

**MODELING AND DETECTION OF METER  
COMPROMISE ATTACKS AGAINST THE SMART  
GRID COMMUNICATION INFRASTRUCTURE**

BY

**ABDURRAOOF SALIH AL-AMOUDY**

A Thesis Presented to the  
DEANSHIP OF GRADUATE STUDIES

**KING FAHD UNIVERSITY OF PETROLEUM & MINERALS**

DHAHRAN, SAUDI ARABIA

In Partial Fulfillment of the  
Requirements for the Degree of

**MASTER OF SCIENCE**

In

**COMPUTER NETWORKS**

October 2014

KING FAHD UNIVERSITY OF PETROLEUM & MINERALS

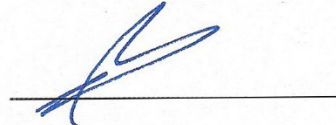
DHAHRAN- 31261, SAUDI ARABIA

DEANSHIP OF GRADUATE STUDIES

This thesis, written by **ABDURRAOOF SALIH AL-AMOUDY** under the direction of his thesis advisor and approved by his thesis committee, has been presented and accepted by the Dean of Graduate Studies, in partial fulfillment of the requirements for the degree of **MASTER OF SCIENCE IN COMPUTER NETWORKS**.



Dr. Ahmad Al Mulhem  
Department Chairman

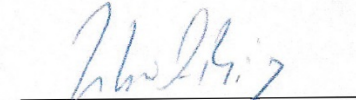


Dr. Salam A. Zummo  
Dean of Graduate Studies

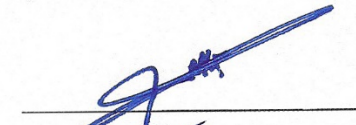
22/11/15  
Date



Dr. Sadiq M. Sait  
(Advisor)



Dr. Zubair Ahmed Baig  
(Member)



Dr. Talal Mousa Al-Kharobi  
(Member)

© Abdurraof Salih Al Amoudy

2014

*For my mother, who offered me ultimate love and support through the course of this  
thesis*

## ACKNOWLEDGMENTS

*To ALLAH, all praises be to You, the most merciful and beneficent, who bestowed me with the knowledge, provided me the courage and endorsed me with the strength to achieve this research work. At the completion of my thesis, I would like to share the credit with a few significant persons who have contributed to making this thesis possible. Firstly, I would like to express my sincerest gratitude to my advisor, Dr. Sadiq, for his all-out support and assistance from the inception until the completion of my thesis work. I thank him for the time and effort he spent to guide me and for sharing his expertise in his scientific research field. In addition to my advisor, I would also like to commend my thesis committee members, namely Dr. Zubair Ahmed Baig and Dr. Talal Mousa Al-Kharobi, for their outstanding suggestions and valuable comments. Secondly, I am grateful to King Fahd University of Petroleum & Minerals for the support given to my research and for providing me with an advanced academic curriculum and a world-class research environment to keep me on track with my studies. Thirdly, I shall be eternally grateful to the Hadhramaut Establishment for Human Development, to whom I am indebted, for providing me the great opportunity to pursue my graduate studies. Fourthly, I greatly appreciate the input of all of my friends, who supported me throughout, in particular, Mr. Saif Ahmad for his exceptional friendship and prompt feedback. Finally, I would like to take this opportunity to express my deepest appreciation to my beloved mother for her unconditional love and unlimited support all throughout my scholastic and career endeavors.*

# TABLE OF CONTENTS

<b>ACKNOWLEDGMENTS</b> .....	<b>V</b>
<b>TABLE OF CONTENTS</b> .....	<b>VI</b>
<b>LIST OF TABLES</b> .....	<b>IX</b>
<b>LIST OF FIGURES</b> .....	<b>X</b>
<b>ABSTRACT</b> .....	<b>XIII</b>
<b>ARABIC ABSTRACT</b> .....	<b>XIV</b>
<b>CHAPTER 1 INTRODUCTION</b> .....	<b>1</b>
<b>1.1 Traditional Grid</b> .....	<b>1</b>
<b>1.1.1 How it works</b> .....	<b>1</b>
<b>1.1.2 The Challenges</b> .....	<b>2</b>
<b>1.2 Smart Grid</b> .....	<b>3</b>
<b>1.3 The NIST Conceptual Model for the Smart Grid</b> .....	<b>5</b>
<b>1.3.1 Bulk Generation Domain</b> .....	<b>6</b>
<b>1.3.2 Distribution Domain</b> .....	<b>7</b>
<b>1.3.3 Customer Domain</b> .....	<b>7</b>
<b>1.3.4 Operation Domain</b> .....	<b>8</b>
<b>1.3.5 Markets Domain</b> .....	<b>9</b>
<b>1.3.6 Service Provider Domain</b> .....	<b>9</b>
<b>1.3.7 Transmission Domain</b> .....	<b>10</b>
<b>1.4 Smart Grid Communication Infrastructure</b> .....	<b>10</b>
<b>1.4.1 Home Area Network (HAN)</b> .....	<b>11</b>

1.4.2 Neighborhood Area Network (NAN).....	12
1.4.3 Wide Area Network (WAN) .....	12
1.5 Smart Grid Protocols.....	13
1.6 Security of Smart Grid .....	14
1.6.1 Smart Grid Attacks .....	15
1.7 Problem Context .....	19
1.8 Research Objectives.....	19
1.9 Research Methodology .....	20
1.10 Research Contribution.....	21
1.11 Thesis Outline.....	21
<b>CHAPTER 2 SMART GRID ATTACKS AND COUNTERMEASURES.....</b>	<b>23</b>
2.1 Requirements for Cyber Security of Smart Grid.....	26
2.2 SCADA Security Concerns .....	32
2.2.1 Platform Vulnerabilities .....	32
2.2.2 Policy Vulnerabilities .....	33
2.2.3 Network Vulnerabilities.....	33
2.3 Smart Meter Attacks and Countermeasures .....	34
2.3.1 Confidentiality.....	35
2.3.2 Integrity.....	36
2.3.3 Availability .....	37
2.3.4 Non-repudiation.....	37
2.4 Physical Layer Attacks and Countermeasures .....	38
2.4.1 Eavesdropping.....	40
2.4.2 Jamming .....	41
2.4.3 Injecting Request or Restrict Access .....	41

2.4.4 Injection Attack .....	42
2.5 Data Injection and Replay Attacks.....	43
2.6 Network-based Attacks.....	45
2.7 Summary.....	46
<b>CHAPTER 3 DETECTING SMART METER COMPROMISE ATTACKS THROUGH NEIGHBORHOOD AREA METER CLUSTERING.....</b>	<b>48</b>
3.1 Background.....	51
3.1.1 Related Work .....	51
3.1.2 AMI Review .....	53
3.1.3 Energy Fraud Attack Tree .....	55
3.1.4 Notations .....	58
3.2 The Attack Model.....	58
3.3 Attack Detection Scheme .....	63
3.3.1 Assumption .....	63
3.3.2 The Scheme .....	65
<b>CHAPTER 4 PERFORMANCE ANALYSIS .....</b>	<b>70</b>
<b>CHAPTER 5 CONCLUSION AND FUTURE WORK .....</b>	<b>84</b>
5.1 Conclusion .....	84
5.2 Future Work.....	85
<b>REFERENCES.....</b>	<b>86</b>
<b>VITAE .....</b>	<b>96</b>



## LIST OF TABLES

Table 1: Main differences between the smart grid and traditional [3].....	4
Table 2: Actors and Applications for Each Domain in the Smart Grid .....	6
Table 3: Smart Grid Communication Protocols.....	13
Table 4: A list of security benchmarks affected by the different Smart Grid attacks, and the location where such attacks take place .....	25
Table 5: Notations of the scheme.....	58

## LIST OF FIGURES

Figure 1: Traditional Power Grid Infrastructure .....	2
Figure 2: The NIST Conceptual Model for the Smart Grid showing interaction between different domains through secure communication and electrical interfaces .....	5
Figure 3: Bulk Generation Domain.....	7
Figure 4: Distribution Domain.....	7
Figure 5: Customer Domain.....	8
Figure 6: Operations Domain.....	8
Figure 7: Markets Domain .....	9
Figure 8: Service Provider Domain .....	10
Figure 9: Smart Grid Communication infrastructure.....	11
Figure 10: DDoS Attack against the DCU [14].....	17
Figure 11: Remote Disconnect Command Attack [14].....	18
Figure 12: The five classes of the attacks that violate the Smart Grid infrastructure .....	24
Figure 13: The three major cyber-security requirements for the Smart Grid .....	26
Figure 14: Attacks with their possible location at smart grid architecture .....	31
Figure 15: Cyber attacks that target the Smart Meter .....	35
Figure 16: Assumed topology for the clustered advanced metering infrastructure (AMI).....	50
Figure 17: Simple building blocks of AMI.....	54

Figure 18: Attack tree for Energy Fraud.....	57
Figure 19: The attack model where the communication topology is centralized .....	60
Figure 20: A compromised smart meter sending correct readings to peer meters and incorrect readings to DCU .....	61
Figure 21: A compromised smart meter relay the same false readings to both its peer meters and the DCU .....	61
Figure 22: Attack Detection Rate for Varying Cluster Size .....	71
Figure 23: False Negative Rate for Varying Cluster Size.....	72
Figure 24: Communication Overhead Imposed by the Detection Scheme.....	73
Figure 25: Attack Detection Rate for Varying Numbers of Compromised Nodes with 4 Different Adversary Classes (N=1000).....	74
Figure 26: False Negative Rate for Varying Numbers of Compromised Nodes with 4 Different Adversary Classes (N=1000).....	75
Figure 27: Attack Detection Rate for Varying Numbers of Nodes in a Cluster and Varying Attacker Ratios.....	76
Figure 28: False Negative Rate for Varying Numbers of Nodes in a Cluster and Varying Attacker Ratios.....	76
Figure 29: Attack Detection Rate for four Packet drop rates and N=100.....	78
Figure 30: The False Rate for four Packet drop rates and N=100 .....	79

Figure 31: Attack Detection Rate for four Packet drop rates and different Cluster Sizes and fixed number of compromised meter ( $r$ ) =45 .....	80
Figure 32: Attack Detection Rate for four Packet drop rates and different Cluster Sizes and fixed number of compromised meter ( $r$ ) =45 .....	81
Figure 33: Attack Detection Rate for fixed Packet drop rate (=25%) and Varying Cluster Sizes with different Attacker ratio .....	82
Figure 34: False Alarm Rate for fixed Packet drop rate (=25%) and Varying Cluster Sizes with different Attacker ratio.....	82

## ABSTRACT

**Full Name** : Abdurraoof Salih Al-Amoudy  
**Thesis Title** : Modeling and Detection of Meter Compromise Attacks Against the Smart Grid Communication Infrastructure  
**Major Field** : Computer Networks  
**Date of Degree** : October 2014

*The increasing demand for power has overwhelmed the current power grid. The Smart Grid uses a new paradigm to provide several distinctive functionalities to the consumers, in order to address the present problem of power demand. This newly developed power grid has an infrastructural design that is fully automated demanding little or no human intervention at all. This can be achieved by integrating the modern communications technologies into the electrical power grid. The information transmission related to billing, power consumption, and other important usage readings is achieved through installation of various sensors in the Smart Grid. However, this integration of technology also brings with it cyber security and privacy challenges. Several security, privacy and reliability issues arise during electric power delivery. The security challenges presented by the Smart Grid are unique and cannot be addressed through existing solutions. In this work, we present a categorization of the attacks that target Smart Grids based on the targeted victim or device, as well as on the type of the attack. We also propose a detection technique for meter compromise attacks against the Smart Grid Communications Infrastructure.*

## ملخص الرسالة

الاسم الكامل: عبد الرؤوف صالح العمودي

عنوان الرسالة: النمذجة والكشف عن الهجمات الإلكترونية التي تتعرض لها العدادات الذكية في شبكات الكهرباء الذكية والحديثة

التخصص: شبكات الحاسوب

تاريخ الدرجة العلمية: محرم 1436 هـ

في وقتنا الحاضر أصبحت شبكات توليد الطاقة الكهربائية التقليدية غير قادرة على تلبية الطلب المتزايد على الطاقة الكهربائية، ولمواكبة هذا الطلب المتزايد تم إنشاء الشبكة الكهربائية الذكية والتي توفر عدة وظائف مميزة للمستهلكين. تعتمد الشبكة الكهربائية الذكية في تصميمها على استخدام أحدث تقنيات الاتصالات الرقمية كالعدادات الذكية وأنظمة المراقبة وغيرها. حيث تمكن هذه الشبكة مؤسسات الكهرباء من جمع معلومات مهمة من أماكن الاستهلاك والتوليد والنقل مثل أنماط استهلاك الكهرباء لدى المستهلك، وأنماط التوليد لمحطات الطاقة وكذلك معلومات مهمة عن أداء الشبكة، وهذا الأسلوب الجديد في إدارة الشبكة ما هو إلا أتمته لعملية تحسين كفاءة ووثوقية وديمومة توليد ونقل الكهرباء. مع كل الميزات التي تتمتع بها الشبكة الذكية إلا أنها تواجه الكثير من التحديات والصعوبات، فقد أدى دمج التقنية الحديثة في الشبكة لظهور العديد من الهجمات الإلكترونية لانتهاك أمن الشبكة، فهناك العديد من القضايا الأمنية وقضايا الخصوصية والموثوقية التي قد تظهر أثناء توصيل الكهرباء. في هذا البحث ركزنا على أحد أنواع هذه الهجمات، والذي يستهدف العدادات الذكية بهدف التلاعب بقراءة العداد أما بزيادة أو نقصان الاستهلاك الكهربائي، لقد قمنا أولاً بتصنيف الهجمات الإلكترونية التي تستهدف الشبكة الذكية بناءً على الخدمة المستهدفة أو الجهاز أو نوع الهجوم. كما قمنا في هذه الدراسة باقتراح تقنية للكشف عن الهجمات التي تتعرض لها العدادات الذكية.

# CHAPTER 1

## INTRODUCTION

### 1.1 Traditional Grid

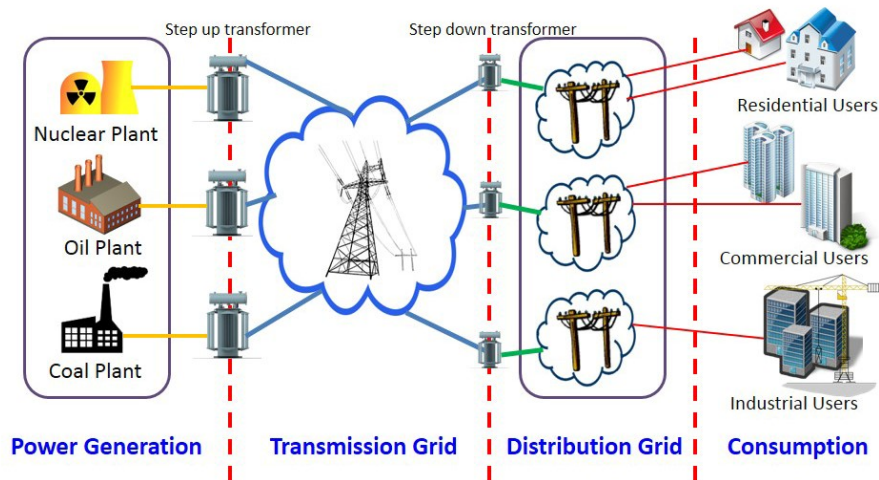
The traditional power grid is the infrastructure that carries electricity from power plants (coal plants, hydroelectric dams, etc.) to a large number of users or customers (household, businesses, and industries) where it is consumed. The most apparent components of the traditional grid for many of us are the towering high-voltage transmission lines that crisscross the countryside or the neighborhood substations that distribute power locally [1].

#### 1.1.1 How it works

Basically, the traditional electricity grid was designed to supply consumers with electricity from where it is generated. It uses a centralized model wherein consumers use electricity that comes from fixed plants through an old, unidirectional communication and circulation system.

The traditional electricity grid shown in Fig. 1. Its transmission system uses high voltage cables to transport electricity over long distances while a medium voltage wires and substations are used in its distribution system for distributing the power locally. Step-up transformers are utilized to raise the electricity during the transmission to sub-stations over

long distance; however, pole-top transformers are used to scale down the voltage when the electricity is transmitted to consumers' locations through medium voltage lines [1].



**Figure 1: Traditional Power Grid Infrastructure**

### **1.1.2 The Challenges**

With the advancement of technology, the traditional power grid has failed to consider that the demand for power keeps increasing exponentially. The absence of communication in the current power grid makes the system simply a generator of power without any regard to the electricity required by consumers. Therefore, a bidirectional communication channel must be created between the electricity utility and consumer in order to regulate the amount of electricity supplied and to make sure that the consumers get only the required power. In addition, two-way communication allows electricity providers to attain three main objectives, namely security, intelligent observing, and load balancing [2].



## 1.2 Smart Grid

Smart Electrical Grid, also known as smart grid (SG), intergrid, intelligent grid, intelligrid, intragrid, or future grid has become one of the fastest growing areas in the information technology industry [3]. It was initiated with the idea of advanced metering infrastructure (AMI) to meet the global demand for electricity and to improve energy efficiency, and the construction of reliable self-healing grid protection against natural catastrophes and malicious disruption. With the birth of Smart Grid, new requirements and demands have driven the electricity industries, so research organizations and government agencies are considering to further study and expansion of the initially perceived scope of the Smart Grid. Due to a two-way process of communication, self-monitoring, self-healing, utilization of modern information technologies, and other salient features promised by the Smart Grid, it has gained the interest of many customers as a way of addressing the present problems of the traditional grid to meet increasing power demand.

The term Smart Grid SG as defined by the European Technology Platform Smart Grid ETPSG [4] is “An electricity network that can intelligently integrate the actions of all users connected to it – generators, consumers and those that do both – in order to efficiently deliver sustainable, economic and secure electricity supplies”. By integrating the latest information and advanced digital communication technologies, the smart grid is capable of generating electrical power in ways that are more efficient and of dropping peak energy demand.

Smart Grid can be viewed from two different ways: one is from the energy transmission viewpoint and the second is from the information transmission viewpoint. In the first, the

Smart Grid is viewed as a traditional grid delivering electricity from power plants to consumers. In the second, the smart grid is viewed as a sensor network: as a sensor it integrates important sensing capabilities, which can in effect imitate various wireless sensors network (WSN) features. For example, data collection can be distributed in a large scale networking environment through an accurate and robust sensing infrastructure (e.g., advanced metering infrastructures). According to a study by the National Institute of Standards and Technology (NIST) [3], the expected advantages and features of this modern grid are as follow:

1. Enhancing, power quality and reliability.
2. Improving capacity and efficiency of the existing grid.
3. Improving resilience to disruption.
4. Reducing the dependence on fossil fuels by means of the integration of renewable energy sources.
5. Automating maintenance and operations.

Table 1 shows the main differences between the two grids [3].

**Table 1: Main differences between the smart grid and traditional [3]**

<b>Traditional Grid</b>	<b>Smart Grid</b>
Electromechanical	Digital
One-way communication	Two-way communication
Centralized generation	Distributed generation
Few sensors	Sensors throughout
Manual monitoring	Self-monitoring
Manual restoration	Self-healing

Failures and blackouts	Adaptive and islanding
Limited control	Pervasive control
Few customer choices	Many customer choices

### 1.3 The NIST Conceptual Model for the Smart Grid

Furthermore, to fully understand this new paradigm, the conceptual model (see Fig. 2) provided by NIST can be used as a reference for different parts of the smart grid electrical system. In this model, it is seen that there are seven domains in the smart grid. Each domain is comprised of a number of *actors* and *applications*, as shown in Table 2. The actors are typically devices, systems, or programs that make decisions and exchange information through a range of interfaces in order to accomplish applications and processes. The applications are several tasks performed by an actor or actors within a certain domain [3]. In the following paragraphs, domains and actors are briefly described.

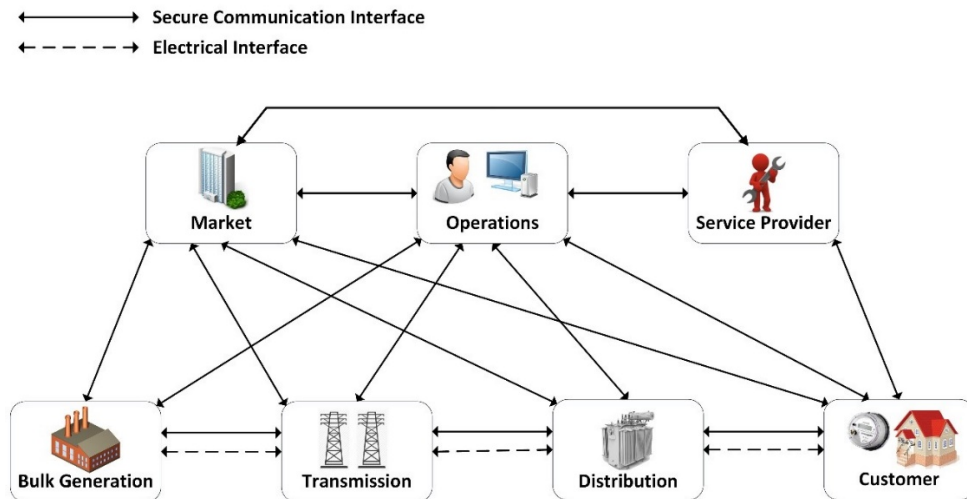


Figure 2: The NIST Conceptual Model for the Smart Grid showing interaction between different domains through secure communication and electrical interfaces

**Table 2: Actors and Applications for Each Domain in the Smart Grid**

<b>DOMAINS</b>	<b>ACTORS</b>	<b>APPLICATIONS</b>
Bulk Generation	Generators of electricity power in huge quantities.	Power generation, asset management, etc.
Transmission	Transmission lines of electricity power over long distances	Monitoring and control systems, stabilize and optimize, etc.
Distribution	Distributors of electricity to and from customers	Substations automation, control, records, assets, management, etc.
Customer	End users of electricity	Building/home automation, solar/wind generation, etc.
Markets	Operators and participants in electricity markets	Market management, retailing, trading, etc.
Operations	Managers of the movement of electricity	Network operations, monitor control, analysis, customer support, etc.
Service Provider	Organizations providing service to electrical customers and utilities	Customer management, installation and maintenance, billing, home management, etc.

### **1.3.1 Bulk Generation Domain**

This domain takes charge of producing huge amounts of electricity by both renewable and non-renewable power sources. There are two kinds of renewable sources: the variable sources which include wind and solar, and the non-variable sources which include biomass, geothermal, hydro and pump storage. On the other hand, the non-renewable energy sources include coal, nuclear, and gas. Stored energy for later distribution may be used in these domains [5]. The resources used by the bulk generation domain are shown in Fig. 3.

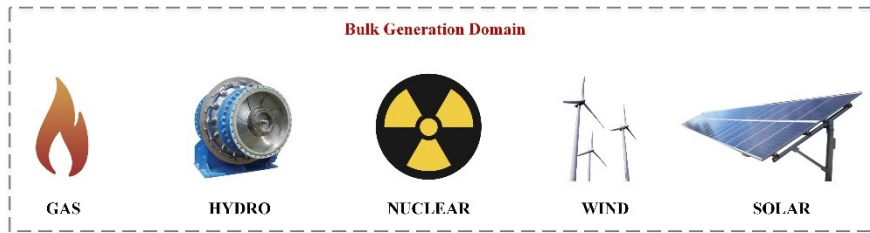


Figure 3: Bulk Generation Domain

### 1.3.2 Distribution Domain

This domain (see Fig. 4) administers several functions. Firstly, it allocates electricity (both sent and received) to the customers. Secondly, it connects all the devices and smart in the grid network. Thirdly, it administers grid’s devices via wireless/wire-line communication. Lastly, it is very possible that the distribution network may be connected to energy storage facilities and alternative distributed energy resources at the distribution level [5].

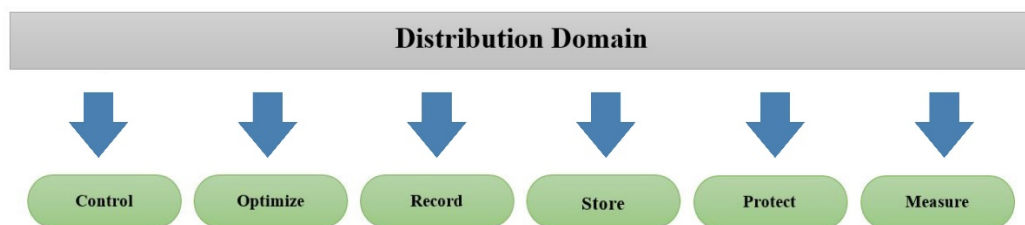
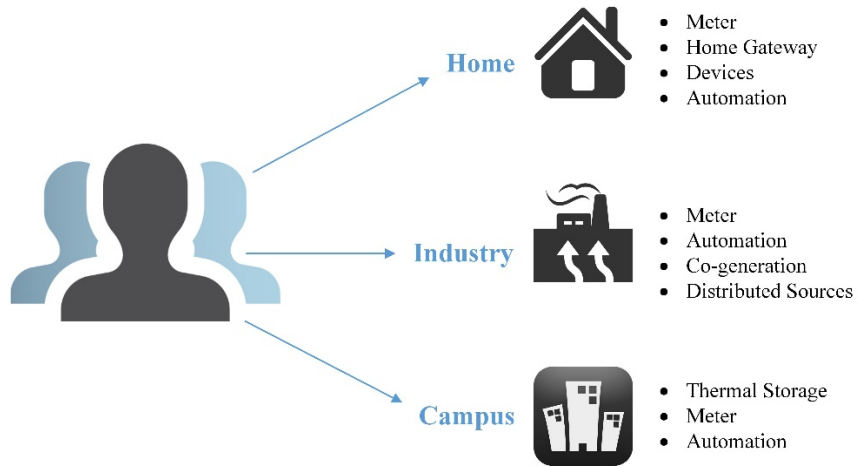


Figure 4: Distribution Domain

### 1.3.3 Customer Domain

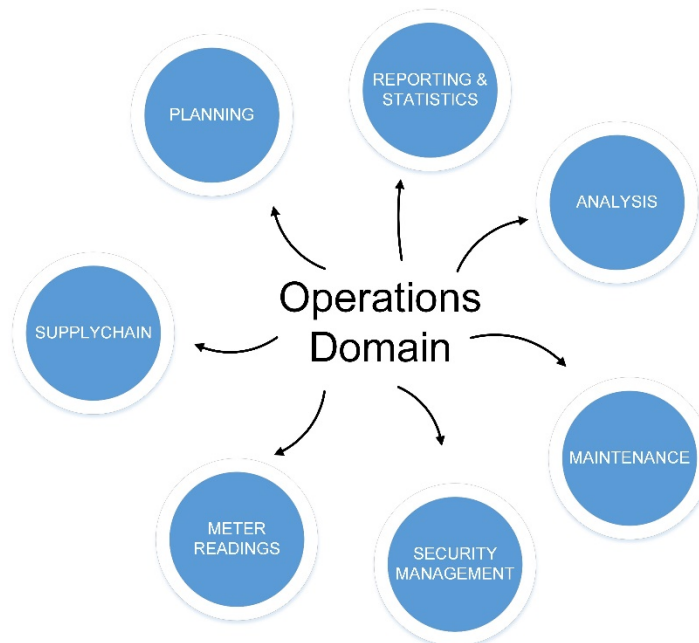
This domain takes charge of connecting the grid’s end users such as household, commercial, and industrial buildings to the power distribution network via the smart meters [5]. These smart meters monitor the flow of electricity consumed by the customers and provide statistics of usage. In addition, this domain also manages the connectivity with plug-in vehicles (PEVs). Fig. 5 summarizes the main functions handled by this domain.



**Figure 5: Customer Domain**

### 1.3.4 Operation Domain

The Operations domain mainly takes charge of managing and controlling the electricity flow of all other domains [5]. This domain undertakes supervisory tasks like monitoring, reporting, controlling and processing of other relevant information. Fig. 6 illustrates the flow of electricity from all other domains into the Smart Grid.



**Figure 6: Operations Domain**

### 1.3.5 Markets Domain

The Markets domain takes charge of the coordination and operations of all involved parties in the Smart Grid [5]. In effect, trading of energy services, wholesaling, retailing, market organization, and information exchange with other parties are handled by this domain. Fig. 7 shows all main functions performed by this domain.



**Figure 7: Markets Domain**

### 1.3.6 Service Provider Domain

The Service Provider domain takes charge of the operations related to the third-party such as information of energy management (see Fig. 8). Additional tasks like demand response programs, outage management and field services may be handled by this domain [5].



**Figure 8: Service Provider Domain**

### **1.3.7 Transmission Domain**

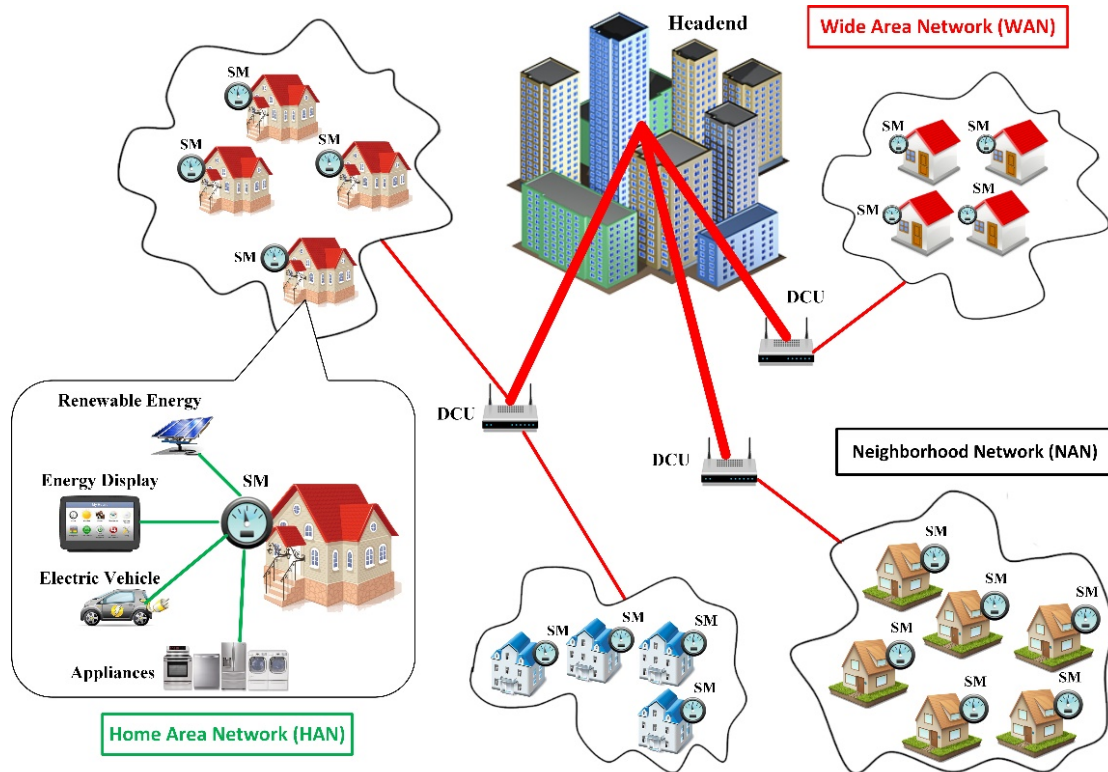
This domain mainly takes charge of transferring the electrical power from generation sources to distribution through several substations. It is electrically connected to both the Bulk Generation and Distribution domains; it also communicates with the Operation, and Markets domains. Maintaining stability of the electric grid by balancing generation (supply) with load (demand) across the transmission network is a primary responsibility of the Regional Transmission Operator or Independent System Operator (RTO/ISO), which typically operate the Transmission domain [5].

## **1.4 Smart Grid Communication Infrastructure**

Communication is the essential part of the smart grid infrastructure (SGI). It takes charge of the connectivity and information transmission of devices throughout among the entire system. [3]. This section will provide an overview of the smart communication layers. The home area networks (HAN), the neighborhood area networks (NAN), and the wide area



networks (WAN) are the three well-known layers of the smart grid infrastructure. Each layer has its own composition of different modules or controlling systems to cater for any provision to expand in the future (see Fig. 9).



**Figure 9: Smart Grid Communication infrastructure**

### 1.4.1 Home Area Network (HAN)

This layer is especially responsible for the setting up of communication between devices at household while its gateway is serving as interface for communication with the neighborhood area network (NAN). It mainly provides facilities for controlling and monitoring at customers' houses and implements sophisticated functionalities. The meter controlling system (MCS), metering module (MM), and Service module (SM) are features of the HAN. Each has its own specific functions: the SM takes charge of providing real-time energy consumption and tariff data to the consumers; the MM takes charge of storing

information about the energy consumption of the consumers; and the MCS takes charge of accumulating and controlling the information exchanged from SM and MM [6].

#### **1.4.2 Neighborhood Area Network (NAN)**

It is the second layer of the grid communication infrastructure is comprised of multiple interconnected MCSs of HAN which are located very close to each other. NAN also contains the smart meter data collector (SMDC) and the central access controller (CAC). All the metering archives are handled by SMDC while the CAC responsible for administering the communication between the HANs and energy provider. As thousands of houses needs to be covered by the network, supporting mesh networking, mostly covering square miles, is one of the main functions of NAN. With put into account that low latencies, typically 10 seconds or less were provided by these networks, because monitor signals are part of the bidirectional communication [6].

#### **1.4.3 Wide Area Network (WAN)**

This layer (WAN) is the last layer of the communication infrastructure in smart grid system. This layer takes charge of providing communication between highly scattered and smaller area networks which serve the power systems at different places. The WAN has three main components: firstly, the energy distribution system (EDS) specifically takes charge of the distribution of energy and metering data; secondly, the supervisory control and data acquisition (SCADA) controller manages the distribution of the grid elements; and thirdly the energy and service corporations (E&SC). The accumulated information from the two components EDS (metering) and SCADA controller (control) is transmitted to E&SC for making advance decisions on price [6].

## 1.5 Smart Grid Protocols

The advent of Smart Grid, which hopes to address several issues regarding the existing power grid, has urged researchers to conduct further studies in the design and development of an efficient infrastructure for connecting different components of SG. Furthermore, new wired/wireless approaches are ready for deployment to different components/applications of the SG to advance the currently used underlying networks and protocols [7]. In order to address these new challenges, the researchers will employ survey methods focusing on the routing issues in the Smart Grid communications infrastructure consist of three major components, (HANs), (NANs) and (WANs). The communication infrastructure in Smart Grid must support the anticipated smart grid services and meet the performance requirements. As the infrastructure connects a huge number of electric devices and administers the intricate device communications, it is created in a hierarchical architecture with interconnected discrete subnetworks, each taking responsibility for distinct geographical regions [8]. Table 3 summarizes the communication protocols that are used in Smart Grid communication architecture [9] [10].

**Table 3: Smart Grid Communication Protocols**

	<b>ZigBee</b>	<b>Z-Wave</b>	<b>HomePlug</b>	<b>Ethernet</b>	<b>WiMAX</b>	<b>Wi-Fi</b>
Connectivity	Wireless	Wireless	Wired	Wired	Wireless	Wireless
Max speed per channel	250 kbps (2.4 GHz) 40 kbps (915 MHz)	40 kbps	14-200Mbps	10-1000Mbps	280Mbps	11-300Mbps
Standards	-IEEE 802.15.4 -Proprietary(L3-L7)	Proprietary (Zensys)	IEEE P1901 Specifications: HomePlug 1.0 HomePlug AV, HomePlug C C	IEEE 802.3	IEEE 802.16 IEEE 802.16e	IEEE 802.11

Reach	10 -75 m (30 m typical)	30 m open-air, reduced indoor	300m	100m (Twisted-Pair Cable)	30 miles	100m (Indoors)
Layer	HAN	HAN	HAN	NAN	WAN	NAN

## 1.6 Security of Smart Grid

Security is an infinite game of wits, between asset owners and attackers. SGI security is not exempt in this. Security is considered one of the greatest challenges that hinder the growth of the Smart Grid [3]. The “two-way communication” between millions of devices within Smart Grid, a key characteristic of Smart Grid, generates a more reliable and robust electrical system. However, these benefits gained by using the Smart Grid come with major issues associated with securing the infrastructure of Smart Grid. Therefore, controlling the entire grid by advanced computers and other smart digital devices, which can affect the reliability of the Grid system, means that the integrity of both the transmitted data and the infrastructure must be well protected [11]. A study reports that two cyber adversaries from China and Russia have obtained access to the United States power grid and may have even implanted Malware into the grid system to cause a future power failure [12].

Equipping the Smart Grid with excellent resources while providing it with ineffective security gives an opportunity to an adversary with malice in mind to even take control of a section of the Smart Grid by violating the communication infrastructure, causing an extensive outage. Since the Smart Grid comprises many interrelated devices, this would in turn lead to power failure and monitoring problems through a major zone of the grid [12]. To fully achieve energy administration and service control, smart meter devices will also

be integrated into water and gas grids. Such an integration will add further complexity to the Smart Grid Infrastructure (SGI) [11]. The Smart Grid is envisioned to alleviate the functionalities of power devices and also modularize expendability and maintenance related issues. It will be composed of non-proprietary products that may utilize open source communication technologies like IP which have in the past proven to be fallible and have non-deterministic behaviors [13].

### **1.6.1 Smart Grid Attacks**

Smart Grid security must treat not only security breaches of the grid system caused by user errors, device failures, and natural catastrophes, but also deliberate cyber-attacks, such as from insider malcontents, terrorists, and industrial hackers [3]. Research shows that there were several attacks targeting the Smart Grid. This section explains and discusses briefly these attacks on the Smart Grid.

- **Eavesdropping:** As a wireless signal propagates over open space, any unauthorized node is capable of capturing the data transmitted and access confidential information. This kind of attack has the following properties:
  1. This attack can be quickly initiated, as low cost and off-the-shelf hardware components are easily available.
  2. Not easy to detect this attack as the attacker does not expose their activity. Such an attack can be mitigated by applying advanced cryptography, in which the unauthorized node can't understand the data [14].
- **Jamming:** The primary aim of this attack is to deteriorate availability by filling the wireless medium with noise signals. There are two types of this kind of attack, (1) Proactive jamming: in this attack, the wireless channel is completely blocked by

continuously giving out noise signals. (2) Reactive jamming: this kind of attack only launches when sensing signals on communication channel. The legal node could suffer from this attack in two ways: first, the channel will always be busy for any channel sensing performed by this node; second, the node may fail of receiving packets. Furthermore, it is not easy to detect a reactive jammer as it is very difficult to know whether the packet loss results from attacks or normal collisions [15].

- **Consumer Device Implant:** In this attack, the adversary tries to implant a bogus device into the system of the Smart Grid to act as a legal consumer device. The motivation behind this is to tamper with the electricity readings of the consumer device. Both the consumers and the electricity utility will be affected by this attack [16].
- **Meter Implant:** A fake meter (or legal meter that runs malicious software) can be planted in the Smart Grid system with the main goal of to disrupting the routine functionalities of the Smart Grid, or to compromise the electricity company's image. In this attack, the amount of the electricity usage bill of a given consumer can be increased/decreased [16].
- **Black Hole:** A Data Collection Unit (DCU) for an SGI may act in an inappropriate manner due to malicious software installation. In this case this DCU can be considered as a Black Hole in the SGI communication network. The Black Hole attack is used to prevent many meters from sending their reading to the control center services (CCS) through the DCU. This attack can disrupt the entire operation of the Smart Grid for a given neighborhood area network (NAN) where this fake DCU exists [16].
- **Hand-held Terminal Exploitation:** Hand-held terminals are used by Smart Grid technicians for the purpose of maintenance or software installation. The internet

connectivity and USB port interface make these terminals exposed to compromise either by a worm or malware, considering that any hacking of these terminals may cause disruptions to SGI operations. The motivation of such an attack is to damage the SGI instruments, such as smart meters and the DCU and this may cause severance to the Smart Grid operation as well as consumer frustration [16].

- **DDoS attack against Data Concentrator Unit (DCU):** The reason of such an attack is to violate the DCU and disrupt communication between NAN and WAN networks. Assuming the entry point of this attack is the smart meter, typical attack steps that would be required are (1) install malicious software on meters through physical manipulation or exploitation of weak points in network, (2) coordination of DoS campaign, and sending malicious packets to (DCU). Fig. 10 illustrates this attack and all the steps in which such an attack can be launched [15].

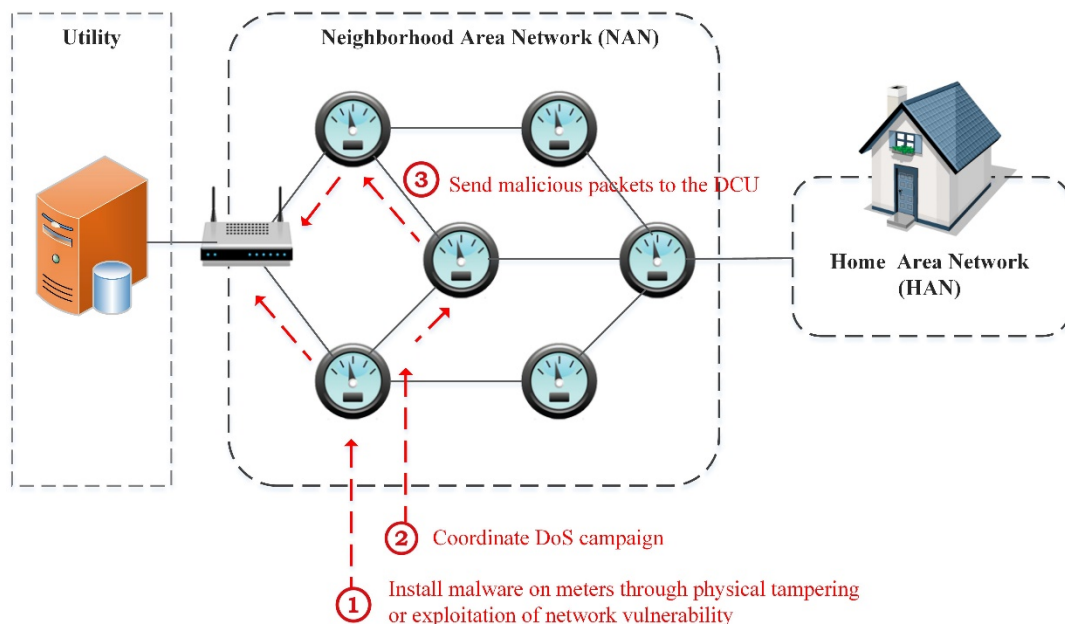


Figure 10: DDoS Attack against the DCU [14]

- Stealing Customer Information:** The motivations identified for this attack include the collection of customer information to learn about customer behavior. This attack can be launched through the meter, by snooping on the incoming and outgoing network traffic of the meter. This attack may call for the following individual steps: (1) stealing decryption keys by physically accessing the meter or executing brute-force attack on the cryptosystem, (2) spying on the AMI traffic, and (3) decryption of the messages and collection of the message content [14].
- Sending Remote Disconnect Commands through the DCU:** The main goal of launching this attack is to disconnect a large number of customers' meters (see Fig. 11). The DCU is very likely to be the point for launches such an attack. The attack steps involved are: (1) installing malicious software on the DCU through physical manipulation or exploitation of vulnerability; (2) collecting information about target smart meter (e.g., IP address); and (3) conveying remote disconnect command [14].

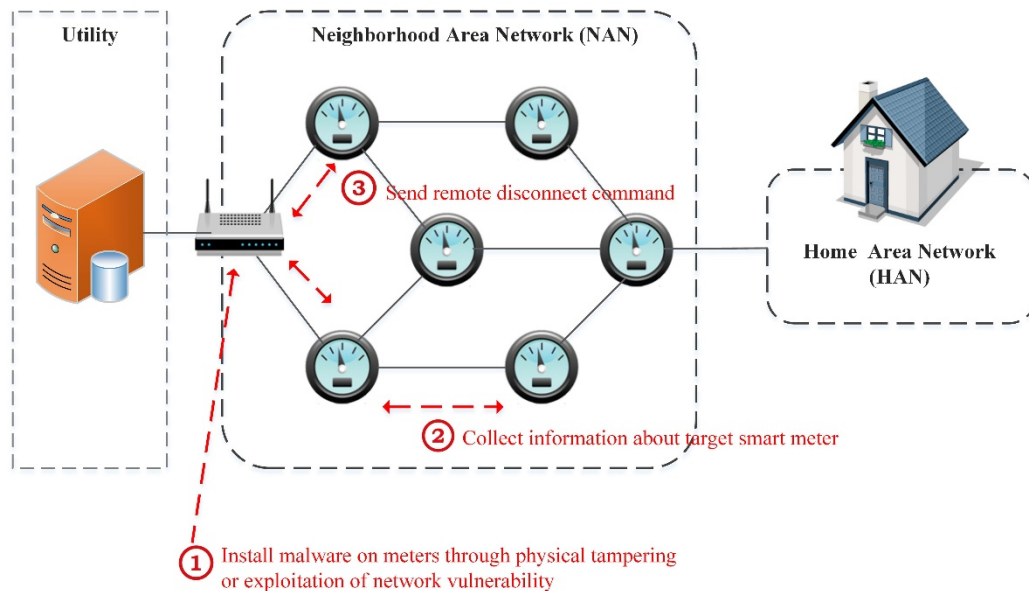


Figure 11: Remote Disconnect Command Attack [14]



## **1.7 Problem Context**

This research mainly focuses on the detection of smart meter compromise attacks that disturb the Smart Grid communication infrastructure. As the Advanced Metering Infrastructure (AMI) of the Smart Grid comprises a multiple of interconnected Smart Grid devices that form a mesh, traditional intrusion detection systems are no longer sufficient and effective for the AMI. Therefore, relying on a single front-end intrusion detection system to check the incoming and outgoing network traffic to identify intruders for an entire neighborhood area network (NAN), may not be suitable for an AMI. Moreover, millions of smart meters were deployed by some utility providers at their service regions, thus affecting the scalability of distributed sensor-based intrusion detection schemes. In this regard, we need to develop a mechanism to perform localized intrusion detection within clusters of smart meters with low data processing overheads.

## **1.8 Research Objectives**

The ultimate objective of this research is to model and analyze Meter Compromise attacks in the Smart Grid Communications Infrastructure (SGI), and present new countermeasures and mitigation techniques against these. A classification of smart grid attacks and countermeasures will also be studied to benefit the Smart Grid research community. We shall work towards a formulation of various attack scenarios based on system and network parameters. The primary objectives of the thesis work can be summarized through the following points:

1. Explore Smart Grid cyber attacks and their effect on the grid.
2. A taxonomy of attacks on the Smart Grid together with an analysis of various countermeasures.
3. Model and analyze Meter Compromise attacks on the Smart Grid and present countermeasures.
4. The proposal of a scheme based on clustering of smart meters within a NAN that supports a timely exchange of readings between peer-meters of a cluster.
5. Performance evaluation of the proposed scheme through simulation under varying network and system parameters.

## **1.9 Research Methodology**

To achieve the above mentioned research objectives, We will follow an approach that combines theoretical, developmental, as well as experimental aspects. The research will be initiated with an extensive literature review that covers most of SG aspects and different types of cyber-attacks violating Smart Grid communication infrastructure. The information gained in this step will smooth the path to build the experimentation models needed in this research. A proposal of novel meter compromise attack mitigation techniques will be the key phase to design experimentation. Simulation of real-life scenarios is essential to gain deeper understanding of meter compromise attacks and how to counter such attacks and reduce their impact on SGI. Documentation is an integral part of this research and will be conducted in parallel with each phase. This will also satisfy the goal of the researchers to publish results in reputable journals and conferences.

## **1.10 Research Contribution**

Despite the Smart Grid's great benefits, its security is still in its early stages. With security being one of the top challenges that hamper the widespread acceptance of SG technology, it has become a major field of study. The existing security frameworks and traditional intrusion detection systems do not adapt well to the Advanced Metering Infrastructure (AMI). Instead of having a single front-end intrusion detection system for an entire neighborhood area network, we propose a distributed information sharing mechanism to perform localized intrusion detection within clusters of smart meters. The scheme effectively reduces the data processing overhead imposed on centralized intrusion detection systems operated in the utility providers' servers positioned in the AMI's demilitarized zone. It operates through collaborative information sharing between smart meters of a given neighborhood or cluster. Information exchange between smart meters is done at fixed intervals of time, assuming loose time synchronization. The exchange of local electricity usage readings between peer meters leverages localized intelligence on observed network traffic by the meters to the DCU, and provides for a holistic visualization of network traffic activity. Meter-to-meter communication topology was implemented, and its effect on the intrusion detection scheme's performance was studied.

## **1.11 Thesis Outline**

The rest of the thesis is organized as follows: In Chapter 2, we provide a taxonomy of different kinds of Smart Grid cyber attacks with a mitigation analysis. Specifically, we group these attacks according to their targeted services or devices, as well as on the type of the attack. Five groups of smart grid cyber attacks will be highlighted, namely Physical

layer attacks, SCADA attacks, Smart Meter attacks, Replay attacks and Data injection, and Network-based attacks.

In Chapter 3, we present a distributed information sharing mechanism to perform localized intrusion detection within clusters of smart meters. This scheme identifies smart meter compromise attacks through collaborative information sharing. The technique is novel, as smart meters within communication range of each other are clustered together for information sharing and collaborative attack detection. In Chapter 4, we present the Performance Analysis of the Proposed Algorithms through a discrete event simulation of varying neighborhood area networks of an AMI. The study is concluded and the direction of its future work is proposed in Chapter 5.

## CHAPTER 2

### SMART GRID ATTACKS AND COUNTERMEASURES

The birth of Smart Grids (SGs) that zero in to a timely, efficient and effective (meaning uninterrupted) power supply to consumers makes their platform essential in today's world. As well as this, while consumers enjoy optimizing their electricity usage, they also enjoy receiving accurate and constant feedback on their electricity usage from the smart meters through support from the underlying smart infrastructure (i.e. various devices that comprise a Smart Grid). However, this integration of modern technologies into the Smart Grid infrastructure also brings cyber security and privacy challenges. Many security, privacy and reliability issues appear during electric power delivery.

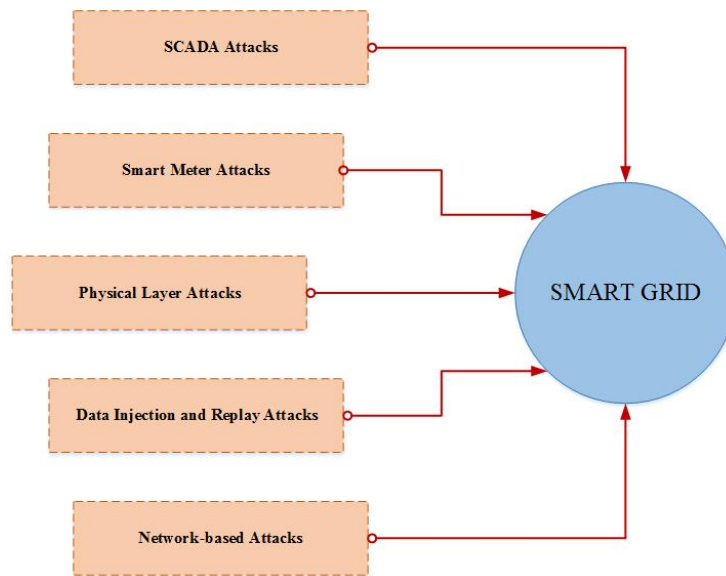
As many of the Smart Grid's functions, like control and monitoring, are heavily reliant on the use of a modern communication technologies, the security of the grid infrastructure against the cyber/physical attacks is significant. Smart Grid (SG) is not exempt from being exploited; it is therefore vulnerable to malicious attacks.

With security being one of the top challenges that hampers Smart Grid, it has become a major field of study. Many attacks of different classes may be committed against the entire Smart Grid system or may be against particular components or devices therein. A proper identification and detection of such attacks represents the first procedure towards defense and protection. Throughout this chapter, we attempt to provide a taxonomy of different kinds of Smart Grid cyber attacks that attack the Smart Grid system. We will also present number of countermeasures. We classify these attacks according to their targeted services

or devices, as well as on the type of the attack. Five groups of Smart Grid cyber attacks and the countermeasures that will be highlighted and fully discussed in this chapter:

1. SCADA attacks,
2. Smart Meter attacks,
3. Physical Layer attacks,
4. Data injection and Replay attacks, and
5. Network-based attacks.

Fig. 12 illustrates the five classes of the cyber attacks that violate the Smart Grid infrastructure.



**Figure 12: The five classes of the attacks that violate the Smart Grid infrastructure**

A summary of security benchmarks affected by the different Smart Grid attacks, and the place where such attacks take place, is explained in Table 4.

**Table 4: A list of security benchmarks affected by the different Smart Grid attacks, and the location where such attacks take place**

<b>Attack Type</b>	<b>Affected Security Property</b>	<b>Victim Location</b>
SCADA	DoS, Confidentiality, and Integrity	Home Area Networks
Smart Meter	Confidentiality, Integrity, Availability, Non-Repudiation	HAN / NAN
Physical Layer	Confidentiality, Data Integrity, and DoS	HAN / NAN / WAN
Data Injection and Replay	Confidentiality and Integrity	Home Area/Neighborhood Area/ Wide Area Networks
Network-based	Availability, Confidentiality	Home Area/Neighborhood Area/ Wide Area Networks

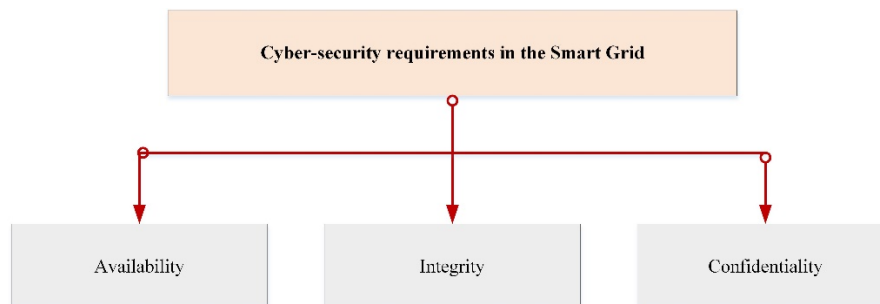
In Section 2.1, a summary of cyber attacks requirements for the Smart Grid is illustrated. Several kinds of SCADA security threats and the proposed mitigation techniques are discussed in Section 2.2. Smart meter-specific attacks and countermeasures are explained in detail in Section 2.3. An in-depth analysis of physical layer attacks that violate the Smart Grid system is thoroughly discussed in Section 2.4. Several data injection and replay attacks are examined in Section 2.5. Lastly, network-based attacks are analyzed and reported in Section 2.6. The summary will be in Section 2.7.

## 2.1 Requirements for Cyber Security of Smart Grid

Smart Grid cyber security requirements can be classified into the following features: requirements for cyber security; typical cyber attacks; and countermeasures [17] [18].

In [19] analyzes information security problems which face the status of Smart Grid and proposes identity-based authentication and security domain to assure the safety of the cyber security for Smart Grid. It also pinpoints the primary source of information security threats to be at six weak points of the Smart Grid system: Distribution network, Power station, Electric vehicles (EV), Advanced Measurement Systems, Indoor Internet users, and Operation networks of the electricity transmission systems. Popular security problems in Smart Grid standards that take on communications protocols and the main motives for these problems have been discussed in Refs [20] and [21]; also the cyber-security weakness and adversary entry points to the grid infrastructure have been highlighted.

Based on the recent detailed guideline for Smart Grid cyber-security that was issued by the cyber-security working team in the NIST, the three major high-level key cyber-security requirements for the Smart Grid system are illustrated in Fig. 13.



**Figure 13: The three major cyber-security requirements for the Smart Grid**



Examples of some typical cyber attacks which may be used by the attacker affect the Smart Grid system as follows: ***DoS or DDoS*** attacks, wherein the main goal is to disrupt the availability of the grid system through hindering message exchange between devices of the Smart Grid system. These types of attack decrease the availability of the system. ***Malicious Software***, generally known as *malware*, exists in various common forms: viruses, worms, Trojan horses, logic bombs, and backdoors or trapdoors. Such attacks may directly or indirectly compromise the availability, integrity, and confidentiality of the Smart Grid. The programmers are deliberately embedding logic bombs, backdoors and trapdoors into programs which may be utilized to launch attacks later. ***Identity spoofing*** are attacks which allow adversaries to impersonate an authorized user without using the user's password. Common types of this attack include man-in-the-middle, message replay, network spoofing (for example IP spoofing), and software exploitation attacks. ***Password Pilfering attacks*** are these in which data confidentiality is violated. Different techniques and methods could be used in such attacks, like guessing, social engineering, password sniffing, and dictionary attack. Unlike technical attacks, the social engineering attacks refer to a method of attacking or penetrating a system using social skills (for example psychological measures). ***Eavesdropping attacks*** are carried out against data confidentiality of the SG communication channel by intercepting IP packets on the LAN or sniffing wireless transmission signals on the home area network (HAN). ***Intrusions*** are attacks which take place when an illegal user gains an access to a cyber-system and gets undesired access to important back-end servers. Examples of popular hacking tools to commit intrusion attacks are Port scan and IP scan. ***Side-Channel Attacks*** have as their main goal the retrieval of the cryptographic keys. The common examples of such attacks are power analysis, timing,

analysis, and electromagnetic attacks. Various components of the Smart Grid system like pole-top equipment, substations devices, HAN devices, and smart meters are vulnerable to side-channel attacks which could lead to an intrusion of customer privacy, administrative access to the grid system, and electricity usage information, passwords [20] [21].

In order to avoid the above mentioned cyber-security attacks, the International Electrotechnical Council (IEC) has put forward a set of relevant mitigation techniques. Technical solutions include encryption, access control, anti-virus, (VPN), intrusion detection system (IDS), firewall, etc. From a security management point of view, solutions include, risk assessment of assets during-attack and post-attack recovery, key management, security incident, security policy exchange and vulnerability reporting, etc. Examples of real cyber-security incidents are Stuxnet and Slammer malwares.

In [18], the cyber security requirements and the most vulnerabilities of the Smart Grid communication were investigated as well as a survey of the existing solutions of the cyber-security in the communication infrastructure of the Grid. They also identify main cyber-security problems in securing and running a secure communication system for the Grid like ***Internetworking***. Because of a weak built-in security in different devices and applications, the communication systems of the Smart Grid are exposed to different types of attacks that vary across the network. In this regard, the Smart Grid should be equipped with a model for a network that minimizes the most vulnerabilities and threats from fabrication, interruption, obstruction, and alteration. Making the transport facilities entirely owned by a utility, would greatly minimize the threats from intruders, as there would be no potential for access from intruders over the Internet. High security steps must be applied to all the holes in Smart Grid network system that connected to the Internet. Also an intrusion

detection systems are required not only at the points of the Grid network which connected to the Internet, but also at the important points within the Grid network well as most vulnerable wireless holes. ***Security policy and operations***: the reliability of the Smart Grid depends on the appropriate operations of many components and the connectivity between them. Several methods could be used by the attackers to disrupt a Smart Grid system including gaining electronic access to a component and configuring it to impersonate another component and/or reporting a false condition or alarm. Denial of Service (DoS) is one of the simplest types of attacks that an attacker might attempt to prevent authorized devices from communicating by consuming excessive resources on one device. The Smart Grid protocol designers should pay attention to such threats during protocol development and ensure that proper care and mitigation are applied. ***Security services***: the network operators can easily identify, control and manage security risks in Smart Grid communications via the help of security services. It has been reported by EPRI that every aspect of a Smart Grid must be secure. Ensuring secure operation of a Smart Grid cannot be achieved only via cyber security technologies, but also through policies, on-going risk assessment, and training. The development of such a procedure takes time, and indeed it needs to take time to ensure that they are done correctly. In order to achieve organizational objectives, the Smart Grid needs access to cost-effective, high-performance security services, including expertise in mobility, security, and system integration. The typical set of security services in Smart Grid communications include security assessment, secure design and implementation, risk management, security policy, managed security, and incident response planning. ***Efficiency and scalability***: in critical systems such as the Smart Grid, the availability of the system is of high importance, so several key issues need to be

addressed. Firstly, to handle all requests and in order that resources do not get overwhelmed, an efficient use of computation and communication resources must be present in the system. Secondly, failures in the system which, for example, result from bad messages must be handled properly by employing a good error management in the system. Furthermore, to avoid resource exhaustion in the face of adversarial action, the error management functions must be fail-safe in nature. Thirdly, the system redundancy must be ensured so that, if sub-systems fail or are compromised, then the entire system does not collapse. Fourthly, in order to detect and respond to cyber attacks, a system must support auxiliary security functions that may be deployed in the Smart Grid communication system.

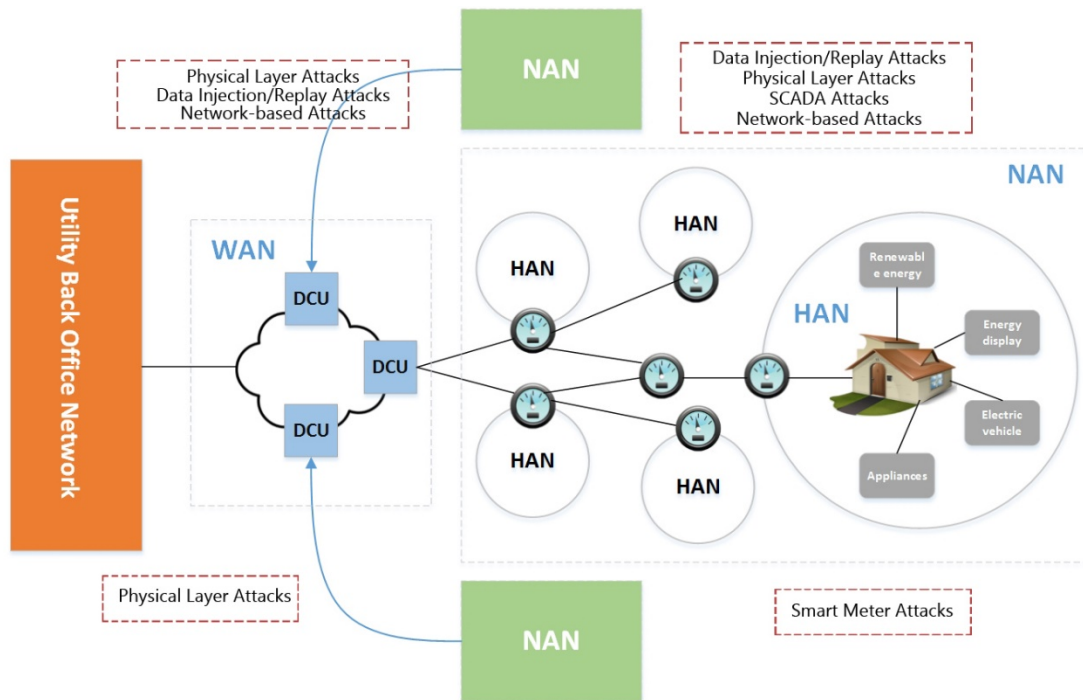
***Differences between Enterprise Network and Smart Grid Networks Security:***

technological advancement has grown rapidly over the last decade. In the IT industry, various security solutions to protect enterprise networks and to safeguard or lessen their vulnerability from any cyber attacks were developed. Solutions like firewalls and intrusion detection systems are the recognized effective ways to secure the communication infrastructure at business world and office levels. But, other solutions and techniques like enterprise network-based cyber security solutions fall short in providing the same level of security at the automation and control levels. The following are the three main differences between the security of Smart Grid network and enterprise network.

1. *Different security objectives:* in the enterprise networks, the main security objective is to protect data. These include data integrity, data confidentiality, and data availability. In contrast, the main security objectives of the Smart Grid are human safety, ensuring system reliability, and protection of equipment and power lines.

2. *Different security architecture:* the data server in any enterprise networks is placed at the center of the network and demands more protection than the other nodes of the network. For Smart Grid networks, terminal nodes require a subset of the controls used for the central device.
3. *Different technology base:* Windows, Linux, and UNIX are the operating systems widely used in an enterprise network, and all the devices are interconnected via Ethernet with IP-based protocol. In Smart Grid networks, many different protocols are used.

The standard Smart Grid architecture, with attack classes highlighted at the appropriate location where these is the possibility of their occurrence are illustrated in Fig. 14.



**Figure 14: Attacks with their possible location at smart grid architecture**

## **2.2 SCADA Security Concerns**

SCADA system is the core to the observing and control of a substation in the Smart Grid infrastructure. It provides powerful integrated solutions when upgrading remotely installed electric equipment and helps the utilities to obtain higher reliability of supply and reduce the costs of maintenance and operating. Equipping the electricity grid with advanced computing devices and technologies has had far-reaching effect on the security of the grid system. The weak points in the electricity grid are a known concern [22]. Connecting the electricity system devices to backend servers and invariably the Internet, has caused the exposure of the Smart Grid system to a vast range of cyber attacks and threats. Supervisory Control and Data Acquisition (SCADA) is one such system that has acquired attention. The main attacks that may violate critical components of Smart Grid infrastructure through SCADA are given in the following subsections [22]:

### **2.2.1 Platform Vulnerabilities**

The existing and known security gaps in company, computing resources, and backend networks are exploitable for hacking devices of the Smart Grid. Due to the uninstalling of the operating system batches, the attacker can disrupt the Smart Grid computing system, to initiate an attack against SCADA devices. In like manner, the absence of intrusion detection systems (IDS) or front-end firewall in certain applications, will give the perfect platform to the attacker for hacking the system of the Smart Grid. Other possible security gaps include software-based attacks, wherein the attacker exploits the vulnerabilities in the software that runs on the devices of the SCADA system. Buffer overflow and DoS are two examples in which the inherent ability of the software to continuously request hardware

resources during the program execution is exploited beyond the system capability. Likewise, flooding the end-servers by initiating a big set of requests for resource allocation will cause a Denial of Service against legal users, and this will affect the customer confidence in the electricity utility.

### **2.2.2 Policy Vulnerabilities**

In general, the main cause of this concern comes from the security administrators defining a set of weak security policies for a certain system. Such a threat exists for information technology systems that have connectivity to the Smart Grid SCADA devices and components. In case a weak password leads to the disruption of a system by an adversary, the person responsible for this violation is the policy administrator. It is thus important for any system to enforce security policies that are strong enough to ensure no exploitable holes due to weak policies.

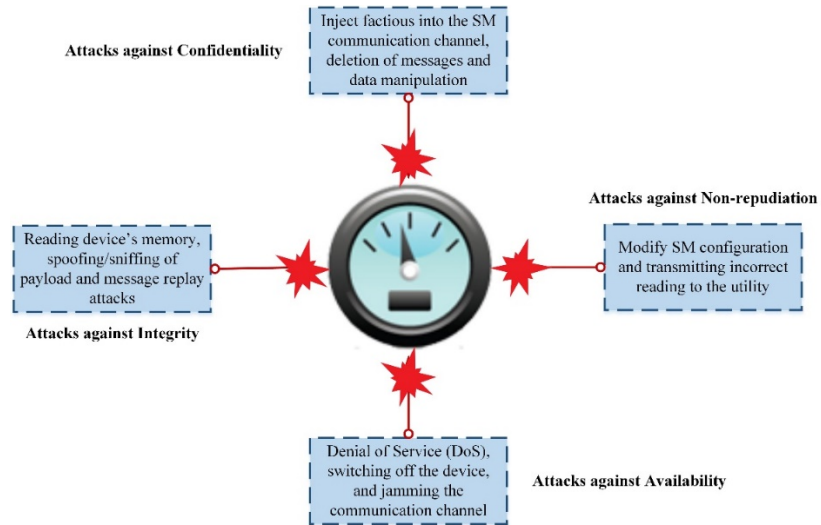
### **2.2.3 Network Vulnerabilities**

The Smart Grid infrastructure comprises some network-layer devices; these devices could pose serious threats to the grid infrastructure. Configuring one of these devices according to weak policies may cause a disruption of the Smart Grid through ingress/egress network holes in the SCADA devices which are connected to the core network of the Smart Grid system. A few examples that clarify how mal-configured network-layer devices can cause a severe threat to the Smart Grid system include packet flag tampering, resetting the data of outstation, fragmented message intervention, and spoofing the source/destination address to tamper with the IP packets of devices at network-level.

## 2.3 Smart Meter Attacks and Countermeasures

The smart meter as a newly developed device is an important component of the Smart Grid system. It is the central connecting point between consumer networks and the electricity utility (see Fig. 15). Furthermore, it is used to measure the amount of electricity used by a consumer. It is simply an electrically powered device that can monitor the energy consumed for the specified time interval (half an hour or one hour, for example) depending on how it is programmed. Bi-directional connectivity is its unique feature, which allows customers to receive tariff information from the utility companies and to send customers' readings back to utility companies for checking and billing purposes. The device can also be separated in two ways according to its functions and capabilities: *i*) metering capabilities, and *ii*) communication capabilities. For that reason, securing the smart meter is of extreme importance to the overall security of the Smart Grid system as any compromise of a smart meter may jeopardize the security of not just the household in question, but the entire neighborhood network and possibly the utility provider's core network. Smart meter cyber attacks that violate the main pillars of information security are summarized in the sections below [23]. Fig. 15 provides a description of these attacks that target the smart meter.





**Figure 15: Cyber attacks that target the Smart Meter**

### 2.3.1 Confidentiality

Cyber attacks that violate confidentiality try to steal sensitive information that should be kept secret or shared only between the trusted entities. Tampering with the memory of smart meters, adjusting the control program of smart meters, spoofing the ingress/payload, and message replay attacks are some examples of how such attacks violate confidentiality. Several mitigation techniques have been proposed to decrease confidentiality breaches through a smart meter. These include replacing the shared secret keys between smart meters and the data concentrator unit (DCU) in a neighborhood area network, and eliminating the traits of the malicious attacks through configuring/resetting the device settings, for example, resetting the secret key, and replacing the actual device. In the Smart Grid system, privacy of customer data is an important concern. Tracking and analyzing the pattern of electricity usage of a certain household may expose many sensitive parameters like consumer habits which could be used by other spam parties for malicious objectives,

such as checking whether the customer is at home or not [24]. Acquiring such sensitive information by such parties may cost the electricity utility through selling this information to its competitors who may use it maliciously.

### **2.3.2 Integrity**

The cyber attacks that violate a smart meter's integrity happen when the legal data of the smart meter is manipulated, erased, or replaced before this data is transmitted to the data concentrator unit (DCU) within a neighborhood area network (NAN). The data can be tampered with by the attacker in two ways, either while it is stored (i.e. within the device's computing resources or memory) or in transit through rigging/erasing/injection of messages. Fabricated data can be injected into the communication channel of the smart meter by the attacker to commit energy fraud by either increasing or decreasing the electricity consumption of a certain household. Such a violation will cost both the end-consumers and/or the electricity company. Two malicious intentions may motivate the attacker to launch a message replay attack. First, the electricity company may receive the same smart meter electricity usage reading from a house as previous ones. Accordingly, an inflated electricity usage reading of a house may go unrecorded. Second, in a similar way, due to a faking attack the reported electricity readings from a household may be reduced to benefit the end consumer, to the cost of the electricity company. Several methods exist to mitigate the effect of attacks against smart meter integrity. The most popular technique is to enable and generate secret keys of suitable length (according to recent technological trends) between the two entities (sender and receiver) during electricity usage data transmission. Such a procedure will help ensure that the message integrity at the receiver side will be verified using a message authentication code (MAC).

### **2.3.3 Availability**

To some extent, the attacks against availability are different from those that violate confidentiality and integrity. The continuing availability of a smart meter within the Smart Grid system is also vulnerable to cyber attacks. A denial of service (DoS) is the best known attack that violates availability and it comes in different forms. However, all of these kinds of attack share the same aim which is to attempt to make the system resources unavailable to its legitimate users. The following are some other examples of such attacks: turning off the device, DoS against network DNS server at the organization, sniffing, and disrupting communication channels through jamming. We need to consider that the problem of disabling the ZigBee security mode in a smart meter, is that it could possibly lead to invoke a remote turn off request to command a smart meter to be switched off. As a result, the electricity reading of a certain household will not be reported unless the smart meter is restarted. Similar results to the previous attack can be expected due to jamming the communication channel. The decryption of secure messages transmitted by the smart meters to the end-servers among data concentrator units (DCUs) will be prevented due to the modification of the stored secret keys at a smart meter. Smart meter availability is affected for all three mentioned scenarios.

The present mitigation techniques that prevent such attacks are empowering the ZigBee security mode, replacement of malicious smart meters, changing the frequency of communication channel during message exchanging, and updating the secret keys.

### **2.3.4 Non-repudiation**

NIAG defines nonrepudiation as *“assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can*

*later deny having processed the data*". In this kind of attack the attacker attempts to deny any misbehavior against the system. For example, a certain malicious smart meter may convey a fake reading to the electricity provider, and then deny having done so. Non-repudiation can be enforced through the use of secret keys for data encryption within the smart meter; no other object is expected to have a copy of the same secret key. Conversely, the absence of a secret-key based approach will hinder the identification of such a cyber-attack [25].

A motive behind the launching of such attacks against the smart meter is to tamper with the configuration of the meter. Within the Smart Grid system, smart meters must be secure enough to resist both hardware and software-based cyber attacks that try to manipulate its configuration. The enormous number of smart meters [26] (i.e. smart meter households) that are deployed in a metropolitan city requires high security in order to avoid a large-scale disaster due to such attacks. Several cryptography-based techniques are proposed for the protection of data confidentiality in the Smart Grid system [27].

## **2.4 Physical Layer Attacks and Countermeasures**

Communication plays a critical role in the Smart Distribution Grid (SDG) as it enables the utilities to attain three key objectives: security, intelligent monitoring, and load balancing. However, compared to wire communications, wireless communications are usually more vulnerable to security attacks. Therefore, developing a suitable wireless communication architecture and its security measures is very important for a Smart Distribution Grid (SDG).

The authors in [28] have investigated and put forward a wireless communication architecture for the Smart Distribution Grid (SDG), followed by an in-depth analysis of the security framework for this communication architecture. To achieve a robust, reliable, and secure communication architecture for a Smart Distribution Grid (SDG), several design rules are formulated as follows:

1. security measures must be considered at all protocol layers, and cross-layer design is adopted whenever possible;
2. protecting the time critical messages through deploying a security mechanism;
3. all the wired communication links must be subjected to high security to strengthen the security of the wireless communication paths.

In addition, information messages should have different security levels based on two important criteria: delay and loss. The messages that are highly dependent on both delay and loss should have the highest security level. Messages that are only dependent on either delay or loss should have a medium level of security, while messages without delay or loss constraint should have the lowest security level. Dedicated resources must be allocated to messages with the highest security level.

Authors [28] have identified threats violating the Smart Distribution Grid (SDG) through the wireless channel as follows:

1. jamming;
2. eavesdropping by outsider nodes;
3. spying on wireless medium by malicious node;
4. executing attacks from wireless channels of the SDG.

Several security measures were proposed for security of the SDG as follows:

1. anti-jamming approaches;
2. securing the physical layer to prevent eavesdropping;
3. securing the network access from any unauthorized nodes through effective authentication schemes;
4. implementing highly secure protocols to disable insider attack.

In [28] and [29] an in-depth analysis of the physical layer attacks were provided as follows:

### **2.4.1 Eavesdropping**

As a wireless signal propagates over open space, any unauthorized node is able to capture the data transmitted and access credential information. As a result, the confidentiality requirements maybe violated. Critical data of the smart meter can easily be noticed through such an attack. Low-cost adversaries exist in the market, to easily launch such attacks using off-the-shelf hardware components. It is not easy to detect such an attack, as the adversary does not expose its activity. With a view to protecting critical data from being exposed to the attackers, a data encryption approach should be used. In any case, if a certain pattern of transmitted data is depicted, a brilliant attacker may still be capable of analyze and decipher the message content. For example, the electricity usage of a household will reduce if this household is unoccupied. If the smart meter communicates with the data concentrator unit (DCU) only when a specific threshold of electricity usage is exceeded, or if the transmitted message length is directly proportional to electricity consumption, a pattern of activity for a certain house could subsequently be constructed.

### **2.4.2 Jamming**

The primary aim of this attack is to disrupt communication and information flow in any wireless network architecture by filling the wireless medium with noise signals. Within the Smart Grid system, an attacker may try to block the exchanging of information with the electricity provider through filling the wireless channel with noise signals. There are two types of this attack:

- i. Proactive jamming. In this attack, the wireless channel is continuously blocked by continuously giving out noise signals.
- ii. Reactive jamming. This kind of attack only launches when sensing signals on the channel. The legitimate node could suffer from this attack in two ways:
  - a. The channel will always be busy for any channel sensing performed by this node.
  - b. The node maybe fail to receive packets. Also it is not easy, to detect a reactive jammer as it is so difficult to know whether the packet error results from attacks or normal collision.

### **2.4.3 Injecting Request or Restrict Access**

The primary purpose behind launching this attack is to interrupt the routine operations of MAC layer within the smart meter. The adversary may succeed in blocking the smart meters from commencing their legal MAC operations or causing packet collisions. This attack can be summarized as follows:

- i. It is almost identical to reactive jamming, wherein the attack is initiated with the main intent of blocking the communication channel.

- ii. It attacks a multi-user access channel.
- iii. The adversary sets its own backoff timer to be of very short length, and so the channel prioritizes access to the attacker each time it desires to communicate, while legitimate smart meters of the Smart Grid system have their access denied.

#### **2.4.4 Injection Attack**

Dissimilar to the two prior attacks that rely heavily on spurious signals, the injection attack inserts structured messages into the wireless channels. Imitation and replay attacks fall into this category. We may describe this attack as follows:

- i. The attacker imitates either a legal sender/receiver node to acquire unauthorized access to the wireless network. A common imitation is device cloning. At the physical layer, the cloning is obtained by means of spoofing the MAC address. Replay attack: a malicious repetition or holdup for a valid data transmission by an adversary.
- ii. This attack has almost identical characteristics to the TCP-SYN flooding attack. That is, when receiving too many fake messages, a victim can be burdened with processing them. Then the overhead system resource cannot respond to legitimate requests any more. Due to this violation the availability requirement is affected. In this attack, the messages remain readable by the receiver so that it is not easy to prevent the attack.

In order to avoid such an attack, suitable security mechanisms should be enabled to confirm message authentication.



## 2.5 Data Injection and Replay Attacks

Another type of cyber attack in the Smart Grid system is the data injection and replay attack. In this, attacks take place when fabricated data is inserted into the smart meter or neighborhood area measurements and this noticed by a network worker. These attacks mainly target the Smart Grid infrastructure, especially monitoring and control sub-systems with the intention of tampering with smart meters and phasor measurement units (PMU). As a result, the operation and control of the electricity provider are misguided [30]. In [30], [31], and [32], an effort is made to examine methodically and intelligently Smart Grid data for possible data injection. The proposed method towards detecting such an attack does a rough calculation on the state of the system from the observed measurements and calculates the remaining quantity between the observed and the estimated measurements.

Message replay attacks happen when an adversary gets a high privilege access to smart meters and can consequently insert control signals into the system. For launching this attack, the attacker may need to (a) obtain customers' electricity usage behavior via capturing and analyzing data exchanged between the appliances and smart meters within the household, and (b) manipulate and insert fake control signals into the system. In general, the primary goals of the replay attack are as follow:

1. Energy fraud, through rerouting electricity to another site.
2. Causing physical harm to the grid system. The famous example of this is Stuxnet Malware.

The authors in [33] focused mainly on one of the most well known security cyber attacks on the Smart Grid system, that is replay attacks. They proposed a mechanism for detecting

replay attacks within the Smart Grid system, wherein the house appliances are considered as linear time invariant systems, where the smart meter is entrusted the task of observing the household devices. The observed minimum variance in actual device readings is tested through a state estimator based on Kalman filters. The suspicious anomalous activities that affect the Smart Grid are discovered via a detector device on the observed readings. This proposed detector device is not only adaptable for serving a single household, but also serves a group of households in the neighborhood. The replay attack is clearly define as a modification to the control signal that is exchanged between consumer appliances within the household and the smart meter.

A theory-based method for identifying the attacks against state estimator perturbations have been illustrated in a graph in [34]. A graph that composed of transmission lines and smart meters is used to model the entire power system. The Control System Center (CSC) is responsible for performing the state estimation in a centralized way. The purpose of the estimation is to retrieve the entire system state. The state remains unsteady based on the adversaries data that have been injected. The measuring of Minimum Mean Square Error (MMSE) used to verify this, the MMSE will invariably be higher in the existence of the malicious data. The likelihood that the Control Center (CC) detects the attack is increased by the increase of the injected energy. A simple optimization is used to confirm the suspicious meters as injecting malicious data into the network, According to the Generalized Likelihood Ratio Test (GLRT). The smallest noticeable attacks which result in highest harm to the state estimates are detected through the algorithm operates in polynomial time.

## 2.6 Network-based Attacks

The man-in-the-middle is a notorious example of topology attacks on a Smart Grid [35]. This attack happens when the adversary prevents network data (e.g., breaker and switch states) and meter's data from distant terminal units, falsifies a part of these, and redirects the modified version to the control center. In the lack of data alerts in recent power systems, the hacker could succeed in adjusting both smart meter and network data so elaborately that they are consistent with the “target” topology.

In [36], the authors present and investigate several kinds of intelligent attacks and countermeasures in the Smart Grid communication system, which aim for higher-level damage or benefits by taking advantage of the network structure as well as of its protocol functionality. Moreover, a fusion-based defense approach is suggested for detecting attacks in the Smart Grid according to the received feedback from individual nodes in the network. Each node in the network is required to communicate with a centralized fusion center to transfer its observations, through the help of the needed communication protocols. The paper emphasizes that deliberate attacks may be aimed to only a specific subset of nodes of the Smart Grid, and consequently feedback from all nodes is extremely important for accurately detecting these attacks. A game-based theory analysis is afterward provided in which the adversary is treated as one player and the protector as another. According to the concept that the adversary plans to violate the most critical nodes, the defense master plan is to ensure that timely local observation by distinct critical nodes, and following communication of findings to the centralized fusion center, are absolutely necessary.

The significant operations of the Smart Grid like error detection and event location estimation are depend heavily on accurate timing information. Well-known example of the attacks that could target timing information in the Smart Grid system is a Time Synchronization Attack (TSA). Due to this attack, three applications of phasor measurement units (PMU) are affected, namely voltage stability monitoring, transmission line fault detection, and event localization [37].

In [38], the authors introduce the effects of Denial-of-Service (DoS) attacks on load frequency control (LFC) of Smart Grids. Unlike the existing works, the authors consider the problem of how DoS attacks affect the dynamic performance of a power system. The data of the Smart Grid that measured through a remote terminal is dispatched to the centralized control centers. The DoS attack can remarkably affect the operations of the Smart Grid, if the communication channel that connected these sensors to the control center is attacked, i.e. sensors unable to deliver messages to the destination. The attacker launches such an attack by jamming the channel through inserting large numbers of packets. The power system is depicted as a linear time invariant model. For a switched linear system, a DoS attack is identified if the calculated Eigenvalues for the system matrix fall outside the unity circle.

## **2.7 Summary**

Cyber attacks that target the infrastructure of the Smart Grid system do not have an impact on the consumer alone, but also affect the business of the electricity utility. There are many threats against the Smart Grid system, which may give rise to attacks based on the profit they will bring to the attacker. Five distinct classes of cyber attacks were studied and

analyzed to facilitate the identification and analysis process. The proposed mitigation techniques which aim to defend against all such attacks have also been studied and listed in this chapter. Smart Grid security is still in its infancy, so a large-scale research work is still required to block the most exploitable threats and holes within the Smart Grid security system without affecting the consumers through deployment of strong security controls and constraints

## CHAPTER 3

### DETECTING SMART METER COMPROMISE

#### ATTACKS THROUGH NEIGHBORHOOD AREA METER

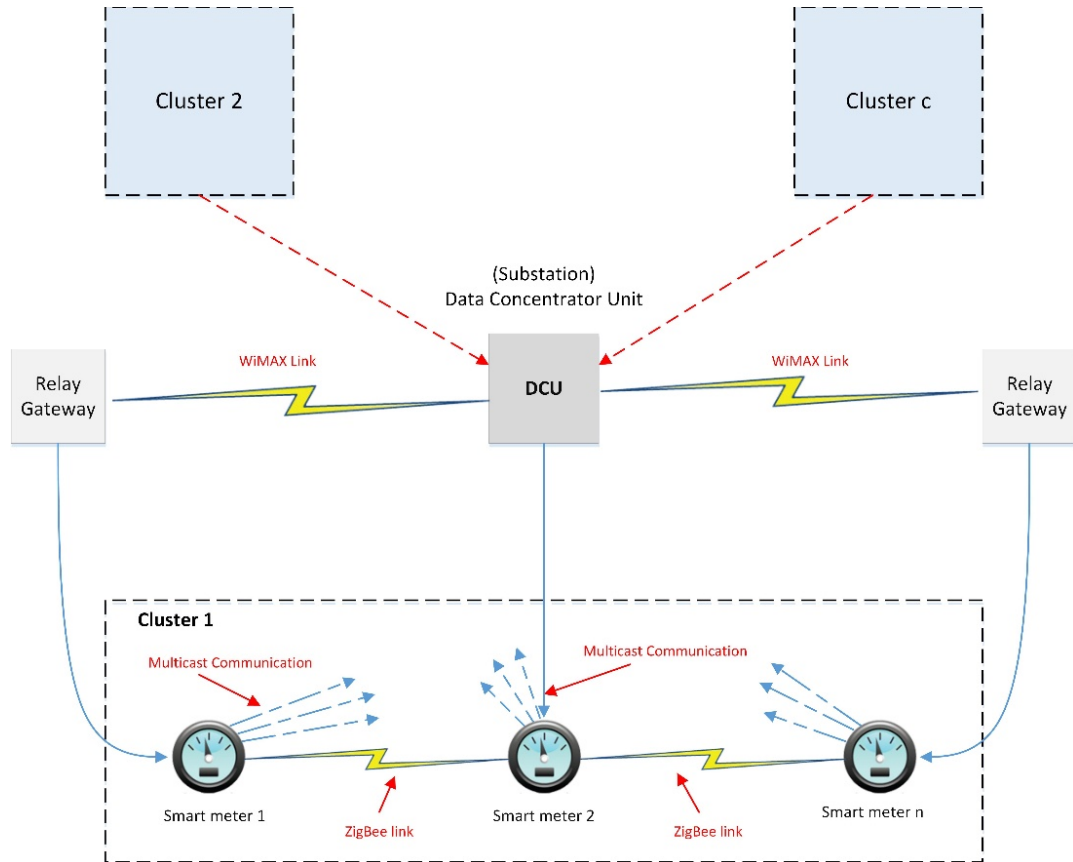
##### CLUSTERING

Conventional intrusion detection systems (IDs) are not easily integrated into the Advanced Metering Infrastructure (AMI). An AMI is not restricted to backend IP-based networks but rather constitutes, in a mesh-like structure, an interconnection of multiple smart grid devices. For this reason, it may not suffice to have a single front-end intrusion detection system which will both protect an entire neighborhood network while at the same time identifying anomalous network traffic. Furthermore, extensive AMIs are in operation the world over, each deploying millions of smart meters equipped with computerized systems which are all potential targets of malicious actors. Compromising a smart meter may jeopardize not only the particular household, but also the whole neighborhood network and perhaps the utility provider's core network, too. Of all the malicious attacks directed against the AMI, it is *Energy Fraud* which is of the greatest concern. *Energy Fraud's* principle point of entry for the launch of its attacks is the compromise of the smart meter with a view to manipulating the readings which are relayed to its service provider. Installation of rogue scripts on the smart meter by means of penetration through its unpatched software and/or firmware is one method an adversary may use to compromise a

smart meter. Additionally, such vulnerabilities may be the target of remote attacks via the Internet or through a Wi-Fi or ZigBee connection. The adversary may also be motivated to disrupt service, steal sensitive information, and exploit the communication infrastructure for the purposes of launching resource exhaustion attacks, such as Distributed Denial of Service (DDoS) attacks. Malicious attacks against smart meters not only allow interference with energy data, but high bandwidth attacks, such as DoS can be launched against other smart grid devices by compromised smart meters.

In this chapter, we propose a novel distributed information sharing mechanism to perform localized intrusion detection within pre-defined clusters of smart meters. Deployment of this scheme (Fig. 16) effectively reduces the data processing overhead which centralized intrusion detection systems operating at the utility provider facility have to absorb. This scheme operates through a system of collaborative sharing between smart meters of the neighborhood or cluster. Smart meters exchange information at fixed time intervals, assuming loose time synchronization. Exchanging local electricity usage readings between peer meters gives leverage to localized intelligence on observed network traffic by the smart meters relayed to the concentrator unit, thereby also facilitating the holistic visualization of network traffic activity. The goals of this chapter can be summarized as follows:

1. Proposed mechanism for the formation of clusters of smart meters within a neighborhood area network,
2. Design of a scheme to support timely exchange of smart meter readings between smart meters within a cluster.



**Figure 16: Assumed topology for the clustered advanced metering infrastructure (AMI)**

The rest of the chapter is organized as follows: section 3.1 provides a background including a literature survey of existing security frameworks and techniques for the AMI; a review of advanced metering infrastructure, AMI, and its unique characteristics and capabilities; an attack tree for *Energy Fraud*; and the scheme notations. In section 3.2, the attacker model for AMI is provided. The attack detection scheme for meter compromise attacks is elaborated upon in section 3.3.



## 3.1 Background

### 3.1.1 Related Work

The required technical proficiencies for securing an illegitimate access to the smart meter device are easily achievable and cause an imminent threat to the security of the entire Smart Grid system. S. McLaughlin et al. 2010, concentrated on the energy fraud attacks. They constructed an *archetypal attack tree* to show the methods and motives of adversaries against the Advanced Metering Infrastructure AMI. The authors identified the main techniques of carrying out an energy fraud attack through a smart meter. This includes deleting the meter's storage, intercepting the communication channel between the meter and backend server, injecting fake data into the network, tampering with the meter's calculation, and physically hacking the meter's memory [39].

Y. Tanaka et al. 2012, proposed a security mechanism for the communication between HAN devices and the smart meter. The data integrity is ensured by the use of public key certificates, thus the origin authentication among all the communicating entities for a secure registration process was also ensured [40]. J. Kamto 2012, proposed a public key-based technique for a secure data transmission between the smart meters and the relay gateway within the smart grid infrastructure. Because of this, intermediate nodes that may work for forwarding the data in multi-hop topologies are incapable of deciphering the critical electricity reading that is transiting through them [41].

M. Nabeel et al. 2012, proposed a security mechanism using Physically Unclonable Functions (PUF), to secure the communication channels within the AMI. The utility provider authenticates a smart meter device via a hardware component which is embedded

in the smart meter. This mechanism hinders key leakages from weak smart meter architectures. Even so, the disruption of the entire smart meter continues unresolved [42].

N. Saputro et al. 2012, proposed an approach for securing data authentication and privacy preservation via cryptographic keys. Such an approach will protect the traffic of a smart meter from any malicious attacks [43] [44]. Several guidelines were provided by D. Grochocki et al. 2012, to ensure the security of AMI. This includes a mechanism to observe all in and out network traffic and detect malicious attacks via a centralized Intrusion Detection System (IDS), and an approach to monitor transiting traffic by embedding sensor hardware in the smart meter, taking into account that a smart meter acts as a relay for network traffic. Furthermore, the authors also propose a hybrid of both a centralized detection sensor and distributed sensors within the meters for detecting malicious traffic within an AMI [45]. Y. Zhang et al. 2011, proposed a distributed intrusion detection system for the smart grid, called SGDIDS. This system made up of an analyzing module (AM) located at each of the three layers of the Smart Grid communication infrastructure: Home Area Network (HAN), Neighborhood Area Network (NAN), and the Wide Area Network (WAN). The algorithms used in this intelligent technique for detection and classification of malicious data, are Artificial Immune System (AIS)-based and Support vector machines (SVM) [46]. H. Li et al. 2010, proposed a scheme for verifying message based on compressed meter readings [47].

R. Berthier et al. 2010, suggested an approach to deal with intrusion threats aimed at the advanced metering infrastructure (AMI), by use of a specification-based intrusion detection system to yield higher accuracies. Such systems were found to introduce significant overheads and are costly to implement [48]. R. Berthier et al. 2011, proposed a

specification-based intrusion detection system that carry out real time screening of the traffic between meters and access points. A set of rules for monitoring application behavior were defined by the authors to ensure smooth system operations in the presence of malicious meters and the threat of DoS (Denial of Service) attacks [49]. Z. Baig, proposed a lightweight pattern matching scheme for detection of attacks in the Smart Grid. The algorithm that used in technique is the graph neuron (GN) to identify malicious or misbehaving devices in the network and to take appropriate measures, which may include replacement of the malicious device [50].

### **3.1.2 AMI Review**

Within the Smart Grid (SG), Advanced Metering Infrastructure (AMI) plays a vital role as it is modernizes the way electricity works by replacing the old mechanical meters with smart meters which enable two-way communication between the customers and service providers. Aside from reading the meter data remotely, with the AMI customers can also perform some customized control like programming the electric appliances to maximize their efficiency and implement a fine demand response [51]. In addition, the real-time data collected from the smart meters help the utility companies to provide a faster diagnosis of outage and improve the reliability of the entire grid by avoiding line congestion and generation overloads [52].

The advanced metering infrastructure (AMI) is composed of smart meters, communications networks and data management systems. Fig. 17 shows the simple building blocks of AMI. The households are equipped with smart meters for collecting data in a time-based way. This collected data is sent back to the utility through a number of commonly different communications networks available like Broadband over Power Line

(BPL), Power Line Communications (PLC), Fixed Radio Frequency (RF) networks, and public networks (e.g., landline, cellular, paging). For the utility to get the information in a useful form, the transmitted data received by AMI's host system should be analyzed, stored, and managed [53].

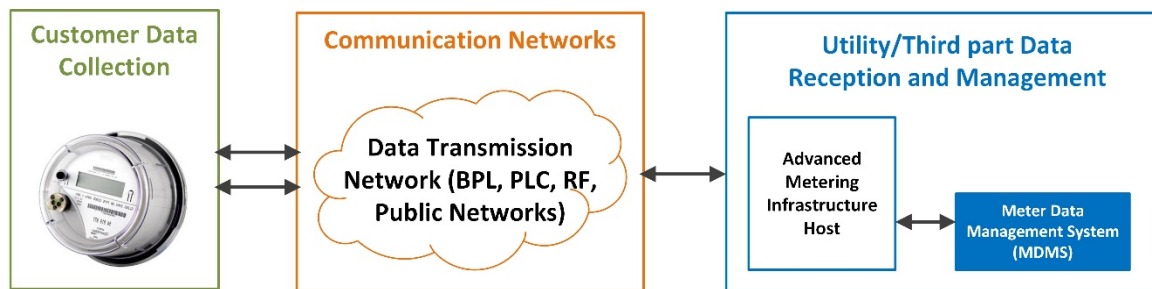


Figure 17: Simple building blocks of AMI

AMI has introduced a huge increase in threats to the power metering. The unique characteristics of AMI, such as complex network structure, resource-constrained smart meter, and privacy sensitive data extend the attack surface and introduce many vulnerabilities for new cyber-attacks. *Energy fraud* is one of the big concerns related to the AIM. A World Bank report finds that up to 50% of electricity in developing countries is acquired via theft [54]. It also has been reported that over 6 billion dollars each year are lost because of *Energy fraud* in the United States alone [55]. In 2009, the FBI reported a wide and organized *Energy fraud* attempt that may have cost a utility up to 400 million dollars annually following an AMI deployment [56]. In Canada, BC Hydro reports \$100 million in losses every year [57]. Utility companies in India and Brazil incur losses around \$4.5 billion and \$5 billion respectively due to electricity theft [58, 59]. There is even a video which shows how to crack the meter and cut the electricity bill in half on YouTube

[60]. As a result, the energy theft issue has become one of the most important concerns which impedes the growth of AMI.

Smart meter is defined as a digital electric device comprise CPUs, communication interfaces, and storage unit. It is a key component of the smart grid infrastructure SGI, connecting households to the utility providers. The four basic functions performed by a smart meter that involving to power controlling are: *a)* the recording and tracking of demand, *b)* the events of power logging, e.g., outages, *c)* the conveyance of electricity usage and information of logging events to the utilities, and *d)* the exchange of control messages, e.g., remote disconnect, managing smart appliances, etc. [61].

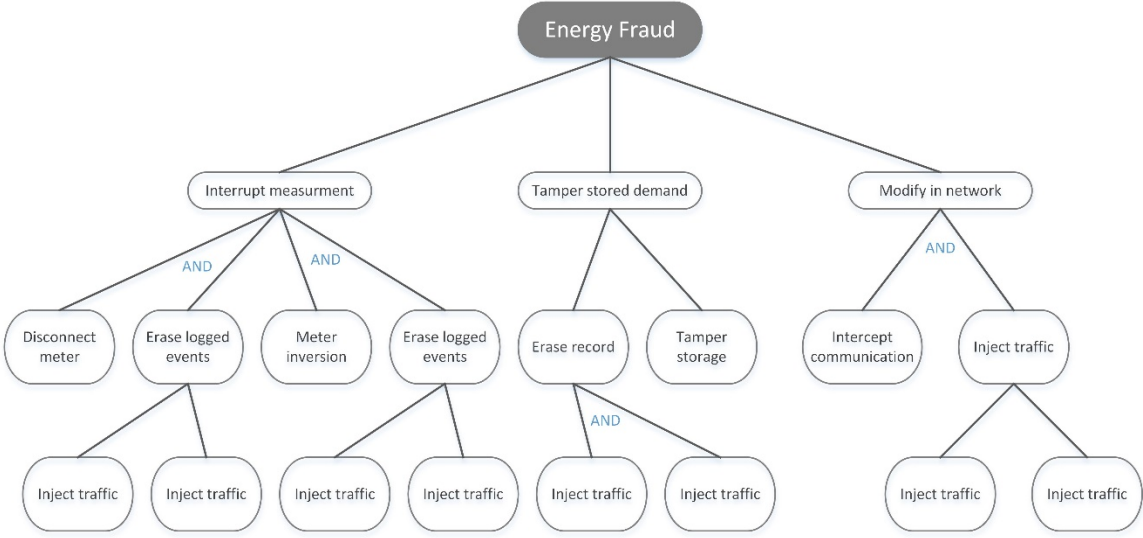
### **3.1.3 Energy Fraud Attack Tree**

As mentioned, *Energy Fraud* is one of the most important concerns related to the AMI. In order to understand strategies for *Energy Fraud* in AMI, we use the modeling-based technique of security attack trees [62]. In this attack tree, “*Energy Fraud*” is set as the adversary’s ultimate goal which is then recursively broken down into sub-goals until a number of likely attacks plans are arrived at and no more attacks can be divided into sub-attacks [61]. The root node of the attack tree represents the single goal of all the attacks. In our case, this goal is *Energy Fraud*. All the nodes below the root node represent a group of sub-goals that describes different procedures towards the root goal. The exact attacks that must happen for the goal to be achieved are represented by the leaf nodes, which have no successor. The logical operators AND and OR are used to augment paths to the root goal and decide whether one or all of the children in a given internal node need to be completed to achieve the goal [61].

Fig. 18 presents the attack tree for *Energy Fraud* in AMI. As shown, the single requirement for *Energy Fraud* is the tampering of the electricity readings and this can be done in three ways: *a)* while it is registered, *b)* while it is at rest in the smart meter, and *c)* as it is passing through the network. The following is a detailed discussion of each of these ways.

- *Disturb measurement:* this is the first class of attacks, wherein an attacker attempts to prevent the smart meter from accurately recording the electricity consumed. This attack is the only one that already existed for the traditional meters, whereas the other two categories are limited to AMI. To launch this attack, there are two ways: “disconnect meter” and “meter inversion”. It is needful to wipe off the logged events, which point out reverse energy flow or outage, in order not to be retrieved by the utility company.
- *Tamper stored demand:* this kind of attack violates the data stored in the smart meter to achieve *Energy Fraud*. As mentioned, the smart meters store a large range of data. This includes tariffs for Time-of-Use (TOU) pricing, logs for both physical events and executed commands, and recorded network commands. As all of the smart meter’s behavior is controlled by the contents of its storage, tampering with this stored content gives an adversary complete control over its operations. Tampering with the stored demand by erasing relevant records, like *audit logs* and *recorded total demand* requires an administrative interface access through extracting the meter password and reset net usage.
- *Modify in network:* this class of attack involves injecting erroneous values into communication between smart meters and utility companies. Launching such an attack needs two discrete types of actions: intercept the communication and inject

or modify the traffic between meter and utility. After successfully intercepting the link between smart meter and the utility, an adversary needs to launch “man-in-the-middle” or “meter spoofing” attacks in order to send false data and event logs [63].



**Figure 18: Attack tree for Energy Fraud**

As shown in Fig. 18, we note that this attack tree is only an example to record the possible attacks that may be launched by an adversary to violate the AMI. This tree could be extended to accommodate more attack sub-trees by considering more attack strategies and techniques of attackers in practice. Recent research on the AMI security and privacy preservation [64-67] would also benefit the construction of the attack tree.

### 3.1.4 Notations

The notations used in this chapter are listed in Table 5

Table 5: Notations of the scheme

---

$mac$	Message Authentication Code
$K_B^A$	A secret key shared between two entities $A$ and $B$
$m_p$	Electricity usage data for node $p$
$\Delta_i$	The time epoch with label $i$
$A$	Sender (Smart Meter)
$B$	Receiver (Data Concentrator Unit)
$w$	The minimum total time required for exchange of all smart meter readings within a cluster
$UB$	The upper threshold of energy usage
$LB$	The lower threshold of energy usage
$N$	The total number of smart meters in AMI
$c$	The total number of clusters

---

## 3.2 The Attack Model

Among all the possible attacks launched by an adversary to violate AMI, one attack category that may pose a serious threat to the AMI is a meter compromise attack, wherein a smart meter is controlled by the attacker, with the intent of committing *Energy Fraud*. In general, there are different kinds of attackers with various motivations who are attempting to violate the AMI. The detailed analysis of the attackers provide a better understanding of their attack techniques. Specifically, there are three types of attackers who are motivated to commit *Energy Fraud* [68].



- *Customer:* It is the energy consumers who are the most likely to defraud the energy supplier. The means of interference and the motivation to tamper with conventional meters are highly individual in nature. It is, for example, the case in developing countries that people defraud energy companies because of low quality infrastructure, poverty, and irregularities in the metering systems.
- *Organized crime:* In this case, the perpetrator is motivated by the monetization of energy fraud. Because AMI is so complex, customers are likely to assign to professional hackers the task of creating malicious software/hardware that compromises smart meters. This kind of hacker will exploit certain design aspects of AMI systems, such as the according of the same password to multiple meters, and thereby capitalize on the cracking of a single smart meter.
- *Utility company insiders:* Generally, utility company insiders are implicitly trusted when dealing with analog meters and the same goes for AMI. However, in order to avoid deliberate misoperation or attacks by malicious utility company employees, it is advisable that the utility company put in place robust customer and group management systems which ensure internal control mechanisms, such as separation of duties.

In this work, we use the smart meter compromise attack in which the adversary's aim is to get compromised smart meters to feed incorrect readings to the data concentrator unit (DCU). Where the communication topology is centralized (see Fig. 19) and all smart meters communicate with the DCU at exact time intervals, compromised smart meters are bound to report incorrect readings. Energy fraud may be perpetrated through the communication to the DCU of a reduced usage reading, thus bringing financial benefit to the household where the compromised meter is located. Should the perpetrator's goal be

the infliction of financial loss on the utility provider's customer base, he may also configure a compromised meter to communicate inflated usage data. The outcome of such an attack is the undermining of consumer confidence which inevitably leads to an erosion of the client base at the DCU.

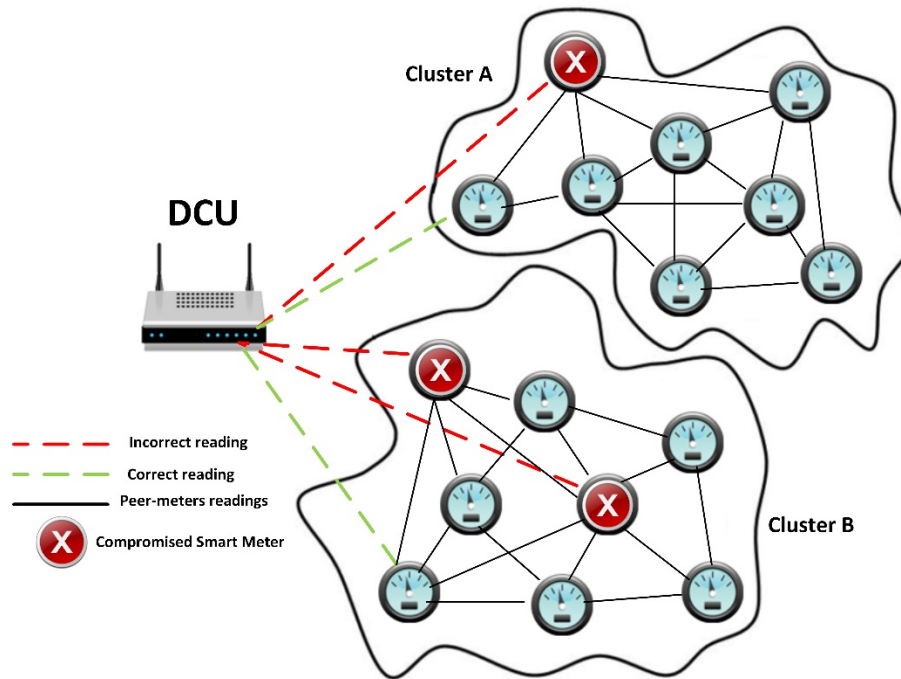
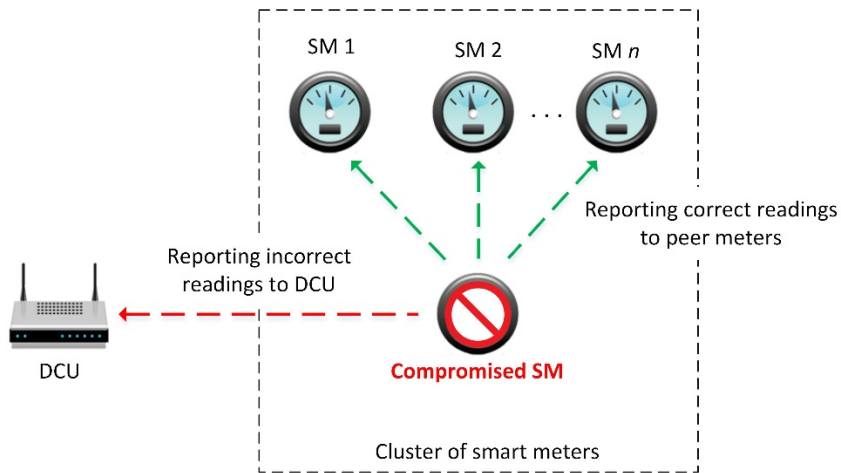


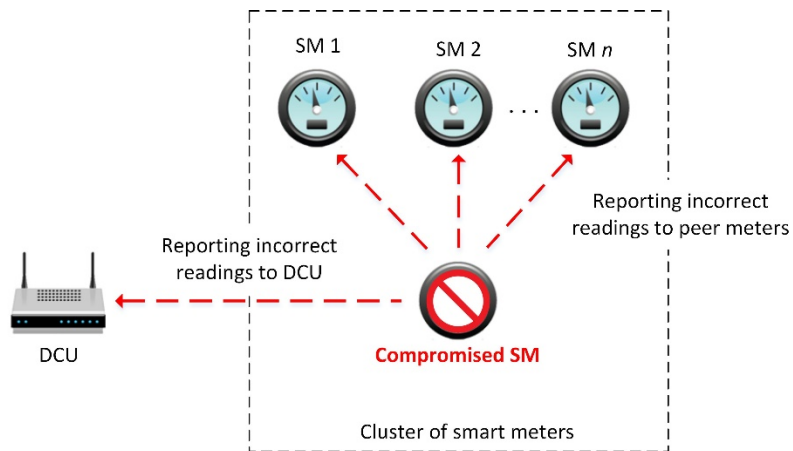
Figure 19: The attack model where the communication topology is centralized

In the proposed scheme, peer smart meters within predefined clusters of operation within the AMI exchange their respective readings during a set operating period. There is a regular exchange of local data between peer smart meters for the purpose of verifying that their individual readings are compatible with the usual patterns of readings one would find during normal smart meter operations.

In such a topology, compromised smart meters can be expected to behave in one of two ways: a) a compromised smart meter (see Fig. 20) may report correct reading (i.e. readings within the upper bound UB and the lower bound LB intervals) to meters sharing the same cluster and report incorrect readings to the DCU, thereby escaping detection, and b) the compromised meter may relay the same false readings to both its peer meters and the DCU (see Fig. 21).



**Figure 20: A compromised smart meter sending correct readings to peer meters and incorrect readings to DCU**



**Figure 21: A compromised smart meter relay the same false readings to both its peer meters and the DCU**

If  $p$  is the probability that a peer smart meter engaged in attack detection receives a true message from a compromised smart meter alluding to the attack and  $x$  is the ratio of compromised smart meters not telling the truth (i.e. meters which deceive their peer meters by relaying to them true readings while conveying false ones to the DCU), then the probability of an attack remaining undetected by the DCU is given by:

$$P = (1 - p)^x \quad (1)$$

Where,  $x < \frac{N}{c} - 1$ .

The value of  $p$  approaches unity for the first attack scenario, in which compromised smart meters relay true readings to both peer meters and the DCU.

A sophisticated and cunning adversary may send two separate and different readings to the DCU and to the peer smart meters. A normal reading forwarded to the peer smart meter will allow the compromised smart meter to operate covertly without raising any alarms within its cluster of operation. Meanwhile the compromised smart meter will relay the fabricated electricity usage reading to the DCU. The adversary succeeds hereby in achieving his goal of perpetrating energy fraud or undermining consumer confidence in the utility provider. In such a scenario, the probability of an attack remaining undetected by the DCU is given by:

$$Q = q \cdot (1 - p)^x \quad (2)$$

Where,  $q$  is the probability that a true message is relayed by a compromised smart meter to the DCU. The higher the number of compromised meters sending two different messages to both the DCU and the peer meters, the lower the probability of the attack being detected.

### **3.3 Attack Detection Scheme**

The attack detection scheme proposed in this chapter is a distributed information sharing system whose aim is to detect intrusion within predefined clusters of smart meters in AMI: the scheme works to detect attacks by an adversary on smart meters within a cluster specified in neighborhood area networks. It is proposed that individual clusters of smart meters be specified at the initialization of the network (Fig. 16) based on their physical coordinates within a neighborhood area network. These coordinates generally remain unchanged throughout, save where a specific device fails or a security breach occurs. For the purpose of ascertaining that the minimum number of peer readings necessary for attack detection is operational at any point in time, the logical clustering of smart meters within a neighborhood area network becomes a key component of the scheme we propose. The principle reason for using clusters of meters for attack detection is twofold: the compromise of a smart meter is detected within the cluster, thereby preempting or reducing the overhead associated with information sharing at the wide area network level; the effects on the attack detection accuracy will be limited within the cluster, should a meter fail or be compromised.

#### **3.3.1 Assumption**

The AMI can have a few hundred to several thousand smart meters in operation in a neighborhood area network at any given point in time. All smart meters are equipped with wireless communication capability based on the ZigBee standard. Typically a smart meter is capable of wireless transmission to and reception from the DCU over distances of about 1,000 meters, with the bit error rate increasing as the distances grow. The application of a

secure key management protocol [69] is crucial to protect the confidentiality of all messages exchanged between the smart meters at the peer level, or between the smart meters and the centralized DCU. The assumption is made that all smart meters of a particular cluster are loosely time-synchronized, so as to guarantee the freshness of messages exchanged to prevent message replay attacks. Furthermore, given that the proposed attack detection scheme relies on timely communication between the smart meters, synchronization is of vital importance.

As part of the detection scheme, communication takes place either between a smart meter and the data concentrator unit, or between two smart meters. The message formats are given by:

$$A \longrightarrow B: \text{mac} \{m_p, K_A^B, \Delta_i\} \quad (3)$$

where,

*mac*: Message Authentication Code

$K_A^B$ : Secret key shared between two entities A and B

$m_p$ : Electricity usage data for node  $p$

$\Delta_i$ : Time epoch with label  $i$

$A$ : Sender (Smart meter)

$B$ : Receiver (Data Concentrator Unit)

### 3.3.2 The Scheme

The attack detection scheme, as illustrated in Algorithm 1, consists of the following four phases of operation.

---

#### Algorithm 1 Meter Compromise Attack Detection Scheme

---

##### 1. Initialization

Define empirical upper and lower bounds ( $UT$  and  $LT$ ) based on an initial run of the AMI for gathering normal electricity usage data.

##### 2. Peer Usage Data Exchange

For each node  $j \in N$  do:

Report household electricity usage reading to peer meters of the cluster.

##### 3. Attack Detection at each node of the network

At each node  $j \in N$  during a time epoch  $\Delta_i$ :

**for**  $k=1$  to  $\frac{N}{c} - 1$  **do**

**if**  $electricity\ usage\ (node_k) < thres(LB) \ ||$

$electricity\ usage\ (node_k) > thres(UB)$  **then**

        Identify  $k$  as compromised

        Report the message ( $m = "k\ is\ compromised"$ ) to DCU:  $m, mac(\Delta_i, k_j^{DCU}, m)$

**end**

**end**

##### 4. Meter-to-DCU Communication

At the DCU:

**if**  $\exists\ node_m\ s.t.\ number\ of\ complaints\ received\ for\ node_m > \frac{N}{2*c} - 1$  **then**

    Confirm  $node_m$  as compromised

**end**

---

*Initialization:* At the network initialization time, which is executed once, smart meters are pre configured with node IDs of other smart meters that constitute the same cluster. The communication between the smart meters and the data concentrator unit is done at fixed

intervals of time. The time window length is given by  $w < \Delta$ , where  $w$  is defined as the minimum total time required for the exchange of all smart meter readings within a cluster for attack detection. This quantity is derived through the averaging of results obtained from several simulation runs for a network with given size and given geographical dispersal of smart meters in a neighborhood area network. The length of the time window is a function of the total number of smart meters that constitute a cluster, as well as the communication standard used (ZigBee in our case). In addition, upper and lower thresholds of energy usage given by  $UB$  and  $LB$  have constant values which are stored within each smart meter of a given neighborhood.

*Usage Data Exchange:* Household electricity usage readings are transmitted by each smart meter to every other peer smart meter within its respective cluster of operation. The communication takes place in each time epoch  $\Delta_i$ .

*Attack Identification:* For an AMI with  $N$  smart meters, and  $c$  clusters, the estimated number of messages that a smart meter will receive within a given  $\Delta_i$  is equal to  $\frac{N}{c} - 1$ . For a given time epoch, if a smart meter receives less than  $\frac{N}{c} - 1$  messages, a smart meter compromise is suspected, and accordingly reported to the data concentrator unit. On the other hand, if all peer smart meter readings are received by a smart meter  $j$ , then  $j$  proceeds with its analysis of the smart meter readings. This analysis comprises the comparison of electricity usage data received from other peer smart meters, with predefined thresholds  $UB$  and  $LB$ . An anomaly is suspected when:

$thres(LB) > usage(household_k)$  or  $usage(household_k) > thres(UB)$ , where,  $thres(LB)$  and  $thres(UB)$  are empirical estimates on the minimum and maximum energy



consumption readings of households within a given neighborhood cluster, defined during network initialization, and  $k$  is a peer smart meter of meter  $j$ .

*Meter-to-DCU Communication:* Smart meters are configured to communicate with the data concentrator unit regularly to communicate household usage readings. An anomaly is detected by the data concentrator unit if the usage data reported by a smart meter for a suspicious meter  $k$  is beyond the upper and lower thresholds of consumption. The communication between the smart meters and DCU is resistant to message replay attacks since a message authentication code is included with each transmitted message.

The overhead associated with maintaining multiple clusters of smart meters within an AMI can be quantified as follows: a large number of clusters in the AMI will reduce the overhead associated with intra-cluster meter-to-meter communication as fewer meters will constitute each cluster. However, in such a scenario, the analysis of meter compromise attacks is done granularly within each cluster, with less communication overhead associated with meter-to-meter message transmission during each epoch of time  $\Delta_i$ .

On the contrary, a smaller number of clusters will reduce the associated overhead with generating and maintaining cluster information at the DCU during *Initialization*. DCU will analyze data coming from a larger number of meters of a cluster, thus increasing the likelihood of identifying the attack. The overhead associated with data communication between individual smart meters of a cluster for such large cluster sizes will be higher. The total overhead as a function of the cluster sizes can be described as follows:

$$CO_{total} = c \cdot \left[ \left( \frac{N}{c} \right) \cdot CO_{meters} + p \cdot \left( \frac{N}{c} - 1 \right) \cdot CO_{dcu} \right] \quad (4)$$

Where,

$N$  is the total number of smart meters in an AMI

$c$  is the total number of clusters

$CO_{meters}$  is the average overhead associated with data communication between the smart meters of a cluster

$CO_{dcu}$  is the average overhead associated with data communication between the smart meters and the DCU

$p$  is the likelihood that a smart meter correctly identifies an anomalous peer reading

If for  $\frac{N}{c} - 1$  readings received by a smart meter during a given  $\Delta_i$ , the likelihood of a meter compromise is  $p > 0$ , then the overhead associated with transmitting this particular anomalous finding to the DCU is as defined above. On the contrary, if none of the smart meters within a cluster are compromised, the overhead associated with data communication with the DCU reduces to zero.

As can be seen from Algorithm 1, individual smart meters of a cluster exchange their respective electricity usage readings with peer meters during each of time epoch  $\Delta_i$ . A node

$k$  is considered to be compromised by a smart meter, if its observed readings are beyond the stipulated bounds of usage (i.e. less than  $thres(LB)$  or greater than  $thres(UB)$ ). Any anomalous reading is considered suspicious by the smart meters within the clusters, and is conveyed to the DCU. During each epoch of time  $\Delta_i$ , if the total number of anomalous confirmations against a node  $k$  received by the DCU is greater than  $\frac{N}{2*c} - 1$ , then node  $k$  is confirmed as compromised.

## CHAPTER 4

### PERFORMANCE ANALYSIS

In this chapter, we provide a detailed performance analysis of the simulation that was performed for varying simulator parameter values. The proposed scheme was tested through a discrete event simulation, written in JAVA code, of varying neighborhood area networks of an AMI. The results were averaged over 100 runs, and these helped quantify the detection rate, false alarms and the communication overhead for varying numbers of nodes in the network, for varying cluster sizes, and for four different levels network compromised by adversary and four different packet loss/drop rates. Data communication between the smart meters was assumed to follow the Poisson distribution.

The values of upper and lower thresholds do not have an effect on the accuracy of attack detection. Based on the empirical household electricity usage readings of a neighborhood, these values will vary.

For the accurate detection of malicious smart meters, all such smart meters must communicate false readings to their respective peer meters of a cluster, while relaying accurate readings to the data concentrator unit (DCU). However, this may not always be the case. We have therefore simulated four different levels of attacks representing four varying attacker behaviors, as follows:

L1: 25% of compromised meters ( $r$ ) convey false readings to the DCU, whereas the remainder 75% convey correct readings. L2: 50% of the compromised meters convey false

readings to the DCU, with the remainder 50% conveying correct meter readings. L3: 75% of compromised meters convey false readings to the DCU, with the remainder 25% conveying correct meter readings. L4: 90% of compromised meters convey false readings to the DCU, with the remainder 10% conveying correct meter readings.

In order to test the effect of varying cluster sizes on the attack detection and false alarm rates we performed simulations for  $c$ . The size of the clusters was varied from 2% to 100% of the total number of meters in the neighborhood ( $N$ ), for each cluster size the attack detection rate is plotted against the number of compromised smart meters  $x$  (see Fig. 22).

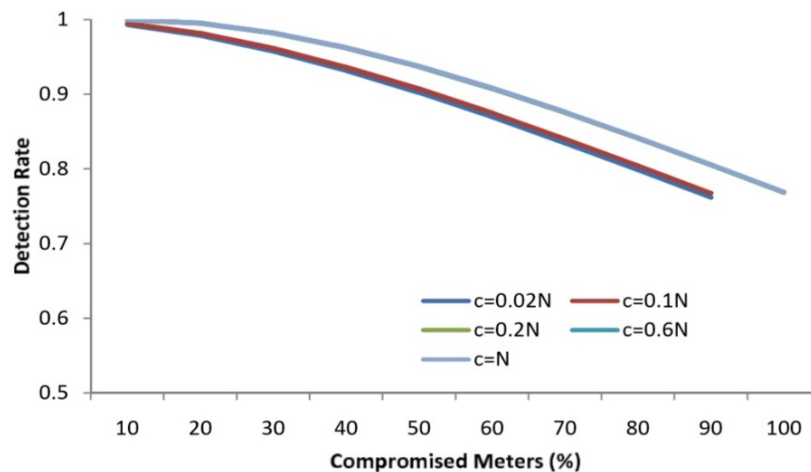


Figure 22: Attack Detection Rate for Varying Cluster Size

The attack detection rate was found to degrade with increasing numbers of compromised meters (Fig. 22). A corresponding increase in the number of compromised meters remaining undetected (i.e., false negative rate) is observable through (Fig. 23). The detection rate is close to the 100% mark for zero compromised meters, thus showing the effect of the detection scheme in distinctly identifying meter compromise attacks.

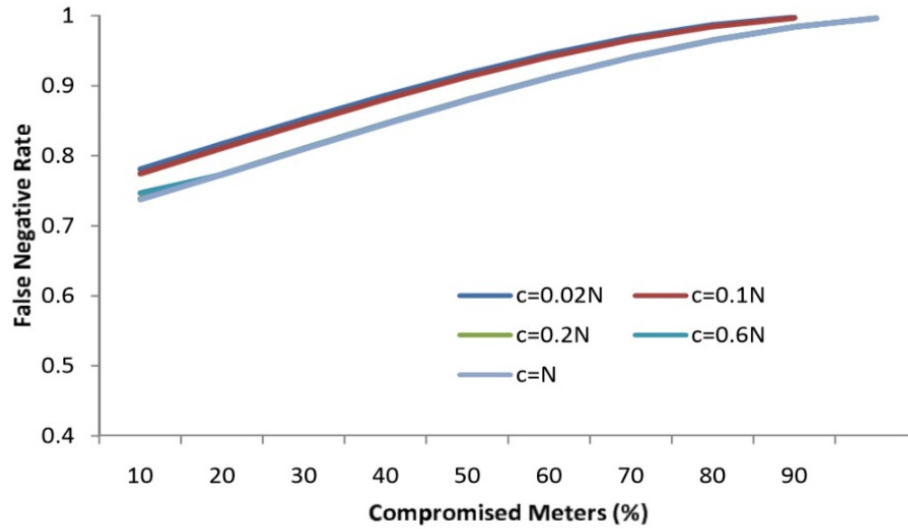
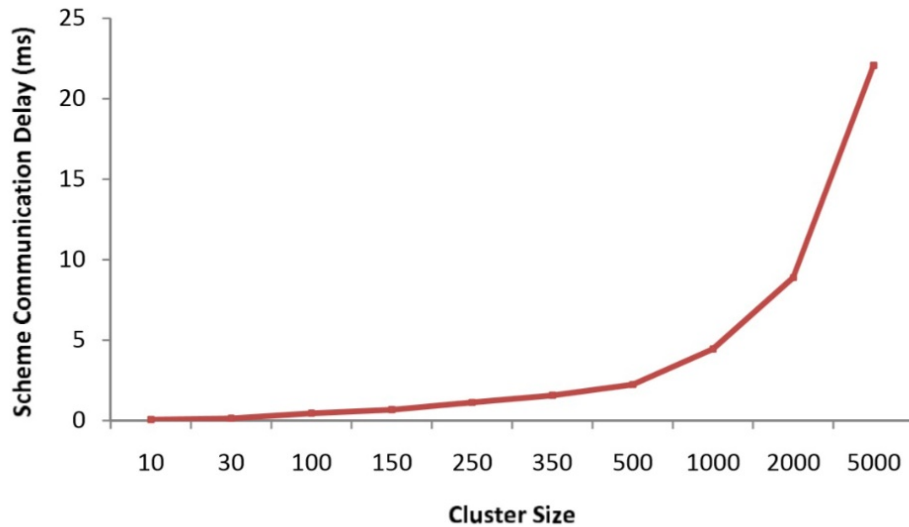


Figure 23: False Negative Rate for Varying Cluster Size

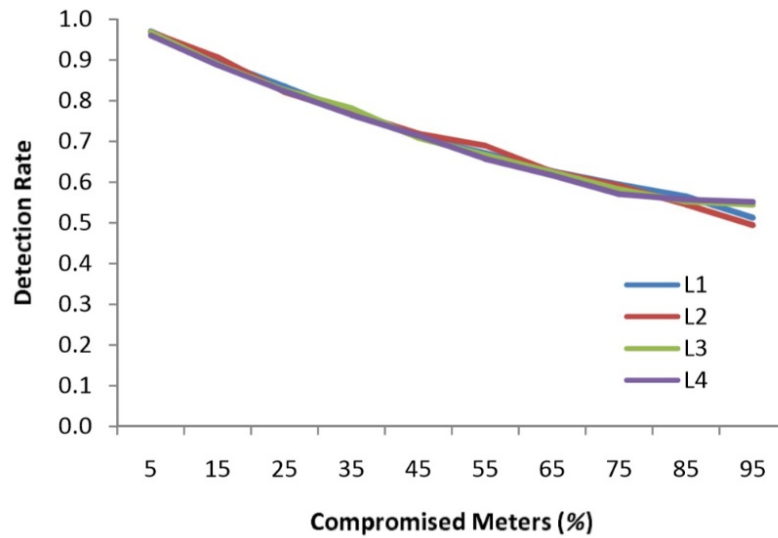
Larger numbers of clusters yield higher detection rates even in the existence of a relatively great number of compromised smart meters ( $c = N$  and  $r \approx 100\%$ ). For instance, with  $c=N$  clusters operational in the network, the attack detection rate is close to 80% even for  $x > 90\%$ . On the other hand, with fewer numbers of clusters in the network, a larger number of smart meters are to be monitored by each smart meter of the cluster, and therefore, the attack detection rate is degraded. Increasing numbers of compromised smart meters in the network will degrade attack detection rate, for all values of  $c$ .

The total delay associated with communication between the smart meters is illustrated in (Fig. 24). Increasing number of smart meters in a cluster will lead to increasing delays. For a cluster of size  $N=1000$ , a delay of approximately 25ms is observed, whereas, for smaller cluster sizes, and with parallel execution of the attack detection process in all clusters, the delay is far less (lowest value reported being 0.2ms for a  $c=0.02N$ ).



**Figure 24: Communication Overhead Imposed by the Detection Scheme**

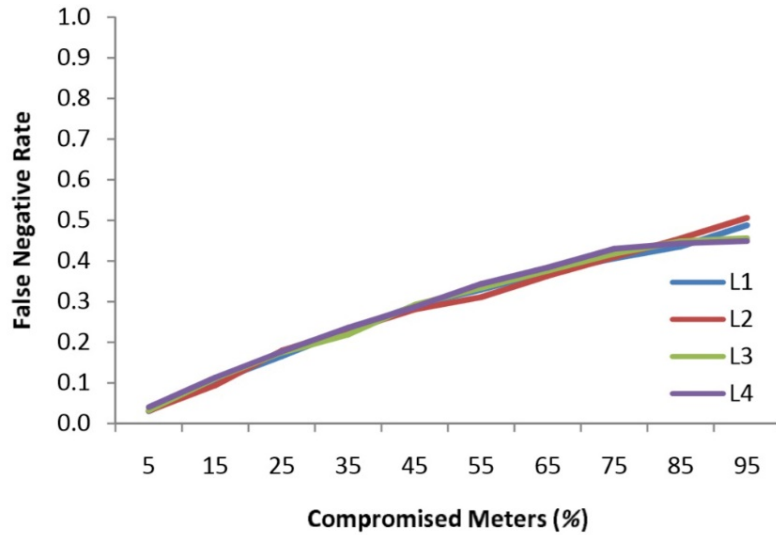
In (Fig. 25), we have simulated the effect of four different levels network compromised by adversary on the detection rate for the best cluster size (i.e.  $c = N$ ), and for varying numbers of compromised meters. As can be observed from the figure, for fewer compromised meters, the effect of varying adversary classes on the attack detection rate is not significant. A detection rate close to 100% is observed for all such cases. On the other hand, with increasing numbers of compromised meters, the detection rate degrades, with a mere 50% of attacks detected with 95% compromised meters. The variation between the different attacker classes is not significant in this case because despite having correct readings conveyed to the DCU, the existence of an enormous number of peer meters in a large network will ensure that there is a high likelihood of more than 50% of the meters in a cluster reporting a misbehaving meter to the DCU.



**Figure 25: Attack Detection Rate for Varying Numbers of Compromised Nodes with 4 Different Adversary Classes (N=1000)**

The false negative rates are also not overly affected with varying attacker behavior. (Fig. 26) illustrates how increasing numbers of attacker meters leads to increasing number of false negatives for the scheme. However, varying attacker behavior, as represented by the four adversary classes (L1-L4), do not affect the false negative rates significantly





**Figure 26: False Negative Rate for Varying Numbers of Compromised Nodes with 4 Different Adversary Classes (N=1000)**

From (Fig.27), we may observe that the detection rate is higher for larger networks, with N=1000 yielding a detection rate close to 100% with only 5% compromised meters. Reducing network size has an effect on the detection rates for smaller numbers of compromised meters. With 50% meters being compromised smaller networks have a degraded detection rate as opposed to larger networks; N=100 yielding a 67% detection rate as compared to a detection rate of 71% for N=1000. For larger networks, more smart meters report misbehaving meter activity to the DCU, and therefore, the detection rate improves.

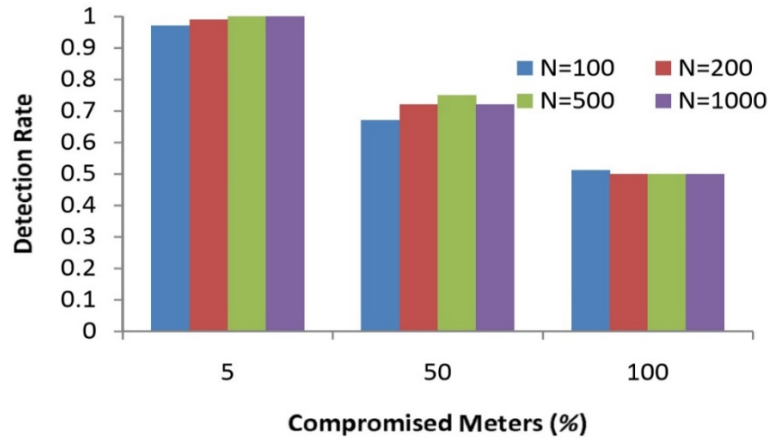


Figure 27: Attack Detection Rate for Varying Numbers of Nodes in a Cluster and Varying Attacker Ratios

The false negative rates for varying  $N$  and fixed  $c=N$ , is presented in (Fig. 28). For fewer compromised meters, the false negatives are comparable for all values of  $N$ . With 50% compromised meters in the network, larger networks yield lesser false negatives as opposed to smaller networks, at par with our analysis of the attack detection rate (Fig. 27). In addition, with a large number of compromised meters (95%), the false negatives are very high (nearly 51%) for all network sizes.

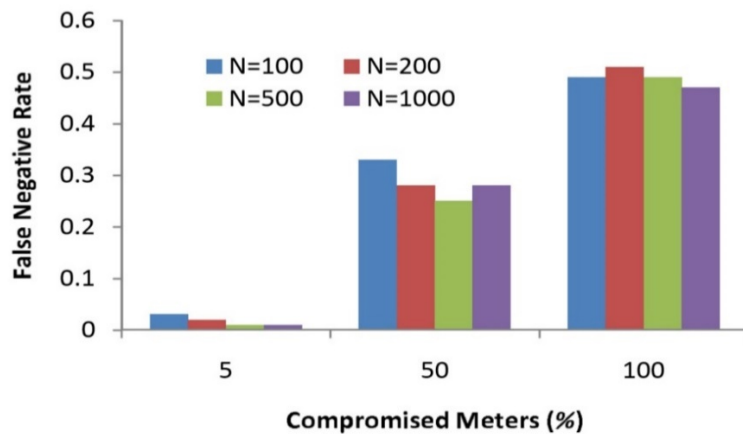


Figure 28: False Negative Rate for Varying Numbers of Nodes in a Cluster and Varying Attacker Ratios

Also in our scheme for the sake of accurate detection of compromised smart meters, each meter must receive  $\left(\frac{N}{c} - 1\right)$  message from its respective peer-meters of a cluster. However, this may not be the case all the time. For a given time epoch, a meter's reading may not reach to the intended peer-meter in a cluster, (i.e. a smart meter receives less than  $\left(\frac{N}{c} - 1\right)$  messages). Possibly this will happen due to a sudden high packet loss/drop rate or due to a malicious activity of the adversary in an attempt to making a large number of meters appear as malicious in a given cluster, then raising false alarms and disrupting the daily operations of an AMI. Because of this, we have therefore simulated four different packet drop rates as follow:

The 25% packet drop rate: 25% of compromised meters ( $r$ ) are fail to convey their readings to intended peer-meter in a cluster. The 50% packet drop rate: 50% of compromised meters ( $r$ ) are fail to convey their readings to intended peer-meter in a cluster. The 75% packet drop rate: 75% of compromised meters ( $r$ ) are fail to convey their readings to intended peer-meter in a cluster. The 90% packet drop rate: 90% of compromised meters ( $r$ ) are fail to convey their readings to intended peer-meter in a cluster.

Fig. 29 shows the attack detection rate for four different packet drop rates and (N=100) cluster size.

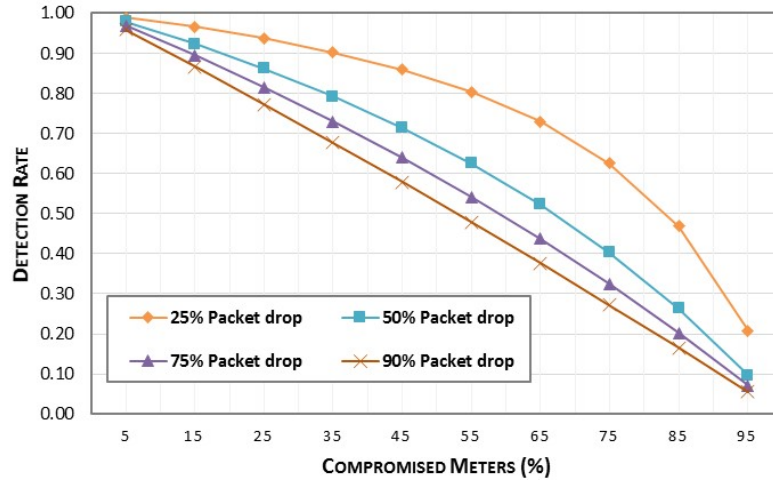
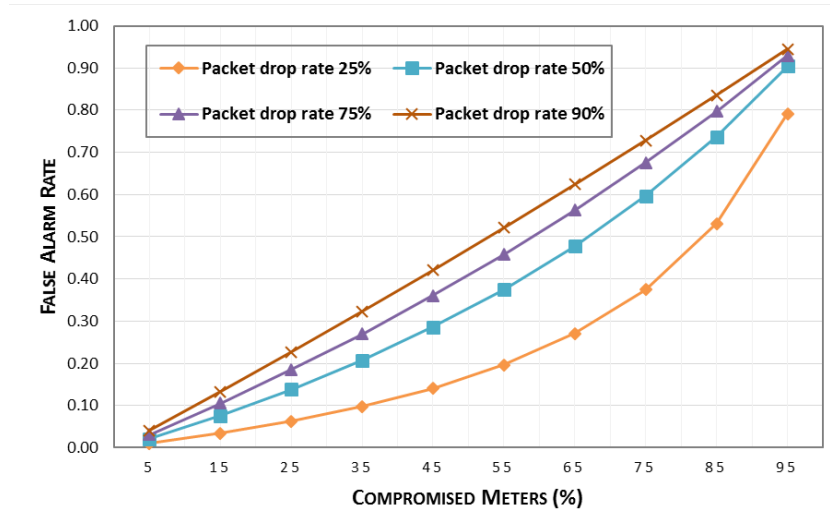


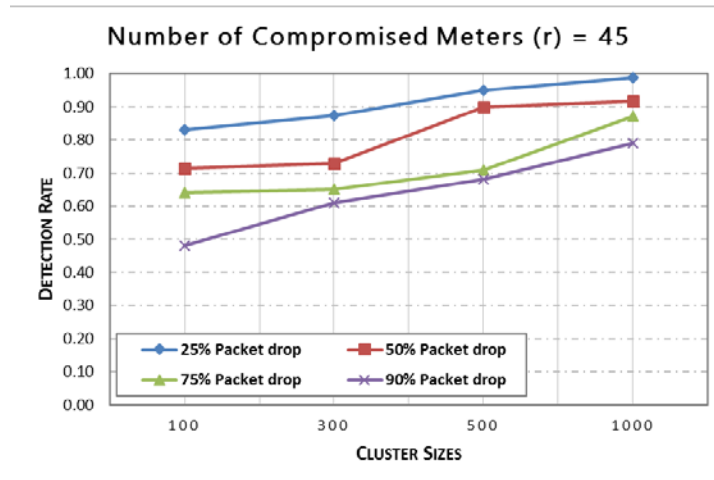
Figure 29: Attack Detection Rate for four Packet drop rates and N=100

The attack detection rate was found to degrade with increasing numbers of compromised meters ( $r$ ). For 25% of packet drop rate, there was a gradual fall in the detection rate with increasing numbers of malicious meters ( $r$ ). A sharp decrease was noticed in detection rate for high packet drop rate (90%). For zero malicious meters the detection rate is close to 100%, thus show capability of the scheme for detect the malicious meters. A corresponding grow in the false alarm rate (i.e. normal meters detected as compromised) is obvious through Fig. 30 The false alarm rate is rose sharply for 90% packet drop rate. A gradual climb in the false alarm rate is observed for 25% packet drop rate. Increasing numbers of compromised smart meters in the network will rise false alarm, for all four values of packet drop rates.



**Figure 30: The False Rate for four Packet drop rates and N=100**

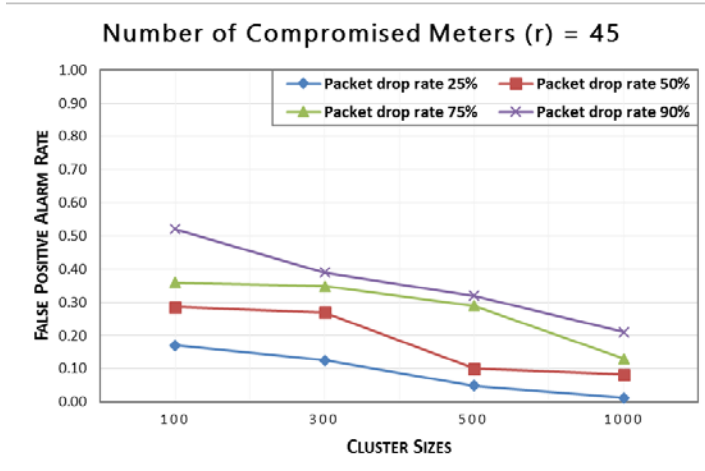
In order to examine the effect of packet loss/drop rate and different cluster sizes (i.e.  $N=100$ ,  $N=300$ ,  $N=500$ , and  $N=1000$ ) on the detection and false alarm rates, we repeated the simulation of scenario (1) with varying the value of  $N$ . Fig. 31 shows clearly the effect of four different packet drop rates on the attack detection rate with fixed number of compromised meters ( $r = 45$ ).



**Figure 31: Attack Detection Rate for four Packet drop rates and different Cluster Sizes and fixed number of compromised meter ( $r=45$ )**

The detection rate is increased markedly with increasing numbers of meters in the cluster. Larger numbers of meters in a cluster yield higher detection rates as large number of meters will collaborate to detect the malicious meters. The lowest value of detection rate were recorded is 49% for cluster size of ( $N=100$  and Packet drop rate 90%) with ( $r=45$ ) compromised meter.

In contrast to the detection rate, the false alarm rate was found to degrade with increasing cluster size (see Fig. 32). Between  $N=300$  and  $N=500$  there was a sharp fall in false alarm rate for a packet drop rate 50%. The false alarm rate was at its lowest value (0.03%) for a packet drop rate 25% and  $N=1000$ .



**Figure 32: Attack Detection Rate for four Packet drop rates and different Cluster Sizes and fixed number of compromised meter ( $r$ ) =45**

In addition, we fixed the packet drop rate (=25%) and varying cluster size (i.e.  $N=100$ ,  $N=300$ ,  $N=500$ , and  $N=1000$ ) with four different values of compromised meters  $r$  (i.e.  $r=35$ ,  $r=45$ ,  $r=55$ , and  $r=65$ ).

Fig. 33 shows that for all values of  $r$ , it observed that the detection rate is gradually increased with increasing the cluster size. Larger networks;  $N=1000$  yielding a high detection rate as compared to the detection rate when  $N=100$ . For larger networks, more smart meters report misbehaving meter activity to the DCU, and therefore, the detection rate improves.

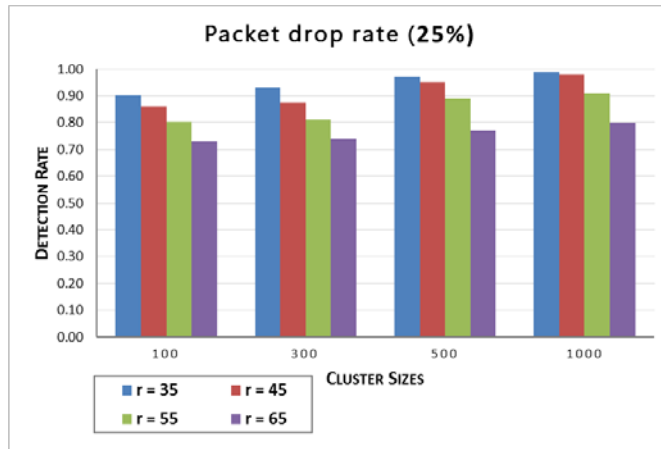


Figure 33: Attack Detection Rate for fixed Packet drop rate (=25%) and Varying Cluster Sizes with different Attacker ratio

The false alarm rates for varying cluster sizes and attacker ratio with packet drop rate (=25%) is illustrated in Fig. 34. For all values of  $N$ , the false alarm rate is gradually dropped with increasing the number of compromised meters ( $r = 35 - r=65$ ). Larger networks yield lesser false alarm rates. In addition, large number of compromised meters ( $r=65$ ), the false alarm rates are the highest for all network sizes.

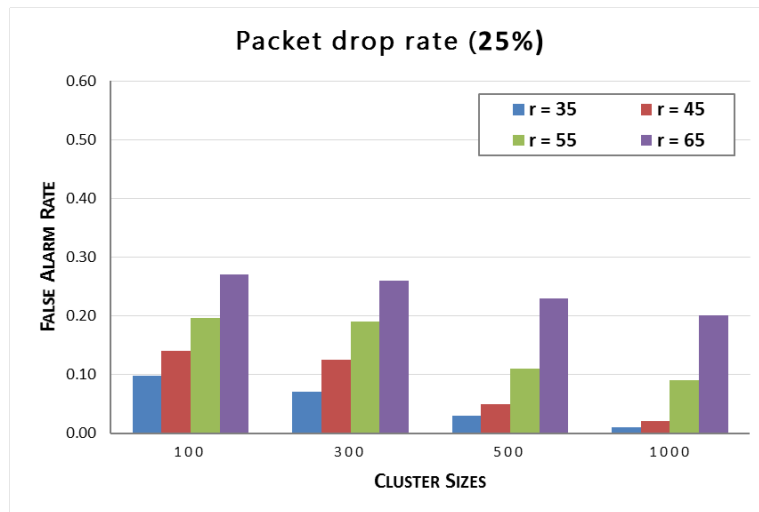


Figure 34: False Alarm Rate for fixed Packet drop rate (=25%) and Varying Cluster Sizes with different Attacker ratio



From the analysis of the simulations, we may observe that our scheme performs consistently even in the presence of varying numbers of compromised meters and diverse adversary types. The effect of peer monitoring on smart meter anomaly detection is therefore a promising approach towards identifying misbehaving smart meters and reporting these to the DCU.

## CHAPTER 5

### CONCLUSION AND FUTURE WORK

#### 5.1 Conclusion

Cyber attacks that target the infrastructure of smart grid systems not only have an impact on the consumer but are also detrimental to the business of the electricity utility. There are many threats against the smart grid system which may develop into attacks based on the profit the attacker will reap. Five distinct classes of cyber attacks were studied and analyzed to facilitate the identification and analysis process. The proposed mitigation techniques which aim to defend against all such attacks have also been studied and reported.

With the growth of the advanced metering infrastructure (AMI), many complicated cases of *Energy Fraud* have emerged and many new technologies and techniques have been developed to try to solve this issue. In this work, we have proposed a detection scheme to identify compromised smart meters in the AMI of a smart grid. The scheme groups smart meters of a neighborhood area network into fixed size clusters, regularly multicasting their respective smart meter readings securely using light weighted cryptographic protocols to peer meters of the cluster. The purpose of information exchange is to verify electricity usage readings of a given neighborhood area network in a peer-to-peer fashion.

## **5.2 Future Work**

As part of our future work, we intend to study the effect of sophisticated adversaries on the performance of our proposed attack detection scheme. In particular, we shall model an adversary who modifies individual smart meter readings of a neighborhood area network based on a random behavior pattern. For such a scenario, the attack detection process is anticipated to present a greater challenge.

## References

- [1] “Smart Grid 101: The Traditional Grid.” Internet: [http://www.smartgridnews.com/artman/publish/Business\\_Smart\\_Grid\\_101/The\\_Traditional-Grid-1599.html](http://www.smartgridnews.com/artman/publish/Business_Smart_Grid_101/The_Traditional-Grid-1599.html), Jan. 21, 2010 [March 5, 2013]
- [2] “Smart Grids Start Here” Internet: <http://www.maxim-ic.com/landing/index.mvp?lpk=485&CMP=467>, Jan. 2011 [March 23, 2013]
- [3] X. Fang et al., “Smart grid - the new and improved power grid: A survey,” *IEEE Communications Surveys and Tutorials*, in press, 2011
- [4] “What is the Definition of a Smart Grid?” Internet: <http://www.globalsmartgridfederation.org/smartgriddef.html> , [April 12, 2013]
- [5] “Smart Grid Conceptual Model.” Internet: <http://smartgrid.ieee.org/ieee-smart-grid/smart-grid-conceptual-model> , [Feb. 12, 2013]
- [6] Y. Zhang et al., "A multi-level communication architecture of smart grid based on congestion aware wireless mesh network," *North American Power Symposium (NAPS), 2011*, vol., no., pp.1-6, 4-6 Aug. 2011
- [7] A. Shreyas, “Analysis of Communication Protocols for Neighborhood Area network for Smart Grid,” California State University, Sacramento, Dept. of Computer Engineering, Report, fall 2010

- [8] Huq, Z, Islam, S., "Home Area Network Technology Assessment for Demand Response in Smart Grid Environment," Australasian Universities Power Engineering Conference, 2010, pp. 1-6.
- [9] S.L. Clements, M,D, Hadley and T.E. Carroll, "Home Area Networks and the Smart Grid," U.S. Dept. of Energy, Apr. 2011
- [10] S. Omerovic, "WiMAX Overview," Faculty of Electrical Engineering, University of Ljubljana, 2005
- [11] Yarali, A., Rahman, S., "Smart Grid Network: Promises and Challenges", Journal of Communications, Vol. 7, NO. 6, June 2012. DOI: 10.4304/jcm.7.6.409-417
- [12] Clemente, Judy, "The Security Vulnerabilities of the Smart Grid," Journal of Energy Security, June, 2009
- [13] Xu Li; Xiaohui Liang; Rongxing Lu; Xuemin Shen; Xiaodong Lin; Haojin Zhu, "Securing smart grid: cyber-attacks, countermeasures, and challenges," Communications Magazine, IEEE , vol.50, no.8, pp.38,45, August 2012
- [14] Grochocki, D., Huh, J.H., Berthier, R., Bobba, R., Sanders, W.H., Cardenas, A., Jetcheva, J.G., "AMI Threats, Intrusion Detection Requirements and Deployment Recommendations," 2012 IEEE International Conference on Smart Grid Communications (SmartGridComm), November 2012
- [15] Eun-Kyu Lee; Gerla, M.; Oh, S.Y., "Physical layer security in wireless smart grid," Communications Magazine, IEEE , vol.50, no.8, pp.46,52, August 2012

- [16] Z. A. Baig, "Rapid Anomaly Detection for Smart Grid Infrastructures through Hierarchical Pattern Matching," *International Journal of Security and Networks (IJSN)*, Vo. 7, No. 2, 2012, pp. 83-94
- [17] Y. Yang, L. Tim, S. Sezer, K. McLaughlin, and H. F. Wang, "Impact of cyber-security issues on Smart Grid," in *Proc. 2<sup>nd</sup> IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, Manchester, Dec 2011, pp. 1-7.
- [18] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," *IEEE Commun. Surveys Tuts.*, vol.14, no. 4, pp. 998-1010, 2012.
- [19] Z. Zhang, H. Liu, S. Niu, and J. Mo, "Information security requirements and challenges in smart grid," in *Proc. 6<sup>th</sup> IEEE Joint International Information Technology and Artificial Intelligence Conference*, Chongqing, Aug 2011, pp. 90-92.
- [20] M. Apurva and K. Himanshu, "Towards addressing common security issues in smart grid specifications," in *Proc. 5<sup>th</sup> International Symposium on Resilient Control Systems*, Aug 2012, pp. 174-180.
- [21] Y. Mo, T. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," in *Proc. IEEE*, vol. 100, no. 1, Jan 2012, pp. 195-209.

- [22] I. Ghansa, "Smart grid cyber security potential threats, vulnerabilities, and risks," *Technical Report*, California Energy Commission, May 2012.
- [23] V. Roberto, Y. Ender, and R. Carroline, "Smart grid security a smart meter-centric perspective," in *Proc. 20<sup>th</sup> Telecommunications Forum*, Nov 2012, pp. 127-130.
- [24] H. Khurana, M. Hadley, L. Ning, and D. A. Frincke, "Smart-grid security issues," *IEEE Security & Privacy Mag.*, vol. 8, no. 1, pp. 81-85, Jan-Feb 2010.
- [25] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy Mag*, vol. 7, no. 3, pp. 75-77, May-June 2009.
- [26] F. Skopik and M. Zhendong, "Attack vectors to metering data in smart grids under security constraints," in *Proc. IEEE 36<sup>th</sup> Annual Computer Software and Applications Conference Workshops*, Izmir, July 2012, pp. 134-139.
- [27] M. Xin and C. Xi, "Cyber security infrastructure of smart grid communication system," in *Proc. China International Conference on Electricity Distribution*, Sept 2012, pp. 1-4.
- [28] X. Wang and P. Yi, "Security framework for wireless communications in smart distribution grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 809–818, 2011.
- [29] L. Eun-Kyu, G. Mario, and O. Y. Soon, "Physical layer security in wireless smart grid," *Communications Magazine, IEEE*, vol. 50, no. 8, pp. 46-52, August 2012.

- [30] A. Rahman and M-R. Hamed, "False data injection attacks with incomplete information against smart power grids," in *Proc. IEEE Global Communications Conference*, Dec 2012, pp. 3153-3158.
- [31] O. Mete, E. Inaki, V. Fatos, K. Sanjeev, and P. Vincent, "Smarter security in the smart grid," in *IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, Tainan, Nov. 2012, pp. 312-317.
- [32] H. Yi, E. Mohammad, N. Huy, Z. Rong, H. Zhu, L. Husheng, and S. Lingyang, "Bad data injection in smart grid: attack and defense mechanisms," *Communications Magazine, IEEE*, vol. 51, no. 1, pp. 27-33, January 2013.
- [33] T. Thien-Toan, S. Oh-Soon, and L. Jong-Ho, "Detection of replay attacks in smart grid systems," in *Proc. International Conference on Computing, Management and Telecommunications*, Jan 2013, pp. 298-302.
- [34] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: attack strategies and countermeasures," in *Proc. IEEE Smart Grid Comm*, Gaithersburg, MD, Oct 2010, pp. 220-225.
- [35] K. Jinsub and T. Lang, "On topology attack of a smart grid," in *IEEE PES Innovative Smart Grid Technologies*, Feb 2013, pp. 1-6.
- [36] P. -Y. Chen, S.-M. Cheng, and K.-C. Chen, "Smart attacks in smart grid communication networks," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 24-29, Aug 2012.



- [37] Z. Zhenghao, G. Shuping, D. D. Aleksandar, and L. Husheng, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87-98, March 2013.
- [38] L. Shichao, L. P.Xiaoping, and S. E. Abdulmotaleb, "Denial-of-Service (dos) attacks on load frequency control in smart grids," in *Proc. IEEE PES Innovative Smart Grid Technologies*, Feb 2013, pp. 1-6.
- [39] S. McLaughlin, D. Podkuiko, S. Miadzvezhanka, A. Delozier, and P. McDaniel, "Multi vendor penetration testing in the advanced metering infrastructure," in *ACM ACSAC*, 2010.
- [40] Y. Tanaka, Y. Terashima, M. Kanda, and Y. Ohba, "A security architecture for communication between smart meters and han devices," in *IEEE Third International Conference on Smart Grid Communications*, Nov. 2012, pp. 460–464.
- [41] J. Kamto, L. Qian, J. Fuller, J. Attia, and Y. Qian, "Key distribution and management for power aggregation and accountability in advance metering infrastructure," in *IEEE Third International Conference on Smart Grid Communications*, Nov. 2012, pp. 360–365.
- [42] M. Nabeel, S. Kerr, X. Ding, and E. Bertino, "Authentication and key management for advanced metering infrastructures utilizing physically unclonable functions," in *IEEE Third International Conference on Smart Grid Communications*, Nov. 2012, pp. 324–329.

- [43] N. Saputro and K. Akkaya, "Performance evaluation of smart grid data aggregation via homomorphic encryption," in *Wireless Communications and Networking Conference (WCNC)*, Apr. 2012, pp. 2945–2950.
- [44] M. Thomas, I. Ali, and N. Gupta, "Integration and security analysis of metering infrastructure," in *Fifth IEEE Power India Conference*, Dec. 2012, pp. 1–6.
- [45] D. Grochocki, J. Huh, R. Berthier, R. Bobba, W. Sanders, A. Cardenas, and J. Jetcheva, "Ami threats, intrusion detection requirements and deployment recommendations," in *IEEE Third International Conference on Smart Grid Communications*, Nov. 2012, pp. 395–400.
- [46] Y. Zhang, L. Wang, W. Sun, R. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *Smart Grid, IEEE Transactions on*, vol. 2, no. 4, pp. 796–808, dec. 2011.
- [47] H. Li, R. Mao, L. Lai, and R. Qiu, "Compressed meter reading for delay-sensitive and secure load report in smart grid," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, Oct. 2010, pp. 114–119.
- [48] R. Berthier, W. Sanders, and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, Oct. 2010, pp. 350–355.

- [49] R. Berthier and W. Sanders, "Specification-based intrusion detection for advanced metering infrastructures," in *Dependable Computing (PRDC), 2011 IEEE 17th Pacific Rim International Symposium on*, Dec. 2011, pp. 184–193.
- [50] Z. Baig, "On the use of pattern matching for rapid anomaly detection in smart grid infrastructures," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, Oct. 2011, pp. 214–219.
- [51] H. Li, X. Liang, R. Lu, X. Lin, H. Yang, and X. Shen, EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid, *IEEE Transactions on Parallel and Distributed Systems*, vol. PP, no. 99, pp. 1-10, 2013.
- [52] X. Liang, X. Li, R. Lu, X. Lin, and X. Shen, UDP: Usage based dynamic pricing with privacy preservation for smart grid, *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 141-150, 2013.
- [53] "Advanced Metering Infrastructure" India Smart Grid Knowledge Portal < <http://indiasmartgrid.org/en/technology/Pages/Advanced-Metering-Infrastructure.aspx> >, 2013
- [54] P. Antmann, Reducing technical and non-technical losses in the power sector, Background paper for the WBG Energy Strategy, Tech. Rep., Washington, DC, USA: The World Bank, 2009.
- [55] P. McDaniel and S. McLaughlin, Security and privacy challenges in the smart grid, *IEEE Security & Privacy*, vol. 7, no. 3, pp. 75-77, 2009.

- [56] B. Krebs, FBI: Smart meter hacks likely to spread, <http://krebsonsecurity.com/2012/04/fbi-smart-meter-hackslikely-to-spread/> , 2012.
- [57] CBC News, Electricity theft by B.C. grow-ops costs \$100m a year, <http://www.cbc.ca/news/canada/britishcolumbia/electricity-theft-by-b-c-grow-ops-costs-100m-ayear-1.969837> , 2010.
- [58] Ministry of power, India, Overview of power distribution, Tech. Rep., <http://www.powermin.nic.in> , 2013.
- [59] Federal Court of Audit, Operational audit report held in national agency of electrical energy, aneel, Brazil, Tech. Rep., No. TC 025.619/2007-2, 2007.
- [60] Electric meter hack! how to cut your electricity bill in half! <http://www.youtube.com/watch?v=YVA8M2YVQW8> , 2013.
- [61] S. McLaughlin, D. Podkuiko, and P. McDaniel. *Energy Theft in the Advanced Metering Infrastructure*. In E. Rome and R. Bloomfield, editors, *Critical Information Infrastructures Security*, Volume 6027 of *Lecture Notes in Computer Science*, chapter 15, pp. 176–187. Springer Berlin, 2010.
- [62] Schneier, B.: Attack trees. *Dr Dobb's Journal* 24(12) (December 1999)
- [63] R. Jiang; R. Lu; Y. Wang ; J. Luo; C. Shen; S. Xuemin, "Energy-theft detection issues for advanced metering infrastructure in smart grid," *Tsinghua Science and Technology* , vol.19, no.2, pp.105,120, April 2014

- [64] F. Skopik and Z. Ma, Attack vectors to metering data in smart grids under security constraints, in *Proc. IEEE 36th Annual Computer Software and Applications Conference Workshops*, 2012, pp. 134-139.
- [65] A. Hahn and M. Govindarasu, Cyber-attack exposure evaluation framework for the smart grid, *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 835-843, 2011.
- [66] S. Depuru, L. Wang, and V. Devabhaktuni, Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft, *Energy Policy*, vol. 39, no. 2, pp. 1007-1015, 2011.
- [67] D. Grochocki, J. H. Huh, R. Berthier, R. Bobba, W. H. Sanders, A. A. C´ardenas, and J. G. Jetcheva, AMI threats, intrusion detection requirements and deployment recommendations, in *Proc. 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, 2012, pp. 395-400.
- [68] V. D. Gligor, "Security of emergent properties in ad-hoc networks," in *Proc. of Int'l Workshop on Security Protocols*, Apr. 2004.

## Vitae

Name Abdurraoof Salih Al-Amoudy

Nationality Yemeni

Date of Birth 6/29/1984

Email abdellruoof@gmail.com

Present Address King Fahd University of Petroleum & Minerals, Dhahran,  
31261, Kingdom of Saudi Arabia

Publication Journal Article:

Baig, Z., Al Amoudy, A., (2013), An Analysis of Smart Grid Attacks and Countermeasures. *Journal of Communications*, 8(8), 473-479, United States, DOI: 10.12720/jcm.8.8.473-479.

Conference:

Baig, Z., Al Amoudy, A., Salah, K., (2015), Detection of Compromised Smart Meters in the Advanced Metering Infrastructure. *8th IEEE GCC conference and exhibition "Towards Smart Sustainable Solutions"*, Muscat , Oman