usage accountability algorithm was given as a solution to more effectively provide accountability and enhance accuracy in the HAN energy calculation schemes. Simulations of the method show the ability to efficiently monitor and identify malicious devices using unexpected amounts of energy. The simulations also demonstrate a marked improvement over estimation with trivial amounts of knowledge of a device's energy usage during operation. The accuracy and overhead required are both well within the typical bounds of current estimation methods.

CHAPTER 6

CONCLUSION

The research presented in this dissertation provides for some understanding of the current security posture of the current smart grid. In addition to a security analysis, methods are proposed to advance and incorporate more internal accountability into the modern home area network (HAN) at a fine-grained level. More specifically, we have studied the malicious device inspection and accountability of devices that consume varying amounts of energy while they are powered on.

We have reviewed the current attacks and countermeasures which have been exploited in a smart grid. The possible vulnerabilities are listed categorically along with the possible and proved exploits. A survey of grid security is important to identify weak points in the grid security environment.

We also propose algorithms to efficiently provide accountability in the smart grid HAN through multiple witness monitoring and inspection of the devices therein. An inspector selection algorithm is proposed as well. The algorithms provided show their validity in environments of a dynamic nature, where complete device inclusion is required and there is always a possibility of changing malicious statuses. The analysis and simulations in the study shows that the proposed algorithms are effective in creating an accountable environment in a smart grid HAN.

Finally, we propose a method for accountability of varying consumption devices. We utilize the ACS-F1 load signature database for method simulation purposes. Algorithm analysis and simulation results show that the method is effective. Simulation results also show that the

method is well within acceptable rate of error based on today's standards of estimation without need of previous knowledge of device profiles.

REFERENCES

[1] Farhangi, H., “The path of the smart grid,” IEEE Power and Energy Mag., vol. 8, pp. 18-28, 2010.

[2] National Institute of Standards and Technology. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0 [online] Available: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf

[3] Mihui, K., "A survey on guaranteeing availability in smart grid communications," Advanced Communication Technology (ICACT), 2012 14th International Conference on , vol., no., pp.314-317, 19-22 Feb. 2012.

[4] Xiao, Y., "Editorial," International Journal of Security and Networks, Vol. 6, No.1, pp. 1 - 1, 2011.

[5] Kundur, D., Feng, X., Mashayekh, S., Liu, S., Zourntos, T., Butler-Purry, K.L., "Towards modelling the impact of cyber attacks on a smart grid," International Journal of Security and Networks, Vol. 6, No.1, pp. 2 - 13, 2011.

[6] Gao, J., Xiao, Y., Liu, J., Liang, W., Chen, C., “A Survey of Communication/Networking in Smart Grids," (Elsevier) Future Generation Computer Systems, Vol. 28, No. 2, Feb. 2012, pp. 391–404.

[7] Khurana H., et aL., "Smart-Grid Security Issues," Security & Privacy, IEEE, vol. 8, pp. 81-85,2010.

[8] Gungor, V. C., Lambert F. C.; “A survey on communication networks for electric system automation” Computer Networks, vol. 50, pp. 877-897, 2006.

[9] Liu, J., Xiao, Y., Li, S., Liang, W., Chen, C., "Cyber Security and Privacy Issues in Smart Grids," IEEE Communications Surveys & Tutorials, Vol. 14, NO. 4, pp. 981 - 997, Fourth Quarter 2012.

[10] Kanabar, M.G., Voloh, I., McGinn, D., "A review of smart grid standards for protection, control, and monitoring applications," Protective Relay Engineers, 2012 65th Annual Conference for , vol., no., pp.281-289, 2-5 April 2012

[11] Ayers, L.M., "Implementing Smart Grid standards: A letter from the trenches," Innovative Smart Grid Technologies Asia (ISGT), 2011 IEEE PES , vol., no., pp.1-5, 13-16 Nov. 2011.

[12] Nano Markets., “Smart Grid Sensing, Monitoring and Control Systems : Market Opportunites 2011” Mar 2011.

[13] SAP Community Network., [Online]. Available: http://scn.sap.com/community/research/blog/2012/08/08/es-in-web-applications-through-automated-type-analysis.

[14] Lin, J., Zhu, B., Zeng, P., Liang, W., Yu, H., Xiao, Y., "Monitoring Power Transmission Lines Using a Wireless Sensor Network," Wireless Communications and Mobile Computing (WCMC) Journal, John Wiley & Sons, accepted.

[15] Wang, L., Xiao, Y., "A Survey of Energy-Efficient Scheduling Mechanisms in Sensor Networks," ACM/Springer Mobile Networks and Applications (MONET), Vol. 11, No. 5, 2006, pp. 723-740.

[16] Gao, J., Liu, J., Rajan, B., Nori, R., Fu, B., Xiao, Y., Liang, W., Chen, C., "SCADA Communication and Security Issues," (Wiley Journal of) Security and Communication Networks, Vol. 7, No. 1, pp. 175–194, Jan. 2014.

[17] Flick, T.; Morehouse J.; “Securing the Smart Grid” Syngress Pub. Sept 23, 2010. pp23.

[18] North American Reliability Corporation. “Reliability Standards” [Online]. Available: http://www.nerc.com/page.php?cid=2|20.

[19] Stefanov, A., Chen-Ching L., "Cyber-power system security in a smart grid environment," Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES , vol., no., pp.1-3, 16-20 Jan. 2012.

[20] Amin, S., Wollenberg B., “Toward a smart grid: power delivery for the 21st century,” IEEE Power and Energy Mag., vol.3, no.5, pp. 34-41, Sept.-Oct. 2005.

[21] Liu, J., Xiao, Y., Gao, J., “Achieving Accountability in Smart Grids,” IEEE Systems Journal, Vol. 8, No. 2, Jun. 2014, pp. 493-508.

[22] Xiao, Z., Xiao, Y., Du, D., "Non-repudiation in Neighborhood Area Networks for Smart Grid," IEEE Communications Magazine, Vol. 51, No. 1, pp. 18-26, Jan. 2013.

[23] Xiao, Z., Xiao, Y., Du, D., "Exploring Malicious Meter Inspection in Neighborhood Area Smart Grids," IEEE Transactions on Smart Grid, Vol. 4, No. 1, Mar. 2013, pp. 214-226.

[24] Harkin, S. (2011, Autumn) "Home energy management in Europe, lots of solutions, but what's the problem", Delta Energy & Environment, [Online]. Available: UK http://www.delta-ee.com/downloads/2011/Delta_Research_Paper_Home_Energy_Mana

[25] Stern, P., Aronson, E., “Energy Use The Human Dimension”, W.H. Freeman and Company, New York, 1984.

[26] Filippi, A., Pandharipande, A., Lelkens, A., Rietman, R., Schenk, T. Wang, Y., Shrubsole, P., "Multi-appliance power disaggregation: An approach to energy monitoring," Energy Conference and Exhibition (EnergyCon), 2010 IEEE International , vol., no., pp.91,95, 18-22 Dec. 2010

[27] My Energy Solutions (2012, Mar.), "Energy efficiency is doing more with less energy", Manhattan Beach, CA [Online]. Available: http://www.myenergysolution.com/home-energy-basics/energy efficiency.html

[28] Squicciarini, C., Lee, W., Bertino, E., Song, C., "A Policy-Based Accountability Tool for Grid Computing Systems," Asia-Pacific Services Computing Conference, 2008. APSCC '08. IEEE, vol., no., pp.95,100, 9-12 Dec. 2008.

[29] World Energy Council (2011, Dec.). Energy Efficiency Policies around the World: Review and Evaluation. [Online]. Available: http://www. worldenergy.org

[30] My Energy Solutions (2012, Mar.), "Energy efficiency is doing more with less energy", Manhattan Beach, CA [Online]. Available: http://www.myenergysolution.com/home-energy-basics/energy efficiency.html

[31] Stern, P., Aronson, E., "Energy Use The Human Dimension", W.H. Freeman and Company, New York, 1984.

[32] Harkin, S., (2011, Autumn) "Home energy management in Europe, lots of solutions, but what's the problem", Delta Energy & Environment, [Online]. Available: UK http://www.delta-ee.com/downloads/2011/Delta_Research_Paper_Home_Energy_Mana

[33] Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D.; "A Survey on Cyber Security for Smart Grid Communications," Communications Surveys & Tutorials, IEEE , vol.PP, no.99, pp.1-13, 0.

[34] Li, X., Liang, X., Lu R., Shen, X., Lin, X., Zhu, H., "Securing smart grid: cyber attacks, countermeasures, and challenges," Communications Magazine, IEEE , vol.50, no.8, pp.38-45, August 2012.

[35] National Communications System, "Supervisory control and data acquisition (SCADA) systems," Technical Report, Oct. 2004, available at: http://www.ncs.gov/library/tech bulletins/2004/tib 04-1.pdf

[36] Dan, G., Sandberg, H., "Stealth Attacks and Protection Schemes for State Estimators in Power Systems," Proceedings of the IEEE SmartGridComm , Oct. 2010.

[37] Biba, K., "Integrity considerations for secure computer systems," Technical report, MITRE Corp., Apr, 1977.

[38] Zheng, Y., Leiwo, J., "A Method to Implement a Denial of Service Protection Base". In Information Security and Privacy, volume 1270 of LNCS, pages 90{101, 1997.

[39] Zheng, Y. L., Leiwo, J., “A Method to Implement a Denial of Service Protection Base”. In Information Security and Privacy, volume 1270 of LNCS, pages 90{101, 1997.

[40] Danezis, G., Clayton, R., “Introducing traffic analysis”. In Digital Privacy: Theory, Technologies, and Practices, Chapter 5. Auerbach Publications, 2008.

[41] Filippi, A., Pandharipande, A., Lelkens, A., Rietman, R., Schenk, T., Ying Wang; Shrubsole, P., "Multi-appliance power disaggregation: An approach to energy monitoring," Energy Conference and Exhibition (EnergyCon), 2010 IEEE International , vol., no., pp.91,95, 18-22 Dec. 2010

[42] Kolter, J., Johnson, M., “Redd: A public data set for energy disaggregation research,” in Workshop on Data Mining Applications in Sustainability (SIGKDD), San Diego, CA, 2011.

[43] Zeifman, M., Roth, M., “Nonintrusive appliance load monitoring: Review and outlook,” IEEE Transactions on Consumer Electronics,, vol. 57, no. 1, pp. 76 –84, February 2011.

[44] Ajay-D-Vimal Raj, R., Sudhakaran1 M., Philomen-D-Anand Raj, P., " Estimation of Standby Power Consumption for Typical Appliances"Journal of Engineering Science and Technology, Review 2 (1) (2009) 71-75

[45] Ridi, C. Gisler and J. Hennebert "Unseen appliances identification". Proceedings of the 18th Iberoamerican Congress on Pattern Recognition (CIARP 2013), Havana, Cuba, 2013.

[46] McLaughlin, S., Podkuiko, D., McDaniel, P., “Energy theft in the advanced metering infrastructure,” Critical Information Infrastructures Security, Lecture Notes in Computer Science 2010, vol. 6027/2010, pp. 176–187, 10.1007/978-3-642-14379-3_15.

[47] Liu; J., Xiao, Y., Gao, J., "Accountability in smart grids," Proc. Of IEEE Consumer Communications and Networking Conference (CCNC), 2011,, pp.1166-1170, 9-12 Jan. 2011

[48] Kalogridis, G., Denic, S., Lewis, T., Cepeda, R., "Privacy protection system and metrics for hiding electrical events," International Journal of Security and Networks, Vol. 6, No.1, pp. 14 - 27, 2011.

[49] Wang J., Rong, L., “Cascade-based attack vulnerability on the us power grid,” Safety Sci., vol. 47, no. 10, pp. 1332–1336, Dec. 2009.

[50] IEC TC57, “Power system control & associated communications - data & communication security,” IEC 62351 Part 1 to 8, Technical Specification and Draft, 2010.

[51] Amin M.; (EPRI) Security Challenges for the electricity infrastructure. IEEE Computer (Security and Privacy Supplement) Volume 24, Number 4, pp 8-10. April 2002.

[52] Li, F., Luo, B., Liu, P., "Secure and privacy-preserving information aggregation for smart grids," International Journal of Security and Networks, Vol. 6, No.1, pp. 28 - 39 , 2011.

[53] Zhang, J., Gunter, C., "Application-aware secure multicast for power grid communications," International Journal of Security and Networks, Vol. 6, No.1, pp. 40 - 52 , 2011.

[54] Association of Home Appliance Manufacturers. "Assessment of Communications Standards for Smart Appliances". [Online] Available: http://www.aham.org/ht/a/GetDocumentAction/i/50696.

[55] Benoit J.; "An Introduction to Cryptography as Applied to the Smart Grid" Cooper Power Systems.

[56] The National Energy Technology Laboratory for the U.S. Department of Energy. "Advanced Metering Infrastructure". February 2008.

[57] Kanabar, M., Voloh, I., McGinn, D., "Reviewing smart grid standards for protection, control, and monitoring applications," Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES , vol., no., pp.1-8, 16-20 Jan. 2012.

[58] Giani, A., Bitar, E., Garcia, M., McQueen, M., Khargonekar, P., Poolla, K., , "Smart grid data integrity attacks: characterizations and countermeasuresπ," Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on , vol., no., pp.232-237, 17-20 Oct. 2011.

[59] Biba, K., "Integrity considerations for secure computer systems," Technical report, MITRE Corp., Apr, 1977.

[60] Zheng, Y., Leiwo, J., "A Method to Implement a Denial of Service Protection Base". In Information Security and Privacy, volume 1270 of LNCS, pages 90{101, 1997.

[61] Meliopoulos, S., Cokkinides, G., Huang, R., Farantatos, E., Sungyun, C.; Yonghee, L., Xuebei, Y., "Smart Grid Infrastructure for Distribution Systems and Applications," System Sciences (HICSS), 2011 44th Hawaii International Conference on , vol., no., pp.1-11, 4-7 Jan. 2011.

[62] ABB Inc. Security in the Smart Grid. ABB White Paper.Available: http://www02.abb.com/db/db0003/db002`8.nsf/0/832c29e54746dd0fc12576400024ef16/$file/paper_Security+in+the+Smart+Grid+%28Sept+09%29_docnum.pdf

[63] Association of Home Appliance Manufacturers. "Assessment of Communications Standards for Smart Appliances". [Online] Available: http://www.aham.org/ht/a/GetDocumentAction/i/50696.

[64] Schwars, K.; "NIST recommends IEC 61850 and other IEC TC 57 Standards for Regulation" [Online] Available: http://blog.iec61850.com/2010/10/nist-recommends-iec-61850-and-other-iec.html.

[65] Wei, D.; Lu, Y.; Jafari, M.; “On protecting industrial automation and control systems against electronic attacks,” in Proc. IEEE Int. Conf. Autom. Sci. Eng., Sep. 2007, pp. 176–181.

[66] Xiao, Z., Fu, B., Xiao, Y., Chen, C., Liang, W., "A Review of GENI Authentication and Access Control Mechanisms," International Journal of Security and Networks (IJSN), Vol. 8, No. 1, 2013, pp. 40-60.

[67] Liu, J., Xiao, Y., Chen, C., "Internet of Things' Authentication and Access Control," International Journal of Security and Networks (IJSN), Vol. 7, No. 4, 2012, pp. 228-241. DOI: 10.1504/IJSN.2012.053461

[68] Liu, J., Xiao, Y., Chen, C., "Authentication and Access Control in the Internet of Things," the proceedings of the 2012 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW 2012), pp. 588-592.

[69] Cheung, H., Hamlyn, A., Mander, T., Cungang Yang; Cheung, R., , "Strategy and Role-based Model of Security Access Control for Smart Grids Computer Networks," Electrical Power Conference, 2007. EPC 2007. IEEE Canada , vol., no., pp.423-428, 25-26 Oct. 2007

[70] Seshadri, A., Luk, M., Shi, E., Perrig, A., van Doorn L., Khosla, P., “Pioneer: Verifying integrity and guaranteeing execution of code on legacy platforms,” In ACM Symposium on Operating Systems Principles, pp. 1-15, Oct. 2005.

[71] Cheung, H., Hamlyn, A., Mander, T., Cungang Yang; Cheung, R., , "Role-based model security access control for smart power-grids computer networks," Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE , vol., no., pp.1-7, 20-24 July 2008

[72] Chen, X., Sung Kim, H.; “RBAC for Home Area Network based Smart Grid” Journal of the Korea Institute of Information Technology Convergence, Vol. 3, No. 2, pp. 95-101, 2010.

[73] Xiao, Y., Rayi, V., Sun, B., Du, X., Hu, F., Galloway, M., “A Survey of Key Management Schemes in Wireless Sensor Networks," Computer communications Journal, Vol. 30 No. 11-12, Sep. 2007. pp. 2314–2341.

[74] Zetter, K., “SCADA System’s Hard-Coded Password Circulated Online for Years”. [Online] Available: http://www.wired.com/threatlevel/2010/07/siemens-scada/.

[75] P. Rus., “SCADA vulnerabilities now with hardcoded backdoors” [Online] Available: http://www.serverbeheersupport.nl/2012/04/scada-vulnerabilities-now-with-hardcoded-backdoors/.

[76] Metke, A., Ekl, A., “Security Technology for Smart Grid Networks,” IEEE Transactionson Smart Grid, vol. 1, 2010.

[77] Smith, S.W.; "Cryptographic scalability challenges in the smart grid (extended abstract)," Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES , vol., no., pp.1-3, 16-20 Jan. 2012.

[78] Nabeel, M., Zage, J., Kerr, S., Bertino, E., Kulatunga, N., "Cryptographic Key Management for Smart Power Grids 2012-1"

[79] Nagaratna, M., Prasad, V.K., Kumar, S.T., "Detecting and Preventing IP-spoofed DDoS Attacks by Encrypted Marking Based Detection and Filtering (EMDAF)," Advances in Recent Technologies in Communication and Computing, 2009. ARTCom '09. International Conference on, vol., no., pp.753-755, 27-28 Oct. 2009.

[80] Jiang, M., Hu, M., Zhou, J., Peng T., "Design and Implementation of IP-SAN Based on Third Party Transfer Protocols," Computing, Communication, Control, and Management, 2008. CCCM '08. ISECS International Colloquium on , vol.1, no., pp.188-192, 3-4 Aug. 2008.

[81] Ernest Young. "Attacking the Smart Grid" Available: http://www.ey.com/Publication/vwLUAssets/Attacking_the_smart_grid/$FILE/Attacking-the-smart-grid_AU1058.pdf. December 2011.

[82] Katzir, L., Schwartzman, I., "Secure firmware updates for smart grid Devices," Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on , vol., no., pp.1-5, 5-7 Dec. 2011

[83] Divan, D., Johal, H., "A Smarter Grid for Improving System Reliability and Asset Utilization," Power Electronics and Motion Control Conference, August, 2006.

[84] Brown, R.E., "Impact of Smart Grid on distribution system design," Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE , vol., no., pp.1-4, 20-24 July 2008.

[85] Mirkovic, H., Reiher, P., "A taxonomy of DDoS attack and DDoS defense mechanisms," SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39C53, 2004.

[86] Van Vliet, M., Yearsley, J., Ludwig, F., Vögele, S., Lettenmaier, D., Kabat, P., "Vulnerability of US and European electricity supply to climate change". Nature Climate Change , (2012).

[87] The Open Web Application Security Project [Online]. Available: https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet.

[88] Halfond, W., Vegas, J., Orso, A., "A Classification of SQL Injection Attacks and Countermeasures", in Proc. Of the Intl. Symposium on Secure Software Engineering, Mar 2006.

[89] "Cross-Site Request Forgery (CSRF)". OWASP, The Open Web Application Security Project. 4 September, 2012.

[90] Chasko, S., LaPorte, T.J., “Smart Grid Security: Preparing for the Standards-Based Future” [Online]. Available: http://www.befutureready.com/security/Landis-and-Gyr-Smart-Grid-Security.pdf.

[91] Chou, N., Ledesma, R., Teraguchi, Y., Boneh, D., Mitchell. J., “Clientside defense against web-based identity theft”. In Proc. 11th Annual Network and Distributed System Security Symposium (NDSS ’04), February 2004.

[92] Energy Transmission in the United State. [Online} Available: teeic.anl.gov/er/transmission/restech/dist/index.cfm.

[93] Shiflett, C., "Security Corner: Cross-Site Request Forgeries". php|architect (via shiflett.org). (December 13, 2004).

[94] Schuba, C., Krsul, I. V., Kuhn, M. G., Spafford, E. H., Sundaram, A., Zamboni, D., “Analysis of a denial of service attack on tcp,” in Proc.

[95] Yaar, A., Perrig, A., Song, D., “Pi: A path identification mechanism to defend against DDoS attacks,” in Proc. IEEE Symposium on Security.

[96] Mirkovic J., Reiher, P., “A taxonomy of DDoS attack and DDoS defense mechanisms,” SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39C53, 2004.

[97] Sun, B., Yu, F., Wu, K., Xiao, Y., Leung, V., "Enhancing Security using Mobility-Based Anomaly Detection in Cellular Mobile Networks," IEEE Transactions on Vehicular Technology, Vol. 55, No. 4, July 2006, pp.1385-1396.

[98] Sun, B., Xiao, Y., Wang, R., "Detection of Fraudulent Usage in Wireless Networks," IEEE Transactions on Vehicular Technology, Vol. 56, No.6, Nov. 2007, pp. 3912 – 3923

[99] Godefroid, P., Levin, M., Molnar, D., “SAGE: Whitebox Fuzzing for Security Testing”. Queue, v.10 n.1, January 2012.

[100] Xiao, Y., Li, C., Lei, M., Vrbsky, S., "Differentiated Virtual Passwords, Secret Little Functions, and Codebooks for Protecting Users from Password Theft," IEEE Systems Journal, Vol. 8, No. 2, Jun. 2014, pp. 406-416.

[101] Lei, M., Xiao, Y., Vrbsky, S., Li, C., “Virtual Password Using Random Linear Functions for On-line Services, ATMs, and Pervasive Computing," Computer Communications Journal, Elsevier, Vol. 31, No. 18, Dec. 2008, pp. 4367-4375.

[102] Godefroid, P.; Levin, M.; Molnar, D.; “SAGE: Whitebox Fuzzing for Security Testing”. Queue, v.10 n.1, January 2012.

[103] European Network and Security Information Agency. “Smart Grid Security”. [Online] Available: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/ENISA_Annex%20II%20-%20Security%20Aspects%20of%20Smart%20Grid.pdf

[104] C4 Security.; “The Dark Side of Smart Grid – Smart Meters (in) Security” available: www.c4-security.com/The Dark Side of the Smart Grid - Smart Meters (in)Security.pdf.

[105] Spett, K., SPI Dynamice “Are your web applications vulnerable”. 2005. Available: http:// http://www.gwtis.com/whitepapers/sqlinjectionwp.pdf

[106] Bhattarai, S., Ge, L., Yu, W., “A Novel Architecture against False Data Injection Attacks in Smart Grid”, Proceeding of IEEE ICC 2012 – Communication and Information Systems Security Symposium, June 2012.

[107] Ray, P., Harnoor, R., Hentea, M., "Smart power grid security: A unified risk management approach," Security Technology (ICCST), 2010 IEEE International Carnahan Conference on , vol., no., pp.276-285, 5-8 Oct. 2010.

[108] Cisco Systems Inc. “Security for the Smart Grid”, Whitepaper 2009. Available: https://www.cisco.com/web/strategy/docs/energy/white_paper_c11_539161.pdf

[109] Hongkai, L.; Chenghong, X.; Jinghui, S.; Yuexi, Y.; "Green power generation technology for distributed power supply," Electricity Distribution, 2008. CICED 2008. China International Conference on , vol., no., pp.1-4, 10-13 Dec. 2008

[110] Liu, J., Xiao, Y., Ghaboosi, K., Deng, H., Zhang, J., "Botnet: Classification, Attacks, Detection, Tracing, and Preventive Measures," EURASIP Journal on Wireless Communications and Networking, Volume 2009, Article ID 692654, 11 pages, doi:10.1155/2009/692654

[111] Leiwo, J., Nikander, P., Aura. T., “Towards network denial of service resistant protocols”. In Proceedings of the 15th International Information Security Conference, August 2000.

[112] Malan, G. R., Watson, D., Jahanian, F.; Howell. P.; “Transport and Application Protocol Scrubbing:. In Proceedings of INFOCOM 2000, pages 1381{1390, 2000.

[113] Smith P., et al., “Network Resilience: A Systematic Approach,” IEEE Commun. Mag., vol. 49, no. 7, July 2011, pp. 88–97

[114] Leon, G., “Smart Planning for Smart Grid AMI Mesh Networks”. EDX Wireless, LLC. Available: http://www.edx.com/resources/documents/EDX_WP_Smart_Grid_AMI_Mesh_Networks_May_11.pdf

[115] AlMajali. A., Viswanathan, A., Neuman. C., “Analyzing Resiliency of the Smart Grid Communication Architectures under Cyber Attack”. USC/Information Sciences Institute.

[116] Rietta, F., “Application layer intrusion detection for SQL injection”. In: 44th annual Southeast regional conference, ACM, New York, USA, pp.531-536, 2006.

[117] Wei, D., Lu, Y., Jafari, M., Skare, P., Rohde, K., "Protecting Smart Grid Automation Systems Against Cyberattacks," Smart Grid, IEEE Transactions on, vol.2, no.4, pp.782-795, Dec. 2011.

[118] Cherry, S., Constantine, L., "Sons of Stuxnet". IEEE Spectrum. (14 December 2011).

[119] Markoff, J., "Malware Aimed at Iran Hit Five Sites, Report Says" . New York Times. p. 15. (11 February 2011).

[120] Krebs, B., "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent" [Online].Available: http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/

[121] http://www.networkworld.com/article/2217684/data-center/attacks-on-power-systems--hackers--malware.html

[122] Poulson, K.; "Slammer worm crashed Ohio nuke plant network." SecurityFocus. Aug 19, 2003. (accessed Nov 27, 2009).

[123] Hebert, J.; Associated Press. "DOE Computers Hacked; Info on 1,500 Taken" [Online] Available: http://www.democraticunderground.com/discuss/duboard.php?az=view_all&address=132x2673379

[124] Krebs. B.; Cyber Incident Blamed for Nuclear Power Plant Shutdown [Online]. Available: http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html. (2008, Jun.)

[125] McAfee Foundstone Professional Services and McAfee Labs "Global Energy Cyberattacks: "Night Dragon". 10 February 2010

[126] Perera. D., Fierce Homeland Security, "MIT: Cyber attack on electric grid 'almost certain'" December 2011 [Online] Available: http://www.fiercehomelandsecurity.com/story/mit-cyber-attack-electric-grid-almost-certain/2011-12-05.

[127] Kai, X., "The Vision of Future Smart Grid," Electric Power, vol. 41, no. 6, 2008, pp. 19–22.

[128] Rahman, M., Bera, P., Al-Shaer, E., "SmartAnalyzer: A noninvasive security threat analyzer for AMI smart grid," Proc. Of IEEE INFOCOM, 2012 pp.2255-2263, 25-30 March 2012

[129] Lu, Z., Lu, X., Wang, W., Wang, C., "Review and evaluation of security threats on the communication networks in the smart grid," Prof. of MILCOM 2010,pp.1830-1835, Oct. 31 2010-Nov. 3 2010

[130] Neuman , C., Tan, K., "Mediating cyber and physical threat propagation in secure smart grid architectures," Proc. of 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp.238-243, 17-20 Oct. 2011

[131] Lu, Z., Lu, X., Wang, W., Wang, C., "Review and evaluation of security threats on the communication networks in the smart grid," Prof. of MILCOM 2010,pp.1830-1835, Oct. 31 2010-Nov. 3 2010

[132] Gungor, V., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., Hancke, G.P., "Smart Grid and Smart Homes: Key Players and Pilot Projects," IEEE Industrial Electronics Magazine, Vol.6, No.4, pp.18-34, Dec. 2012

[133] Kok, K., Karnouskos, S., Ringelstein, J., Dimeas, A., Weidlich, A., Warmer, C., Drenkard, S., Hatziargyriou, N., Lioliou, V., "Fieldtesting smart houses for a smart grid," in Proc. 21st Int. Conf. Electricity Distribution (CIRED), Frankfurt, June 2011, pp. 1–4.

[134] Citron, D. K., & Pasquale, F. (2010). Network Accountability for the Domestic Intelligence Apparatus. Hastings LJ, 62, 1441.

[135] Kelso, J., "2009 Buildings Energy Data Book," D&R International, Ltd., Silver Spring, Maryland October 2009.

[136] Du, Y., Du, L., Lu, B., Harley, R., Habetler, T., "A review of identification and monitoring methods for electric loads in commercial and residential buildings," Energy Conversion Congress and Exposition (ECCE), 2010 IEEE , vol., no., pp.4527,4533, 12-16 Sept. 2010

[137] E. McCary and Y. Xiao, (2014) "Smart Grid HAN Accountability with Varying Consumption Devices," Proceedings of The 2014 International Conference on Security Management (SAM '14)

[138] Xiao, Y., "Accountability for wireless LANs, ad hoc networks, and wireless mesh networks," Communications Magazine, IEEE , vol.46, no.4, pp.116,126, April 2008

[139] Cederquist, J., "An Audit Logic for Accountability," Proc. 6th IEEE Int'l. Wksp. Policies for Distrib. Sys. and Networks, pp. 34–43.

[140] Du, D., Hwang, F., "Combinatorial Group Testing and its Applications," Singapore: World Scientific, 1993.

[141] Dorfman, R. "The detection of defective members of large populations," Ann. Math. Statist., vol. 14, pp. 436–440, 1943.

[142] Parker, N., "How Many Net Connected Devices are in Your Home". [Online] Available: http://www.nbnco.com.au/blog/how-many-net-connected-gadgets-in-your-home.html

[143] Stathopoulos, T., J. Heidemann, and D. Estrin. A remote code update mechanism for wireless sensor networks. Technical report, UCLA, Los Angeles, CA, USA, 2003

[144] Xiao, J., Li, J., Boutaba, R., Hong, J.W.-K., "Comfort-aware home energy management under market-based Demand-Response," Network and service management (cnsm), 2012 8th international conference and 2012 workshop on systems virtualiztion management (svm) , vol., no., pp.10,18, 22-26 Oct. 2012

[145] Cisco Systems Inc., "Internet protocol architecture for smart grid" White Paper, Jul 2009. [Online]. Available: http://www.cisco.com/web/strategy/docs/energy/CISCO_IP_INTEROP_STDS_PPR_TO_NIST_WP.pdf

[146] Fouda, M.M.; Fadlullah, Z.M.; Kato, N.; Takeuchi, A.; Nozaki, Y., "A novel demand control policy for improving quality of power usage in smart grid," Global Communications Conference (GLOBECOM), 2012 IEEE , vol., no., pp.5154,5159, 3-7 Dec. 2012

[147] Bu Shengrong, F. R. Yu, and P. X. Liu, "Dynamic Pricing for Demandside Management in the Smart Grid," IEEE Online Conference on Green Communications (GreenCom'11), Sep. 2011. U.S. NETL, "Advanced Metering Infrastructure," White Paper, Feb. 2008. [Online]. Available: http://www.smartgrid.gov/standards/roadmap

[148] Xiao, Y., "Flow-Net Methodology for Accountability in Wireless Networks," IEEE Network, Vol. 23, No. 5, Sept./Oct. 2009, pp. 30-37.

[149] World Energy Council (2011, Dec.). Energy Efficiency Policies around the World: Review and Evaluation. [Online]. Available: http://www. worldenergy.org

[150] My Energy Solutions (2012, Mar.), "Energy efficiency is doing more with less energy", Manhattan Beach, CA [Online]. Available: http://www.myenergysolution.com/home-energy-basics/energy efficiency.html

[151] Ramanathan, R., Engle, R. F., Granger, C., Vahid-Araghi, F., Brace, C., "Short-run forecasts of electricity loads and peaks," Int. J. Forecast., vol. 13, pp. 161–174, 1997.

[152] Dae-Man H., Jae-Hyun L., "Design and implementation of smart home energy management systems based on Zigbee," Consumer Electronics, IEEE Transactions on , vol.56, no.3, pp.1417,1425, Aug. 2010

[153] Clements, S., Carroll T., Hadley, M. "Home Area Networks and the Smart Grid". No. PNNL-20374. Pacific Northwest National Laboratory (PNNL), Richland, WA (US), 2011

[154] Froehlich, J., Larson, E., Gupta, S., Cohn, G., Reynolds, M. S., Patel, S. N., "Disaggregated End-Use Energy Sensing for the Smart Grid," IEEE Pervasive Computing, vol. 10, no. 1, pp. 28-39, 2011.

[155] Fay, D., Ringwood, J. V., Condon, M., Kelly, M., "24-h electrical load data—A sequential or partitioned time series?,"Neurocomputing, vol. 55, no. 3-4, pp. 469–498, 2003.

[156] Shu F., Hyndman, R.J., "Short-Term Load Forecasting Based on a Semi-Parametric Additive Model," Power Systems, IEEE Transactions on , vol.27, no.1, pp.134,141, Feb. 2012

[157] Matthews, H. S., Soibelman, L., Berges, M., Goldman, E., "Automatically Disaggregating the Total Electrical Load in Residential Buildings: a Profile of the Required Solution," Intelligent Computing in Engineering - ICE08, 2008

[158] Eckmann, J.P., S.O. Kampshort, and D. Ruelle (1987): Recurrence Plots of Dynamical Systems. Europhysics Letters, 4: 973-977

[159] Takens, F. (1981): Detecting Strange Attractors in Turbulence. In Dynamical Systems and Turbulence. Rand, D., L. Young (eds). Berlin: Spriner

[160] Popescu, F., Enache, F., Vizitiu, I., "Recurrence Plot Analysis for Characterization of Appliance Load Signature" COMM 2014 International Conference on Communications, 2014

[161] Davison, A. & Smith, R. (1990). Models for exceedances over high thresholds (with discussion). J. R. Stat. Soc. Ser. B Stat. Methodol., 52, 393–442

[162] Beirlant, J., P. Vynckier, and J. L. Teugels (1996). Tail index estimation, Pareto quantile plots and regression diagnostics. Journal of the American Statistical Association 91, 1659{1667.

[163] Dupuis, D. J. (1998). Exceedances over high thresholds: a guide to threshold selection. Extremes 1, 251{261.

[164] Drees, H., L. de Haan, and S. I. Resnick (2000). How to make a Hill plot. Annals of Statistics 28, 254{274.

[165] Coles, S. G. (2001). An Introduction to Statistical Modeling of Extreme Values. Springer.

[166] Choulakian, V. and M. A. Stephens (2001). Goodness-of-t tests for the generalized Pareto distribution. Technometrics 43, 478{484.

[167] Lee, J., Y. Fan, and S. A. Sisson. "Bayesian threshold selection for extremal models using measures of surprise." arXiv preprint arXiv:1311.2994 (2013).

[168] Danielsson, J., L. de Haan, L. Peng, and C. G. de Vries (2001). Using a bootstrap method to choose the sample fraction in tail index estimation. Journal of Multivari- ate Analysis 76, 226{248.

[169] Ferreira, A., L. de Haan, and L. Peng (2003). On optimising the estimation of high quantiles of a probability distribution. Statistics 37, 401{434.

[170] Drees, H. and E. Kaufmann (1998). Selecting the optimal sample fraction in univariate extreme value estimation. Stoch. Proc. Appl. 75, 149{172.

[171] Mindlin, G., Gilmore. R., 1992. Topological analysis and synthesis of chaotic time series. Phys. D 58, 1-4 (September 1992), 229-242.

[172] Koorse, S.J., "False positives, detection limits, and other laboratory imperfections: The regulatory implications", En- vironmental Law Reporter, 19 (1989) 10211-10222.

[173] American National Standard Dictionary for Technologies of Electromagnetic Compatibility (EMC), Electromagnetic Pulse (EMP) and Electrostatic Discharge (ESD) (Dictionary of EMC/EMP/ESD Terms and Definitions)," ANSI C63.14-1998 , vol., no., pp.1,44, Dec. 3 1998

[174] Audio-Technica U.S. Inc. 2014. Types of Interference. [Online] Available: http://www.audio-technica.com/cms/site/6d4b2edb868000db/

[175] Burrel J., "Disruptive Effects of Electromagnetic Interference on Communication and Electronic Systems". MSc Telecommunications Research project, George Mason University (April 2003), 3 4pp.

[176] Schwartz, T., Stevens, G., Ramirez, L., Wulf. V., "Uncovering practices of making energy consumption accountable: A phenomenological inquiry". TOCHI 2013, 20(2), article 9. (2013).

[177] Guo, Y. Jones, M. Cowan, B. Beale, R. 2013. "Take it personally: personal accountability and energy consumption in domestic households". In CHI '13 Extended Abstracts on Human Factors in Computing Systems (CHI EA '13). ACM, New York, NY, USA

[178] Haeberlen A., Kouznetsov, P., and P. Druschel, "PeerReview: Practical accountability for distributed systems," Proc. of ACM SIGOPS 2007.

[179] Xiao, Zhifeng; Xiao, Yang. "P-Accountable Networked Systems," INFOCOM IEEE Conference on Computer Communications Workshops , 2010 , vol., no., pp.1,5, 15-19 March 2010

[180] Po-An Chou; Ray-I Chang, "Unsupervised Adaptive Non-intrusive Load Monitoring System," Systems, Man, and Cybernetics (SMC), 2013 IEEE International Conference on vol., no., pp.3180,3185, 13-16 Oct. 2013

[181] Chang, H.; Lian, K.; Su, Y.; Lee, W., "Power-Spectrum-Based Wavelet Transform for Nonintrusive Demand Monitoring and Load Identification," Industry Applications, IEEE Transactions on , vol.50, no.3, pp.2081,2089, May-June 2014

[182] Gisler, C.; Ridi, A.; Zujferey, D.; Khaled, O.A.; Hennebert, J., "Appliance consumption signature database and recognition test protocols," Systems, Signal Processing and their Applications (WoSSPA), 2013 8th International Workshop on , vol., no., pp.336,341, 12-15 May 2013

[183] Kudo M., "Electronic submission protocol based on temporal accountability," in Proceedings of the 14th Annual Computer Security Applications Conference, 1998, pp. 353-363.

[184] Patel, S. N., T. Robertson, J. A. Kientz, M. S. Reynods, and G. Abowd. At the flick of a switch: detecting and classifying unique electrical events on the residential power line. In Proceedings of the Conference on Ubiquitous Computing , 2006.

[185] Srinivasan, D., Ng, W. S., and Liew , A. C . Neural Network Based Signature Recognition for Harmonic Source Identification. IEEE Transactions on Power Delivery, 21(1):398-405, 2006.

[186] Lin, G., Lee, S., Hsu, J., and W. Jih. Applying power meters for appliance recognition on the electric panel. In IEEE Industrial Electronics and Applications, Taichung, Taiwan, 2010.

[187] Marchiori, A., Hakkarinen, D., Han, Q., and Earle, L., "Circuit-Level Load Monitoring for Household Energy Management," IEEE Pervasive Computing, vol. 10, no. 1, 2010

[188] Kim, H., Marwah, M., Arlitt, M., Lyon, G., and Han, J,. Unsupervised disaggregation of low frequency power measurements. In Proceedings of the SIAM Conference on Data Mining, 2011

[189] Kolter, J. Z., and Jaakkola, T. 2012. Approximate Inference in Additive Factorial HMMs with Application to Energy Disaggregation. In International Conference on Artificial Intelligence and Statistics, 1472–1482.

[190] Johnson, M. J., Willsky, A. S. "Bayesian Nonparametric Hidden Semi-Markov Models," Massachusetts Institute of Technology, Tech. Rep. arXiv:1203.1365, 2012

[191] Saitoh, T., Osaki, T., Konishi, R., Sugahara, K., "Current Sensor Based Home Appliance and State of Appliance Recognition," SICE JCMSI, vol. 3, pp. 86-93, Mar. 2010

[192] Hart, W., Non-intrusive appliance load monitoring. Proceedings of the IEEE, 80(12), 1992

[193] Bergés, M., Goldman, E., Matthews, H. S., Soibelman, L., Anderson, K., "User-centric Non-Intrusive Electricity Load Monitoring for Residential Buildings," ASCE Journal of Computing in Civil Engineering

[194] Baranski, M., J. Voss, Non-Intrusive Appliance Load Monitoring Based on an Optical Sensor, EEE Power Tech Conference, Bologna, 2003

[195] Liang, J., Ng, S. K. K., Kendall, G., Cheng, J., Load signature study — part i: Basic concept, structure, and methodology. IEEE Transactions on Power Delivery, 25:551–560, 2010.

[196] Suzuki, K., Inagaki, S., Suzuki T., Nakamura, H., Ito, K., Nonintrusive appliance load monitoring based on integer programming. In Int. Conference on Instrumentation, Control and Information Technology, Tokyo, Japan, 2008.

[197] Zoha, A., Gluhak, A., Imran, M., Rajasegarar, S., Non-intrusive load monitoring approaches for disaggregated energy sensing: A survey. Sensors, 12(12):16838{16866, 2012

[198] Xenakis C., Panos, C., Stavrakakis, I; A Comparative Evaluation of Intrusion Detection Architectures for Mobile Ad Hoc Networks, Computers & Security, Vol. 30, No. 1, 2011, pp. 63-80.