NTNU
Norwegian University of
Science and Technology

# Security of the Smart Grid

Wisdom Edem Avevor

Master of Science in Telematics - Communication Networks and Networked
Submission date: June 2018
Supervisor: Lillian Røstad, IIK
Co-supervisor: Christian Frøystad, SINTEF Digital

Norwegian University of Science and Technology
Department of Information Security and Communication Technology

| | |
|---|---|
| **Title:** | Security of the Smart Grid |
| **Student:** | Wisdom Edem Avevor |

**Problem description:**

The way energy is dispatched is undergoing fundamental changes. The traditional grid, which is only capable of transmitting electricity from the generation plants to the customer, is managed from a central location. With the growing population and changes in consumer behaviors, the traditional grid is insufficient due to its lack of an automated system for monitoring and control, thereby resulting in longer response times. The smart grid is an adequate solution to address this requirement. The smart grid benefits from the added communication network to increase system efficiency, provide customers with tools to manage energy use, improve reliability, resiliency and power quality and enable the use of innovative technologies including renewable, storage and electric vehicles. However, the smart grid's use of communication network makes it a potential targets for attackers to exploit.

This master thesis investigates different modeling techniques that can be used to identify security risks and apply a suitable one in exploring the risks and threats in the smart grid. In addition, this thesis identifies attacks that can be used to exploit the security of smart grid.

| | |
|---|---|
| **Responsible Professor:** | Lillian Røstad, IIK |
| **Supervisor:** | Christian Frøystad, SINTEF Digital |

# Abstract

Given the incorporation of a communication network into the traditional power grid, the smart grid is equipped with devices that provide sensing, measurement, and control. This gives the smart grid numerous advantages over the traditional power grid. However, the smart grid has a risk of cyber attacks which can result in failures of critical systems. Understanding the threats to the smart grid is paramount in ensuring adequate security.

This thesis aims at identifying the attacks that can be used in compromising the smart grid as well as security modeling techniques that aid in identifying and presenting the security risks. It first reviews existing literature on security modeling techniques that aid in security risk analysis and compare the techniques so as to evaluate its applicability to the smart grid. A demonstration of the efficacy of using a modeling technique in identifying risks in the Advanced Metering Infrastructure (AMI) network of the smart grid. Finally, an attack tree is presented which provides an overview of attacks against smart grid obtained from literature.

A review of 84 relevant papers is done to identify the attacks against the smart grid in order to create an attack tree which gives an overview of how security requirements can be compromised. Furthermore, another 26 relevant papers are reviewed to identify modeling techniques that can be used in security analyses. This is followed by an evaluation of the identified techniques based on four groupings: asset identification, risk identification, risk evaluation, and mitigation steps. Lastly, a demonstration of how Consultative Objective Risk Analysis System (CORAS) can be used in identifying and understanding the security risks in the smart grid is done. The application of CORAS shows how effective it is in helping to achieve the research objectives of this thesis. Lastly, the attack tree revealed how individual attacks stack up in compromising the major security requirements.

The results of the review give insights as to directions for future work and improvements: (i) It is important to extend the CORAS application evaluate the risks identified in this thesis and document mitigation steps by first performing research on formalizing evaluation criteria for the risks (ii) It is paramount to perform develop formal assessment criteria for all

security modeling techniques to assess the strengths and short-comings of each of the techniques.

# Preface

This thesis is submitted in fulfillment of the requirements for the two year master of science (MSc) degree in Telematics with specialization in Information Security at the Norwegian University of Science and Technology (NTNU).

I would like to express sincerest gratitude to my supervisor, Christian Frøystad, for his constant constructive criticism in this thesis. This has been invaluable and helped me immensely to focus and improve the quality of my work.

Lastly, I would also like to thank my family, friends and colleagues for their support throughout the course of my masters studies.

# Contents

# List of Figures

# List of Tables

# List of Acronyms

**AMI** Advanced Metering Infrastructure.

**AMQP** Advanced Message Queuing Protocol.

**BAN** Building Area Network.

**CORAS** Consultative Objective Risk Analysis System.

**COSEM** Companion Specification for Energy Metering.

**CPN** Colored Petri Nets.

**DAP** Data Aggregation Point.

**DCU** Data Concentrator Unit.

**DDS** Data Distribution Service.

**DLMS** Device Language Message Specification.

**DoS** Denial of Service.

**FAN** Field Area Network.

**HAN** Home Area Network.

**HEMS** Home Energy Management System.

**IC** Integrated Circuit.

**ICT** Information and Communication Technology.

**IoT** Internet of Things.

**MAD** Malicious Activity Diagram.

**MQTT** Message Queue Telemetry Transport.

**NAN** Neighbour Area Network.

**NIST** National Institute of Standards and Technology.

**OSGP** Open Smart Grid Protocol.

**PMU** Phasor Measurement Units.

**PN** Petri-Nets.

**PPN** Probabilistic Petri-Nets.

**PSTN** Public Switched Telephone Network.

**RFID** Radio Frequency Identification.

**RTUs** Remote Terminal Units.

**SCADA** Supervisory Control And Data Acquisition.

**SGN** Stochastic Game-Nets.

**SOMAD** Security Oriented Malicious Activity Diagram.

**SPN** Stochastic Petri-Nets.

**SysML** Systems Modelling Language.

**TPN** Time Petri-Nets.

**UML** Unified Modeling Language.

**WAMS** Wide Area Measurement System.

**WAN** Wide Area Network.

**WiMAX** Worldwide Interoperability for Microwave Access.

# Chapter 1
# Introduction

## 1.1 Motivation

Although there have been several attempts to define what a smart grid is, there is currently no distinct definition of what a smart grid is. A number of tentative definitions have been documented in literature. The smart grid can be described as the traditional power network which incorporates Information and Communication Technology (ICT) that seeks to provide a reliable and economic system that handles power supply and consumption [9]. The traditional power grid is an incredibly complex network comprising transmission networks, distribution networks, and the "last mile". The incorporation of another extremely complex network, the communication network, to the traditional grid has many benefits. The communication network allows data from sensory nodes such as smart meters and Phasor Measurement Units (PMU) to be aggregated and analysed at control centers. Taking this a step further by connecting these devices to the internet ensures distributed monitoring, analyses and remote control which is achievable through the Internet of Things (IoT).

Thus, the smart grid superficially brings great improvement to the traditional grid. However, on closer inspection, the added network connectivity adds more ways the grid can be compromised. A skillful adversary can disrupt the entire grid from the comfort of his home. With this premise, the task set out for this research is to discover security risks and threats facing the smart grid using visualization techniques as well as investigate the individual attack that can be used to exploit the security risks. In this way, our motivation is finding security threats and possible attacks in the smart grid

## 1.2 Keywords

Security Risk Analysis, Modeling Techniques, CORAS, Smart Grid , Advance Metering Infrastructure.

## 1.3 Research Objectives

The goal of the thesis is to identify attacks that can be used to compromise the smart grid as well as investigate different risk modeling techniques and apply a suitable one to explore the security risks associated with the smart grid. More specifically, it aims to answer the following questions:

1. What different modeling techniques are used in security risk analysis and which of the techniques better aids in identifying and understanding the security risks and threats in a smart grid?
2. What attacks can be used to compromise the smart grid?

## 1.4 Contribution

This master thesis summarizes the usage of modeling techniques in security risk assessment from papers published in the period 2008-2018. The span was chosen so as to attain a comprehensive application of each of the techniques. It goes on to provide a comparison of the identified techniques in relation to their applicability to the smart grid. Similar comparisons of modeling techniques could not be found. A demonstration of how a modeling technique is used in identifying attacks in Advanced Metering Infrastructure (AMI) is also presented.

In addition, this master thesis provides a summary of attacks that have been shown to compromise the smart grid from literature published within the time frame of 2015-2018. This time span was chosen so as to focus on recent attacks. An attack tree is presented to provide an overview of how the attacks stack up in compromising security requirements of the smart grid. This is not the first of its kind, however, to the best of my knowledge, the resulting attack tree contains the largest number of attacks presented in any relevant paper. The novelty of this attack tree is the number of coordinated attacks.

## 1.5 Thesis Structure

This section provides a summary list of the contents in this thesis. The list describes what each chapter entails. Firstly, the background, as well as related works, is presented. This is followed by the research methods used and implementations of the method. The thesis concludes with recommendations for future.

- Chapter 2 explains relevant background theories to gain insights into the thesis. This commences with an explanation of IoT and smart grid. It concludes with a presentation of the smart grid security concerns.

- Chapter 3 explains the methods and steps taken to answer each of the research questions posed in this thesis. It defines how a literature review adaptation of a systematic review is applied. This is followed by presentation of an application of Consultative Objective Risk Analysis System (CORAS) method to a constructed case study which is used in answering research question 1. Finally, the steps taken to identify attacks in literature are presented.

- Chapter 4 discusses security risk modeling techniques. Firstly, a theoretical explanation of various security modeling techniques used in literature is presented. The chapter concludes with an investigation and documentation of applications of the modeling techniques used in literature.

- Chapter 5 describes the CORAS language and Tool of which gives insight as to how it is applied in the thesis

- Chapter 6 provides a step by step implementation of security risk analysis of a constructed AMI using CORAS

- Chapter 7 investigates and documents the attacks against the smart grid that have been discussed or implemented in literature

- Chapter 8 discusses the significant findings obtained in the preceding chapters

- Chapter 9 sums up conclusions for each research question and presents some recommendations for future research work

# Chapter 2 Smart Grid

In this chapter, the IoT as well as the changes that transform the traditional grid into a smart grid is discussed. This is followed by an overview of the smart grid architecture. Emphasis is placed on the communication technology the IoT brings to the electrical grid. This is done by pinpointing the most applicable and utilized communication mechanisms that could be adopted in the smart grid by introducing their technology and use. Next, the security objectives of a smart grid which includes confidentiality, integrity, and availability are discussed. This chapter concludes with an elaboration on the threats that the smart grid faces.

## 2.1 The Internet of Things

IoT has gained increased popularity in the ICT world over the last decade. The term "Internet of Things" was invented by Kevin Ashton in 1999 [10] and can be described as the network of physically connected devices that interact to fulfill a common goal. Cisco describes IoT as the next evolution of the internet, defines it as *"the point in time when more things were connected to the internet than humans"* and further predict that there will be 50 billion devices connected to the Internet by 2020 [11]. According to the authors in [10], IoT can also be considered as the global network which allows the communication between human-to-human, human-to-things, and things-to-things (which is any electronic device in the world by providing a unique identity to each and every object).

IoT generally adopts the basic architecture of sensor networks and thus can be segregated into 3 layers; *Perceptual layer*, *Network layer* and *Application layer.* The perceptual layer aims to obtain and process data from the physical environment. This layer is mainly composed of Radio Frequency Identification (RFID) and sensors which sense the physical environment as well as actuators that affect the environment. These devices are linked via the network layer using wireless and wired technologies, standards, and protocols like Public Switched Telephone Network (PSTN), 2G/3G/LTE, Wi-Fi and Zigbee that provide connectivity. The application layer, which is the brain of the system, is responsible for service providing and data processing while ensuring data integrity, authenticity as well as confidentiality. This layer uses protocols such as Message Queue Telemetry Transport (MQTT), HTTP, Advanced Message Queuing Protocol (AMQP) and Data Distribution Service (DDS) to enable process-to-process connectivity [12].

IoT has many applications in the power grid. According to [13] *"The smart grid is already considered to be one of the first and largest examples of the IoT".* Smart metering is one important application of the IoT for environmental sustainability and energy-related issues in recent years [14]. Traditionally, utility companies required employees to go on site to manually gather operational data including electricity meter readings. This may introduce inefficiencies due to factors such as reading errors. The smart grid incorporates Advanced Metering Infrastructure (AMI) which enables meters to be read digitally and thus abolishes manual reading of meters. The communication infrastructure ensures data is aggregated in real-time which ensures accurate meter readings and improved billing. Another important application of IoT is in achieving online visual monitoring of the smart grid transmission line. Monitoring the power transmission line is key to providing more stable and reliable service to customers by promptly identifying and addressing points of failures. The traditional grid's monitoring system is unable to provide real-time monitoring due to high operation cost and incomplete network coverage [15]. Deploying IoT sensors on the grid mitigates these challenges.

## 2.2 Smart Grid Architecture

Upgrading the current electricity infrastructure to the smart grid is a very daunting and complex task [16]. Many standardization bodies have developed their own conceptual model for the smart grid. The National Institute of Standards and Technology (NIST)'s conceptual model is one of the most well-known reference models of the smart grid. According to NIST [17], there are seven main domains, namely: Bulk Generation, Transmission, Distribution, Customers, Operations, Markets and Service Providers. These domains are interconnected via a secure communication network as shown in Figure 2.1

### 2.2.1 Smart Grid Subsystem

The smart grid is made up of subsystems. The key subsystems include AMI and operations. These key subsystems are discussed in the subsequent sections:

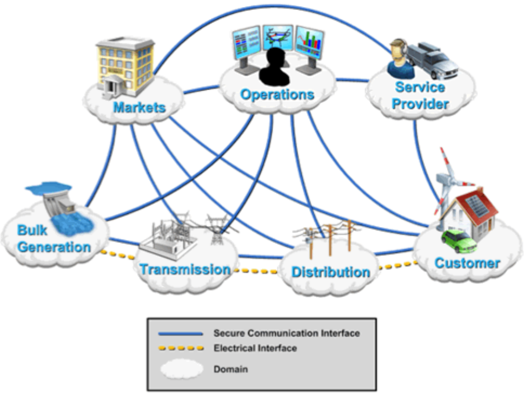


**Figure 2.1:** The NIST conceptual model for smart grid

### Operations

Operations consist of technologies such as Supervisory Control And Data Acquisition (SCADA) and Wide Area Measurement System (WAMS). SCADA is a system of software and hardware elements that is implemented to optimize, supervise and control power generation and transmission. SCADA uses magnitude information received from Remote Terminal Units (RTUs)(devices that are deployed in the field) for its operations. On the other hand, WAMS rely on PMU which measure both magnitude and phase angle for optimization and control. Another key difference between SCADA and WAMS is that SCADA is relatively slower and retrieves data asynchronously. This makes it suitable for local areas whereas WAMS are better suited for monitoring and control in wide geographic areas [18].

### Advanced Metering Infrastructure

AMI is made up of multiple technologies such as smart meters and communication technologies that collectively provide communication between consumers and operators. This communication enables real-time monitoring of energy consumption which is beneficial not only to energy suppliers but also end-consumers. For the suppliers, the AMI provides more efficient way to obtain power consumption records as well as accurately localizing outages. For the end-users, they can adjust their consumption by participating in real-time market pricing and demand response so as to reduce utility cost [18]. Thus, the AMI can be said to be made of two parts: metering and communications as shown in Figure 2.2 with the smart meter performing the measurement of energy consumption of customers. As such, the smart meter must be able to detect energy consumption in real time. The metering side of the smart grid consists of Time of Use pricing, data management systems, and advanced meter reading while the communication is made of networks and control infrastructure [1].

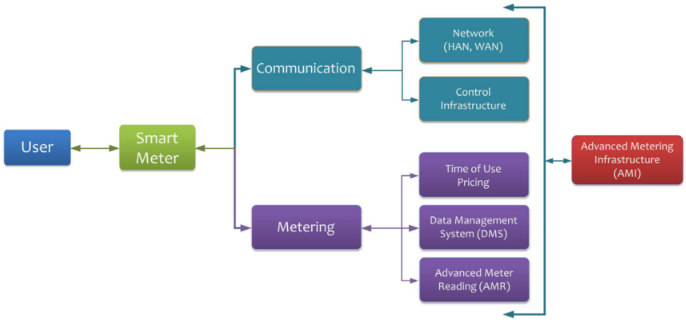


**Figure 2.2:** A smart grid perspective with all components [1]

### 2.2.2 AMI Communication Network

The AMI in smart grid comprises several communication networks. These are mainly divided depending on the coverage area: Home Area Network (HAN), Building Area Network (BAN), Neighbour Area Network (NAN) , Field Area Network (FAN) and Wide Area Network (WAN).

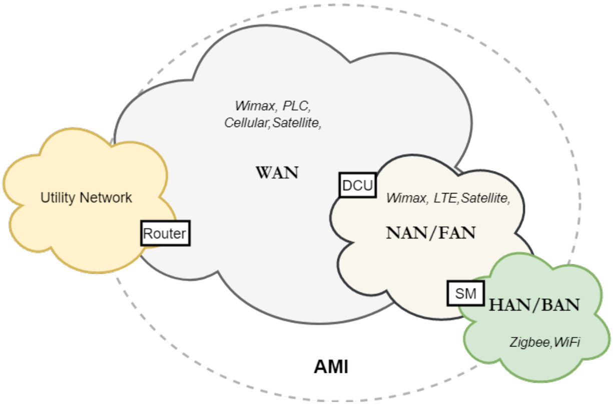


**Figure 2.3:** Distribution network communication mechanisms

#### HAN and BAN

HAN is the communication network within customer premises which connects various smart devices such as washers and electric vehicles with the aim of optimizing energy usage. HAN consists of Home Energy Management System (HEMS) and smart meter. HEMS allows customers to monitor and adjust their energy consumption either in real-time or periodically while the smart meter relays energy usage information to the utility company. The HAN can thus be described as the convergence of communication infrastructure, the power grid and the supporting information architecture [19]. BAN is deployed to cover multiple apartments or offices thus can be an aggregation of HANs with one smart meter that communicates with the utility company. The technologies that are used in the HAN and BAN include Wireless LAN, ZigBee, Mobile communications and Femtocells

#### NAN and FAN

NAN is deployed between customer premises and utility company's WAN to enable smart meters exchange information. NAN is a critical segment of the smart grid communication network since it is tasked with transportation of massive volume of data and control signals between a number of smart meters installed at customer premises and the utility company. FAN allow communication between the utility company and the sensors and equipment deployed in the field. The communication infrastructure used in NAN and FAN include Worldwide Interoperability for Microwave Access (WiMAX), cellular network and Wi-Fi [20].

#### WAN

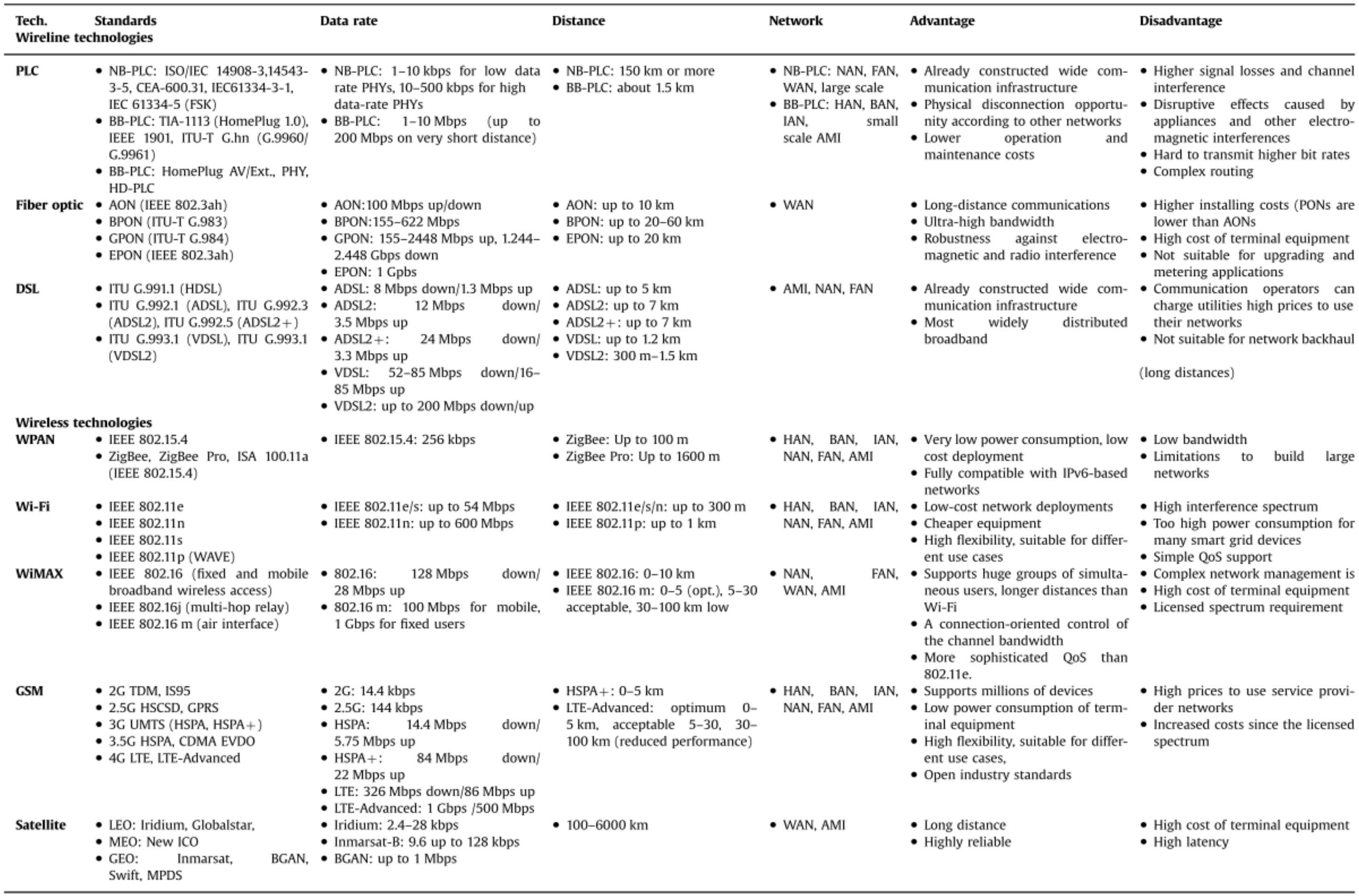
WAN accumulates data from multiple NANs and transports it to the private networks of the utility company. It also provides long distance communication between Data Aggregation Points (DAPs) of different systems such as substations, control centers, generation plants and distribution grid. Thus, WAN is essential for bi-directional communication needed for services such as monitoring of power quality and automation of distribution [20]. This network adopts communication technologies that are suitable for long-range and have high-bandwidth such as Power Line Communication, Satellite, WiMAX and cellular networks.

A comprehensive list of communication technologies used in the smart grid is presented in Figure 2.4

### 2.2.3 Communication Protocols Used

This section focuses on introducing the communication protocols used by various nodes in the smart grid, based on published literature. These protocols include a variety of specialized protocols such as Device Language Message Specification (DLMS), Open Smart Grid Protocol (OSGP), and Wireless M-BUS.

Wireless M-Bus specifies the communication protocol between smart meters (powered by batteries) and Data Concentrator Units (DCUs). Wireless M-Bus transceivers



| Tech. | Standards | Data rate | Distance | Network | Advantage | Disadvantage |
|---|---|---|---|---|---|---|
| **Wireline technologies** | | | | | | |
| **PLC** | • NB-PLC: ISO/IEC 14908-3,14543-3-5, CEA-600.31, IEC61334-3-1, IEC 61334-5 (FSK)<br>• BB-PLC: TIA-1113 (HomePlug 1.0), IEEE 1901, ITU-T G.hn (G.9960/G.9961)<br>• BB-PLC: HomePlug AV/Ext., PHY, HD-PLC | • NB-PLC: 1–10 kbps for low data rate PHYs, 10–500 kbps for high data-rate PHYs<br>• BB-PLC: 1–10 Mbps (up to 200 Mbps on very short distance) | • NB-PLC: 150 km or more<br>• BB-PLC: about 1.5 km | • NB-PLC: NAN, FAN, WAN, large scale<br>• BB-PLC: HAN, BAN, IAN, small scale AMI | • Already constructed wide communication infrastructure<br>• Physical disconnection opportunity according to other networks<br>• Lower operation and maintenance costs | • Higher signal losses and channel interference<br>• Disruptive effects caused by appliances and other electromagnetic interferences<br>• Hard to transmit higher bit rates<br>• Complex routing |
| **Fiber optic** | • AON (IEEE 802.3ah)<br>• BPON (ITU-T G.983)<br>• GPON (ITU-T G.984)<br>• EPON (IEEE 802.3ah) | • AON:100 Mbps up/down<br>• BPON:155–622 Mbps<br>• GPON: 155–2448 Mbps up, 1.244–2.448 Gbps down<br>• EPON: 1 Gpbs | • AON: up to 10 km<br>• BPON: up to 20–60 km<br>• EPON: up to 20 km | • WAN | • Long-distance communications<br>• Ultra-high bandwidth<br>• Robustness against electromagnetic and radio interference | • Higher installing costs (PONs are lower than AONs<br>• High cost of terminal equipment<br>• Not suitable for upgrading and metering applications |
| **DSL** | • ITU G.991.1 (HDSL)<br>• ITU G.992.1 (ADSL), ITU G.992.3 (ADSL2), ITU G.992.5 (ADSL2+)<br>• ITU G.993.1 (VDSL), ITU G.993.1 (VDSL2) | • ADSL: 8 Mbps down/1.3 Mbps up<br>• ADSL2: 12 Mbps down/ 3.5 Mbps up<br>• ADSL2+: 24 Mbps down/ 3.3 Mbps up<br>• VDSL: 52–85 Mbps down/16–85 Mbps up<br>• VDSL2: up to 200 Mbps down/up | • ADSL: up to 5 km<br>• ADSL2: up to 7 km<br>• ADSL2+: up to 7 km<br>• VDSL: up to 1.2 km<br>• VDSL2: 300 m–1.5 km | • AMI, NAN, FAN | • Already constructed wide communication infrastructure<br>• Most widely distributed broadband | • Communication operators can charge utilities high prices to use their networks<br>• Not suitable for network backhaul<br>(long distances) |
| **Wireless technologies** | | | | | | |
| **WPAN** | • IEEE 802.15.4<br>• ZigBee, ZigBee Pro, ISA 100.11a (IEEE 802.15.4) | • IEEE 802.15.4: 256 kbps | • ZigBee: Up to 100 m<br>• ZigBee Pro: Up to 1600 m | • HAN, BAN, IAN, NAN, FAN, AMI | • Very low power consumption, low cost deployment<br>• Fully compatible with IPv6-based networks | • Low bandwidth<br>• Limitations to build large networks |
| **Wi-Fi** | • IEEE 802.11e<br>• IEEE 802.11n<br>• IEEE 802.11s<br>• IEEE 802.11p (WAVE) | • IEEE 802.11e/s: up to 54 Mbps<br>• IEEE 802.11n: up to 600 Mbps | • IEEE 802.11e/s/n: up to 300 m<br>• IEEE 802.11p: up to 1 km | • HAN, BAN, IAN, NAN, FAN, AMI | • Low-cost network deployments<br>• Cheaper equipment<br>• High flexibility, suitable for different use cases | • High interference spectrum<br>• Too high power consumption for many smart grid devices<br>• Simple QoS support |
| **WiMAX** | • IEEE 802.16 (fixed and mobile broadband wireless access)<br>• IEEE 802.16j (multi-hop relay)<br>• IEEE 802.16 m (air interface) | • 802.16: 128 Mbps down/ 28 Mbps up<br>• 802.16 m: 100 Mbps for mobile, 1 Gbps for fixed users | • IEEE 802.16: 0–10 km<br>• IEEE 802.16 m: 0–5 (opt.), 5–30 acceptable, 30–100 km low | • NAN, FAN, WAN, AMI | • Supports huge groups of simultaneous users, longer distances than Wi-Fi<br>• A connection-oriented control of the channel bandwidth<br>• More sophisticated QoS than 802.11e. | • Complex network management is<br>• High cost of terminal equipment<br>• Licensed spectrum requirement |
| **GSM** | • 2G TDM, IS95<br>• 2.5G HSCSD, GPRS<br>• 3G UMTS (HSPA, HSPA+)<br>• 3.5G HSPA, CDMA EVDO<br>• 4G LTE, LTE-Advanced | • 2G: 14.4 kbps<br>• 2.5G: 144 kbps<br>• HSPA: 14.4 Mbps down/ 5.75 Mbps up<br>• HSPA+: 84 Mbps down/ 22 Mbps up<br>• LTE: 326 Mbps down/86 Mbps up<br>• LTE-Advanced: 1 Gbps /500 Mbps | • HSPA+: 0–5 km<br>• LTE-Advanced: optimum 0–5 km, acceptable 5–30, 30–100 km (reduced performance) | • HAN, BAN, IAN, NAN, FAN, AMI | • Supports millions of devices<br>• Low power consumption of terminal equipment<br>• High flexibility, suitable for different use cases,<br>• Open industry standards | • High prices to use service provider networks<br>• Increased costs since the licensed spectrum |
| **Satellite** | • LEO: Iridium, Globalstar,<br>• MEO: New ICO<br>• GEO: Inmarsat, BGAN, Swift, MPDS | • Iridium: 2.4–28 kbps<br>• Inmarsat-B: 9.6 up to 128 kbps<br>• BGAN: up to 1 Mbps | • 100–6000 km | • WAN, AMI | • Long distance<br>• Highly reliable | • High cost of terminal equipment<br>• High latency |

**Figure 2.4:** Smart grid communication technologies [1]

use a low-overhead protocol, transmission-only modes and long-range sub-GHz transmission bands which makes them require low energy, hence a recommended standard for the metering application [21].

DLMS is an application layer specification consisting of the general concept for communication between entities. Thus, it is concerned with procedures for data exchange and access services for the smart devices. The Companion Specification for Energy Metering (COSEM) provides an object data model for implementing necessary metering functionality for the DLMS layer [21].

OSGP is an application layer specification defined by the ISO/IEC 14908 standard and is primarily used in smart metering applications as well as other smart grid devices. The encryption scheme used by OSGP is RC4 stream cipher and uses a non-standard digest function for message authentication. This differs from that used in DLMS/COSEM. This makes the protocol stack lightweight in comparison [22].

## 2.3 Security Requirements

The smart grid, as already explained, is made up of a myriad of interconnecting devices such as sensors and monitors which share data. The data shared includes energy consumption information, locations of faults, the status of relays, etc. All the interconnecting devices in smart grids are susceptible to attacks [23]. The major security requirements in smart grid are the CIA triad (Confidentiality, Availability, and Integrity). An explanation of each of the requirements is given below:

- ***Confidentiality:*** Ensuring that data is inaccessible to unauthorized persons. Depending on the type of data, a loss of confidentiality could result in a breach of customer privacy or sensitive details about the system.
- ***Integrity:*** Integrity in context of the smart grid means ensuring accuracy and trustworthiness of information by preventing data alterations or destruction by unauthorized persons. Integrity loss results in false or modified data which in turn could can affect power management
- ***Availability:*** Ensuring that power and/or data continues to be transmitted regardless of the state of the system. It is regarded as the most important security criterion in the smart grid due to the fact that compromising availability disrupts access to information in a smart grid [2]

The authors of [24] make a case as to why accountability should be considered as a requirement. As such, an explanation of some of these added requirements is given below:

- ***Accountability:*** Ensuring that every action is traceable and cannot be disputed. This is useful in events where there are discrepancies between data sent by different sources.
- ***Authentication:*** Ensuring that both parties involved in communication are who they claim to be by validating their identities. Loss of authentication can grant adversary access to information and/or allow him to connect illegitimate device to the smart grid.

### 2.3.1 Security Threats

Understanding the cycle of a cyber attack is key. Generally, there are four steps by which a cyber attack is implemented. These steps, shown in Figure 2.5, are reconnaissance, scanning, exploitation and maintaining access [2]. The first step, reconnaissance, involves information gathering about the target system either through social engineering or traffic analysis. Scanning, the next step, is done to probe the target system in search of vulnerabilities. Exploitation is where the smart grid's vulnerabilities discovered in the previous step is exploited. After this is done, an attacker then attempts to obtain permanent access to the target in the maintaining access stage.

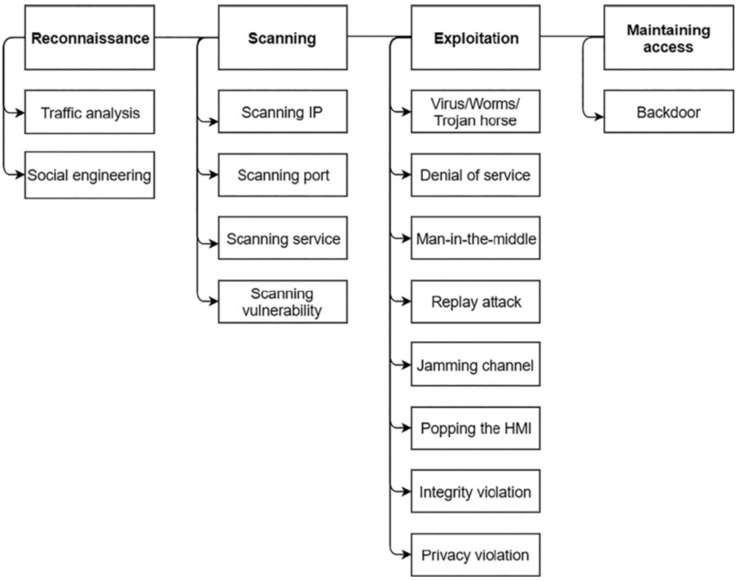


**Figure 2.5:** Attack cycle and related cyber attacks [2]

Cybersecurity threats to can be mapped to the 3 major security requirements discussed in section 2.3 as shown in Figure 2.6.

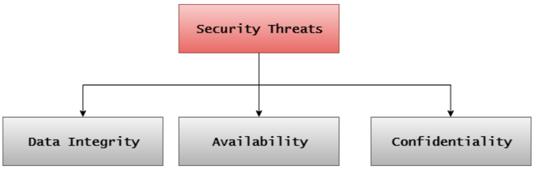


**Figure 2.6:** Mapping of smart grid threats to security requirements

### Network Availability

Threats against network availability aim to make resources unavailable for nodes that need transmitting data. This can be done by blocking transmission, delaying transmission or flooding the network with messages to consume network bandwidth and CPU resources thereby making the system inaccessible. These threats can be generally considered as Denial of Service (DoS). DoS is the most common and one of the worst attacks in the smart grid network [23, 25] . The smart grid allows easy connection to the communication network and as such it is very easy to launch DoS attacks against the smart grid [26]

### Data integrity

Threats against data integrity targets data which includes device running status, voltage readings, energy consumption and pricing information. The goal is to modify these data in the smart grid. Data integrity attacks can be accomplished using Man-in-the-middle attacks, Replay attacks, Masquerading attacks and Rogue access points and malicious software

### Confidentiality

Threats against confidentiality targets similar data being transmitted compared with data integrity attacks. The difference is that the attacker does not try to alter information that is transferred but only eavesdrop on the communication network to attain the desired information. As such these attacks do not hamper the smooth running of the grid and may not lead to massive consequences such as a blackout. This can be accomplished by using rogue nodes or malicious software.

# Chapter 3
# Methodology

This chapter specifies the process to undertake so as to arrive at suitable answers to the research questions enumerated at the start of this thesis. Tools that are employed to aid the project are also documented. The topics included in this chapter are: Research Methodology, Risk Modeling Techniques, Risk and Threat Identification and Threat Exploration.

## 3.1 Research Methodology

This section throws light on the research methodologies that are used in accomplishing the research objectives of this thesis; thus identifying security risks in a smart grid using a suitable modeling technique as well as identifying what attacks an attacker can use to exploit the smart grid.

The research is done in a coherent manner to ensure that logic is applied in comparing security risk modeling techniques as well as in choosing a suitable technique to be used in identifying security risks in the smart grid. Furthermore, this also ensures that the logic is applied in identifying and analysing attacks against the smart grid. By so doing, the result is credible and can be verified. The research methods used in this thesis are:

- A literature review of different modeling techniques used for security analysis is primarily done. This is done so as to give an insight as to which modeling technique should be adopted in analysing the security risks in a smart grid as well as threats which aim to compromise the smart grid. A qualitative research approach where a document analysis of security modeling techniques and their implementations, obtained from journals and articles, is key to answering research question 1. Qualitative research is chosen due to it's exploratory and data-driven nature [27]. Documents are practical, manageable, cover a long span of time and require data selection instead of data collection [28]. This makes document analysis an efficient and effective way of obtaining data.

- This is followed by an exploratory case study on a section of the smart grid, the AMI network. An exploratory case study is adopted because it sets out to explore any phenomenon which serves as a point of interest to the researcher [29]. This is done to analyse how the security risks and threats compromise this section of the grid. The analysis and documentation of the security threats and risks of the smart grid are done using CORAS tool[1], an open source diagramming applications for CORAS diagrams.

- Lastly, a literature study is used to explore the attacks the smart grid is susceptible to, which have been discussed in publications. The aim of doing this is to identify the various attacks that can be employed to attain an attacker's goal of compromising the smart grid security requirements. The findings are used in constructing an attack tree which presents an overview of the relationship between the various attacks.

### 3.1.1 Risk Modeling Techniques

A literature review is a research method that is used to address the research problems by identifying, critically assessing and combining the findings of all relevant studies. Thus, a literature review is used in this thesis to explore various security modeling techniques and its applicability in smart grid security. The end goal is to identify which of the technique provides the best framework for exploring security risks in the smart grid. The review adopts the five steps proposed by Khalid et. al. in their article [30] to answer research question 1. These steps include:

- **Step 1 : Framing the question**
  This step requires that the objective of the review is specified in the form of unambiguous questions. Questions developed include:

  1. What is the aim of the security related research conducted.
  2. What modeling technique is used by the research in identifying security risks.
  3. How is the modeling technique used in security analysis.

- **Step 2: Identifying relevant work**
  This step requires that extensive search is done. An electronic search of security modeling techniques in all published articles and reviews is conducted, using

[1] The tool can be downloaded from http://coras.sourceforge.net

the electronic databases **IEEEXplore**[2] and **SpringerLink**[3]. IEEE Xplore is a research database with text access to publications covering a wide range of topics in engineering and technology domain. It is chosen as one of the sources because it provides web access to over 4.5 million technical literature in engineering and technology. SpringerLink is also chosen because it is one of the world's most comprehensive online collection of scientific, technological and medical publications.

The electronic search of security modeling techniques conducted follow the procedure shown in Figure 3.1. A quick trial search is performed on **Google Scholar**[4] using keyword *'Security modeling'* to get a rough estimation of the number of related articles as well as the different security risk modeling techniques. Based on the results, the keywords is refined to include each of the modeling technique to be reviewed. Thus the keywords used are "attack tree security", "petri nets security", "game nets security", "bow tie security", "CORAS security", and "uml security". Table 3.1 shows the number of hits each of the keywords returned from the databases.

| **Search Keyword** | **IEEEXplore** | **SpringerLink** |
|---|---|---|
| 'attack tree security' | 718 | 4,165 |
| 'petri nets security' | 391 | 928 |
| 'game nets security' | 66 | 4,672 |
| 'bow tie security' | 5 | 340 |
| 'CORAS security' | 25 | 36 |
| 'uml security | 325 | 1,243 |

**Table 3.1:** Number of articles based on the pilot search in various digital libraries

- **Step 3 : Assessing the quality of studies**
  This step aims to filter the number identified related articles based on specified criteria and quality checklist. The following criteria are used :

  1. Article must contain research relating to risk analysis using a modeling technique
  2. Article must contain a case studies application of a modeling technique for security analysis
  3. Article must be in English

[2] https://ieeexplore.ieee.org
[3] https://link.springer.com
[4] https://scholar.google.no

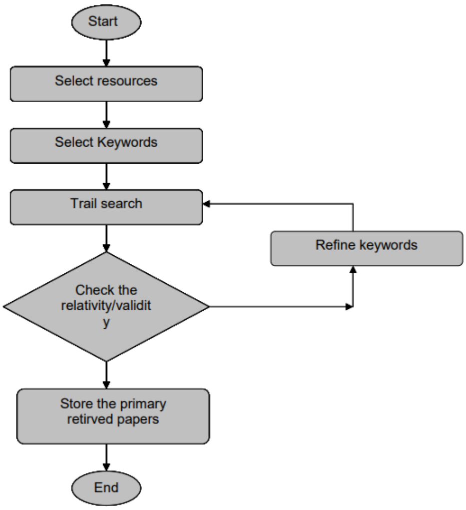


**Figure 3.1:** Search strategy for finding relevant articles [3]

The title of each article is subjected to filter criterion 1. The abstract and conclusion of articles that meet criterion 1 is read and filter criterion 1 re-applied. The filtered articles is then subjected to criterion 2 and 3 by skimming through the body of the paper. This, in turn, reduces the final articles chosen to 26 after which further analysis is performed.

- **Step 4: Summarizing the evidence**
  A summary of the results is presented based on groupings in Table 3.2 and the differences between the groupings are explored.

  - **Research Objective:** Papers are first classified based on the objective of the research either as 'base model implementation' or as 'proposal and implementation of extensions to established methods'. As the naming implies, the papers are grouped by whether the research is based on implementation using established methods or tweaking of the established methods.
  - **Modeling Technique:** This grouping classifies articles based on the modeling technique that is implemented in the paper. These include attack tree, bow-tie, CORAS, petri-nets, game nets and Unified Modeling Language (UML).
  - **Applied Method:** All the papers are then evaluated based on how they are applied. The evaluated groupings are (i)Asset identification, (ii)Risk identification, (iii)Risk evaluation and (iv)Mitigation steps. Asset identification involves identifying items of value that the stakeholders of

target system have interest in protecting. Risk identification involves discovery and documentation of the key threats that pose danger to the assets. Risk evaluation involves assessing the risks in terms of probability of risk occurrence or consequence of risk occurrence or both. Mitigation steps involve the implementation of countermeasures to either prevent the asset from being compromised or reduce the likelihood of it happening.

| **Classification** | **Sub Categories** |
|---|---|
| Research Objective | implementation of base model and implementation of extensions |
| Modeling Technique | Attack tree, CORAS, Petri-nets, Game-Nets and UMLactivity diagram |
| Applied Method | Asset identification, Risk identification, Risk evaluation, Mitigation steps |

**Table 3.2:** Classification of security modeling research papers and articles

- **Step 5: Interpret the findings**
  This step addresses the question posed in step one without any bias so as to provide validity to the result.

### 3.1.2 Risk and Threat Identification

Exploring the security risks and threats in a smart grid is done by application of the CORAS method which facilitates the analysis of security risks. In order to limit the scope of our analysis, a constructed case study of the AMI section of the smart grid is done to which the CORAS method is applied. An overview detailing the specific communications technology applicable to the utility company's AMI is first described. This ensures that the threats and risks associated with the AMI using these communication technologies can be identified. Next, a section of the CORAS methodology is applied to the AMI network. The complete CORAS method can be divided into seven steps [4] as shown in Figure 3.2. A brief insight as to what each step entails and how it is used in the case study is given below:

- **Step 1:** The first step is an introduction meeting which sets up preparations for a risk analysis. The participants of this meeting include representatives of the target system and security analysts. The objective of this step is to have an overview of the target AMI system and what analysis will be performed.

- **Step 2:** The second step, also a meeting with customer representatives, is set up to allow the security analysts the opportunity to present their understanding of customers requirements. The objective is to attain a uniform agreement on what the target system is as well as what the analysis should be about. Thus, a high-level analysis consisting of threats, vulnerabilities and unwanted events is performed.

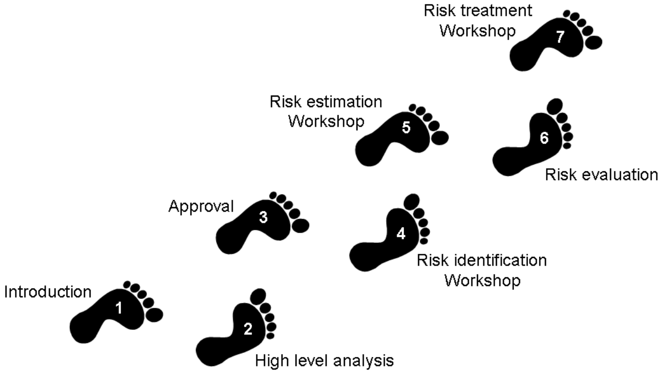


**Figure 3.2:** CORAS method for security risk analysis [4]

- **Step 3:** The third step involves a more refined description of the target system to be analysed together with the assumptions and preconditions that are made. This step concludes after the customer is satisfied with the documentation and approves it.

- **Step 4:** The fourth step involves identification of risks. This is done through a workshop where brainstorming of the target system is done typically with experts on the target system. The aim of this step is to identify vulnerabilities, undesirable events, threats as well as threat scenarios.

- **Step 5:** The fifth step involves estimation of risks. This, also done through a workshop, is done with the objective of estimating the probability of occurrence of undesirable events as well as the consequences that will arise as a result.

- **Step 6:** The sixth step involves evaluation of risks. The objective is to analyse whether the risks that are identified are acceptable.

- **Step 7:** The final step involves identification of treatments or countermeasures to reduce the likelihood of risks that are unacceptable. Furthermore, the cost-to-benefit of the treatment is also evaluated.

In answering research question 1, steps 5, 6 and 7 are skipped. This is because steps 5 and 6 are purposeful for presenting the probability of occurrence of the risks while step 7 leans towards identifying mitigation steps for the risks. The objectives set out in these steps is out of the scope of this research question. The CORAS tool is used to present the risks associated with the AMI network. Chapter 5 gives a brief insight into the components and usage of CORAS tool software. Learning the semantics of this tool was thus essential to completing the research objective.

### 3.1.3 Threats Exploration

A comprehensive literature review is performed on articles published on **IEEEXplore** is done so as to answer research question 2. An overview of the attacks and how they are related is presented using an attack tree. The attack tree aids in visualizing which attacks can be employed to achieve an attackers' objectives. Developing an attack tree involves several steps, one of which is the need to break down the high-level goal resulting in low-level attacks an adversary executes to attain the high-level goals. The mapping of the attacks to the goal results in an attack tree. The methodology used in creating the attack tree is given below:

- **Define the system:** The definition of the system is done using a high level of abstraction. The target system used is the entire smart grid.
- **Identify type of attacker:** Since different attackers have different goals, identifying the various types is done. The attacker types in the smart grid include a network attacker (an attacker who targets the communication network), a physical attacker (an attacker looking to cause physical harm to the system) and a software attacker (an attacker that targets and exploits vulnerabilities in the software running on various systems).
- **Identify the goals of the various attackers:** Each of the identified attacker types is explored so as to deduce their goals. Furthermore, attacks which comprise the overall goals are investigated. The attacks are continuously decomposed into smaller and smaller tasks which produce an overview of attacks and sub-attacks is an attack tree.
- **Attacks** A literature review of attacks that can be used to accomplish each of the goals is done. This is done so that all the attacks that can be used to accomplished the goal is included in the attack tree. Steps described in section 3.1.1 are also applied here. A query of IEEE Xplore using 'smart grid attack' is done with restrictions to publications made within the last 3 years. The query returned 750 results. Two (2) selection criteria are used in filtering the articles. The first criterion is that the articles must have the keywords either in the title or the abstract of the paper. The second criterion requires the articles to

discuss the attack. The 84 selected articles are classified into categories using the classification scheme in Table 3.3. After grouping according to Table 3.3, a chart showing the percentage of shares is done. The objective is to identify important information as to which fields are the focus of research.

- **Research Year:** The first grouping is done based on the year of publication of the articles. This is done to evaluate whether trends exist that piques future research
- **Research Type:** This grouping classifies articles either as 'modeling/simulation' if it is based on mathematical functions or simulation or as 'survey/review' if it lacks a case study implementation of an attack
- **Security Requirement:** Papers are then classified based on the security requirement the attacks target. The three main categories are confidentiality, availability, and integrity
- **Attacks:** Finally, All the papers under each of the security requirements are grouped based on the attack they present.

| **Classification** | **Sub Categories** |
|---|---|
| Research Year | 2018, 2017, 2016 and 2015 |
| Research Type | Modeling and Survey/Review |
| Security Requirement | Confidentiality, Integrity and Availability |

**Table 3.3:** Classification scheme used for research papers and articles

# Chapter 4
# Security Risk Modeling

This chapter presents theory of risk modeling techniques that are used in security risk assessment as well as the results of the literature review of risk modeling techniques. This chapter contains three (3) main sections: Modeling techniques, Review of security risk modeling techniques and Choice of suitable modeling technique. Thus, this chapter presents and reviews six (6) modeling techniques: UML Activity Diagram, Attack Trees, CORAS, Petri-nets, Game-nets, and Bow-Tie.

## 4.1 Modeling Techniques

Understanding real-world systems can prove difficult. This is due to the fact that representing massive data for easy understanding as well as obtaining needed information from the data can be a daunting task depending on the way the data is represented [31]. There is no easy way of making systems easier to comprehend but there are a variety of techniques that provide significant aid in understanding complex systems. Visualization, a representation of an object or set of information as an image, is a powerful tool that provides easy understanding of data as well as interpretation complex set of data.

Utilizing visualization for security analysis of computer and information networks can be accomplished in a plethora of ways. One such method is the use of security models. Security modeling is a procedure for optimizing security whereby a definition of the system behaviour as well as an attacker's intents and capabilities are clearly defined. In addition, the system properties which the attacker intends to compromise are defined [32]. This ensures that risks, as well as countermeasures that ensure that the risks can either be prevented or mitigated, can be identified. Security risk modeling techniques include bow-tie, activity diagram, petri-nets, game-nets, CORAS and attack trees. An overview of these modeling techniques is given below after which a literature review of how these techniques are used in research is presented.

### 4.1.1 UML Activity Diagram

UML activity diagram, inspired by Jim Odell time diagram, is a type of process modeling language that is used in various stages of Object Oriented Development Method. Activity diagram, thus, can be used to model the dynamic behavior of systems as well as business processes [33]. There are a number of variations and extensions of UML activity diagrams that have been used in research for security analysis. Among these include Systems Modelling Language (SysML) activity diagram, Malicious Activity Diagram (MAD) and Security Oriented Malicious Activity Diagram (SOMAD)

SysML activity diagram reuses a subset of UML packages and covers four aspects of system modeling namely structure, behavior, requirement and parametric diagrams. SysML activity diagrams can be split into two parts: activity nodes and activity edges [34].

MAD are extensions of UML activity diagram used during information system designing stage to model security treats. Changes MAD brings to UML includes constructs such as Mal-Activity, Mal-Swim lane, Mitigation Activity and Mitigation Link. Mal-Activity defines malicious activities targeting the assets, Mal-Swim provides the definition of the malicious process while Mitigation activity and Mitigation Link provide the definition of the mitigation process. SOMAD is an extensions for MAD with the purpose to support security of information systems. MAD lacks constructs for some important information system security risk management domain models such as vulnerability, threats, and security criterion. These missing constructs are included in SOMAD [35].

### 4.1.2 Attack Trees

Attack trees, introduced by Bruce Schneier, defines an easy way model treats against computer systems [36]. Attack trees is a diagram that depicts possible ways an attacker can reach his target. After, comprehending the myriad ways to compromise the system, better countermeasures can be defined to combat the attacks. Attack trees, like the name suggests, uses a tree structure to model attacks against a system whereby the goal of the attacker is the root node whereas the varied paths to achieve the goal is the leaf node. Attack tree adopts two Boolean operators, **OR** and **AND**, in constructing the tree. **OR** nodes represent choices or alternatives whereas the **AND** nodes represent various ways to attain the same goal. Each node becomes a sub-goal, and children of that node are ways to achieve that sub-goal.

After the attack tree is completed, attributes and values can be assigned to each leaf node. Attack attributes assist in associating risk with an attack while values can be used to compute the security of the goal. The values in the attack tree could take the form of operational or development expenses. An attack tree can also include special knowledge or equipment that is needed for an attack, the time required to complete the attack, and the physical and legal risks assumed by the attacker. Furthermore, attack trees support design and requirement decisions. If an attack costs the perpetrator more than the benefit, that attack will most likely not occur. However, if there are easy attacks that may result in benefit, then those need a defense [37].

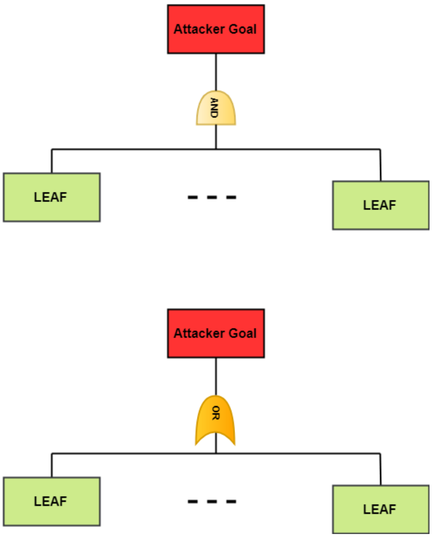


**Figure 4.1:** Atomic structure of an Attack Tree

### 4.1.3 CORAS

CORAS is a framework for analysing security risk which consists of three main parts. These are (i) a methodology for analysing risks (ii) a customized visual language for modeling risks and (iii) a tool that supports the language [38].

The methodology combines some aspects of techniques for complementary risk analyses with UML. This combination of different risk analysis methods make it possible for the analysis of varied aspects of a system which includes security [39].

The CORAS language helps to elaborate the rationale behind different aspects of risks. These include relevant information needed to identify and understand risks, what causes the risk and sufficient ways to deal with risks. The language provides options for a variety of diagrams. Each diagram is applicable to specific aspects of the risk analysis and is usually linked in a chain. The basic CORAS language is made up of five diagrams; *asset diagram*, *threat diagrams*, *risk diagrams*, *treatment diagrams* and *treatment overview diagrams* [40].

The tool is used in performing security analysis in accordance with the CORAS methodology using the graphical CORAS language. A detailed presentation of the tool and its applicability is presented in [39].

### 4.1.4 Petri-Nets

Petri-Nets (PN) is a quantitative model which was first introduced by Carl Adam Petri for the purpose of presenting chemical process. However, PNs have been used in modeling a variety of systems due to its versatility in expressing different relationships. Basic Petri nets consist of two distinct nodes that are connected together by arcs. The first node (places) represents the system state or object and the second node (transitions) represents the transition which determines the system dynamics. The two nodes are connected via directed arcs. PN are good for modeling concurrent, asynchronous, non-deterministic and stochastic systems [5]. As such there are a number of extensions of PN that have been used in research. These extensions associate each transition with additional variables. These extensions include Colored Petri Nets (CPN), Probabilistic Petri-Nets (PPN), Weighted Petri nets, Time Petri-Nets (TPN) and Stochastic Petri-Nets (SPN).

Weighted Fuzzy logic replaces the Boolean logic of Petri-net with fuzzy logic [41] whereas with CPN, tasks such as formal analysis of system behavior properties, simulation-based verification, and time-related aspects can be achieved [42]. Both SPN and TPN add a time factor to transitions. The difference SPN and TPN between them is that SPN make use of random delay while TPN use time intervals. The transition will not be fired immediately after receiving system resources but only after the timer has expired [43]. PPN nets add probabilities to inputs of a transition and are introduced in [5] for safety analyses. PPN has two basic relationships are defined; 'AND' relationship and 'OR' relationship. These relationships work just as described in attack tree and this makes PPN a model that can be employed in answering research question 2.

Basic PN is defined as a five-tuple vector [5]:

$$PN = (P, T, In, Ot, M) \tag{4.1}$$

where:

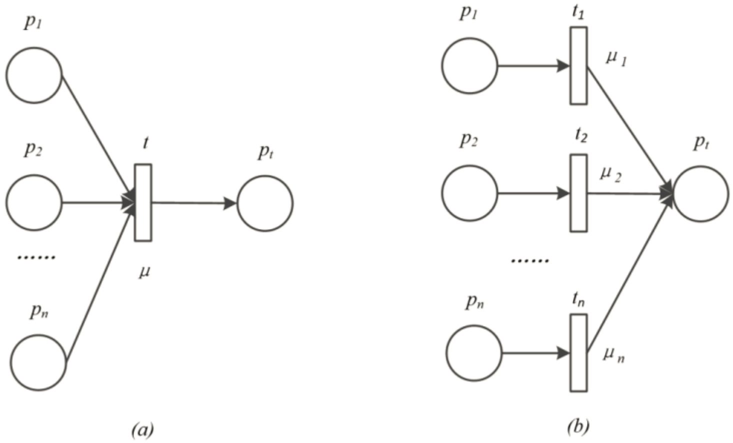


**Figure 4.2:** *"AND"* and *"OR"* relationship modeling in PPN [5]

1. $P$ is a finite set of places, $P = \{p_1, p_2, ..., p_n\}$ is a finite set of places.

2. $T = \{t_1, t_2, ..., t_m\}$ is a finite set of transitions, where $m$ is the number of transitions.

3. $In$ is an $n\ x\ m$ **input** matrix determining the directed arcs from places to transition, $In = P * T \to \{0, 1\}$

4. $Ot$ is an $n\ x\ m$ **output** matrix determining the directed arcs from places to transition, $In = P * T \to \{0, 1\}$

5. $M : P \to \{0, 1\}$ is a marking vector

Extending PN to PPN adds two more vectors to make a 7-tuple vector [5]. Thus:

$$PPN = (P, T, In, Ot, M, A, U) \tag{4.2}$$

Where:

- *P, T, In, Ot, M* maintain the same definition under PN above.

- $A$ is a probability vector. $A = (\alpha_1, \alpha_2, ..., \alpha_n)$, where $\alpha_i \in [0, 1]$ means the probability of $p_i = 1, 2, ..., m$

- $U : T \to \{0, 1\}$ is a certainty vector. $U = (\mu_1, \mu_2, ..., \mu_m$ , where $\mu_i \in [0, 1]$

### 4.1.5 Stochastic Game-Nets

Stochastic Game-Nets (SGN), also a quantitative and visual communication tool, can be used to model the relationship between two entities and analyse the associated risks. Thus, SGN can be used to enhance understanding of complex dynamic networks and systems. SGN combines the advantages of SPN with the advantages of game theory thereby improving the efficacy of security analysis [6]. As such SGN adopts PN's model in that, it also uses transitions and places as well as arcs that connect them. SGN is popular for its powerful modeling and analysing ability which is very useful for modeling and analysing complicated and dynamic game problems. Thus, SGN is effective for describing prioritized, concurrent, asynchronous and stochastic events [44].

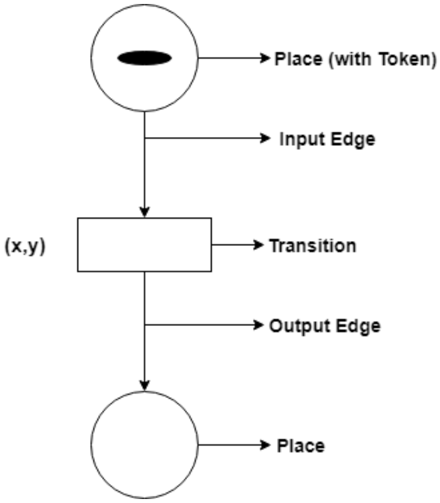


**Figure 4.3:** Basic Stochastic Game Nets [6]

The definition of stochastic game net is presented in [45] using a nine-tuple vector as given below:

$$SGN = (N, P, T, F, \pi, \lambda, R, U, M_0) \tag{4.3}$$

where:

1. $N = \{1, 2, ...n\}$ represents the set of players,
2. $P = \{P_1, P_2, ..., P_n\}$ is a finite set of places
3. $T = \{T_1 \cup T_2 ... \cup T_m\}$ is a finite set of transitions where $T_k$ is the set of transitions with respect to player k for $k \in N$,

4. $\pi : T \rightarrow [0, 1]$ is a routing policy representing the probability of choosing a particular transition

5. $\lambda = \lambda_1, \lambda_2, ..., \lambda_w$ is a set of firing rates of transitions where $w$ is the number if transitions

6. $R : T \rightarrow (R_1, R_2, ..., R_n)$ a reward function for the players taking each transition, where $R_i \in (-\infty, +\infty)$

7. U is the utility function of players,

8. $M_0$ is the initial marking, which denotes the initial state of the players

9. $F \subseteq I \cup O$ is a set of arcs, where $I \subseteq (P * T)$ and $O \subseteq (P * T)$ such that $P \cap T = \phi$ and $P \cup T \neq \phi$, where $\phi$ is an empty set, for a convenience, we denote $\bullet x = \{y|(y, x) \in F\}$ the pre-set of x, similarly, $x\bullet = \{y|(x, y) \in F\}$ the post-set of x

### 4.1.6 Bow-Tie

Bow-Tie is a visual tool that is primarily used to model an accident scenario. The scenario begins with causes of the accident and concludes with the consequences of the accident while having the accident event as the center. Thus, with the undesirable event in the center, bow-tie is made up of *Fault Tree* on the left side of the event and *Event Tree* on the right side of the event. The fault tree focuses on identifying the possible event that results in the critical event while the event tree focuses on the probable consequences of the critical event based on whether the safety barriers are successful or a failure [46]. Figure 4.4 shows a basic bow-tie diagram having fault tree with Basic Event ($IE$) which results in an Event ($E$) which has the potential to cause the Undesirable Event ($UE$). The Event tree consists of a dangerous phenomenon ($DF$).

## 4.2 Review of Security Risk Modeling Techniques

The 26 papers that are selected for review cover application of modeling techniques for security risk analysis. The applications cover a wide range of target systems such as SCADA system, Online Banking System, Cyber-Physical System, Smart-card payments, etc. Each of the papers is reviewed by analysing the research goals, the context of study as well as the results obtained. The studies are evaluated based on the following groupings: (i) Asset Identification (ii) Risk identification (iii) Risk evaluation (iv) Mitigation steps

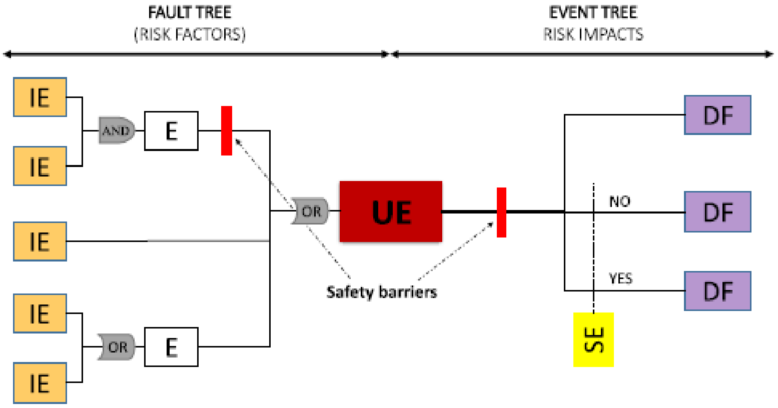


**Figure 4.4:** Bow-Tie diagram [7]

### 4.2.1 Findings & Analysis

The review methodology described in section 3.1.1 is used here to analyse the various security modeling techniques. The review of 26 articles is done with reference to the questions posed in step 1 which concern (i) The aim of the security-related research conducted and the system it is conducted on, (ii) The modeling technique used in identifying security issues and (iii) The methodology used in security analysis.

The results, obtained in step 4 of the methodology, details how these questions are addressed. These are discussed in the subsequent sections.

#### Aim of the security related research conducted

All chosen articles are grouped into two categories: (i) The proposal and/or application of an extension to an existing method (ii) Application of the existing base method.

The reason for grouping into these categories is to explore and attain an in-depth understanding of the rationale behind the research. Each article's title, abstract, research method, result and conclusion are reviewed so as to attain the focus of the study. The result of the categorization is shown in Table 4.1. This table also includes the target system of the research. This is useful as it gives a premise for further analysis as well as give information that may be useful for researchers who may be interested in research on a particular system. Analysing the result shows that there is a marginally higher percentage of research (56%) conducted using an established base modeling technique as compared to the percentage of research that proposes and implemented extensions to the established modeling techniques (44%). With

| **Research objective** | **Article** | **Use-case/ Target System** | **Number** | **Percentage** |
|---|---|---|---|---|
| Proposal and/or implementation of extensions to established methods | [47] | Smart Car | 12 | 46.15% |
| | [48] | Smart Homes | | |
| | [49] | Oil Pipeline | | |
| | [50] | SCADA System | | |
| | [51] | Cloud Security | | |
| | [52] | Time-stamp Services | | |
| | [53] | University System | | |
| | [54] | Web Registration | | |
| | [55] | Mobile Communication | | |
| | [56] | Smart-card payment | | |
| | [57] | Online Banking System | | |
| | [58] | Petroleum Company | | |
| Application of the existing base method | [59] | Vehicular Ad hoc Networks | 14 | 53.85% |
| | [60] | Mobile System | | |
| | [61] | Online Banking System | | |
| | [62] | Forwarding and Control planes Separation Network Structure in SDN | | |
| | [63] | Homeland Security | | |
| | [64] | Smart Identifier Network | | |
| | [65] | Spam Filter Security | | |
| | [66] | Cyber Physical System | | |
| | [67] | E-commerce System | | |
| | [68] | Power System | | |
| | [69] | Enterprise Network | | |
| | [44] | Web Services | | |
| | [70] | SCADA | | |
| | [71] | Maritime Communication | | |

**Table 4.1:** Research Purpose and Target in relation to modeling techniques

regards to target system of analysis, four (4) of the research papers use payment systems as the target system while another three (3) use cyber-physical systems as case studies. These findings are discussed further in section 8.1.

### Modeling Techniques used

Table 4.2 shows the type of modeling technique used by the research in analysing the security of a system. The result shows that attack trees modeling technique is the most frequently used modeling technique in research with a share of 38.46%. UML activity diagram and game-nets followed with a 15.38 % each. This is followed by CORAS and petri-nets attaining 11.54 % each. Research using bow-tie represent the least with 7.69%.

| **Index** | **Modeling Technique** | **Reference** | **Total** | **Percentage** |
|---|---|---|---|---|
| 1 | Attack Tree | [47], [48], [49], [50], [51], [60], [61], [62], [59], [63] | 10 | 38.46% |
| 2 | CORAS | [52], [67], [68] | 3 | 11.54 % |
| 3 | Bow-Tie | [58], [71] | 2 | 7.69 % |
| 4 | Petri-Nets | [64] [65] [66] | 3 | 11.54% |
| 5 | Game-nets | [57], [69], [44], [70] | 4 | 15.38% |
| 6 | UML Activity Diagram | [53], [54], [55], [56] | 4 | 15.38% |

**Table 4.2:** The modeling techniques used in research articles

### Application of visualization technique

Table 4.3 shows how the techniques are used in the research. All 26 research papers employ the modeling techniques for asset identification. 25 out of 26 papers, representing 96.15%, identify and represent risks using their chosen modeling technique. The paper that fails to do so, [53], uses UML activity diagram for only asset identification. Fifteen (15) out of the total (26), representing 57.67%, go on to demonstrate how the identified risk could be evaluated. Finally, with regards to presenting mitigation steps to reduce the likelihood of risks, only seven (7) out of the total (26), representing 26.92% implement this.

It can also be seen from Table 4.3 that UML based research papers are never used in risk evaluation and mitigation steps. Even with risk identification, only three (3) out of four (4) model this. All game-nets related paper touch on both asset identification as well as risk identification but all of them fail to implement mitigation procedures for the identified risks. Two (2) out of the four (4) implement risk evaluation. All three (3) Petri- nets related paper, as well as all two (2) bow-tie based papers, implement asset identification, risk identification, and risk evaluation. However, all these five (5) papers fail to address mitigation of the risks. It can be noted that only CORAS and attack tree based research uses all four security

| **Modeling Technique** | **Reference** | **Asset Identification** | **Risk identification** | **Risk Evaluation** | **Mitigation Steps** |
|---|---|---|---|---|---|
| Attack Trees | [47] | ✓ | ✓ | ✓ | |
| | [60] | ✓ | ✓ | | |
| | [50] | ✓ | ✓ | ✓ | ✓ |
| | [61] | ✓ | ✓ | | ✓ |
| | [62] | ✓ | ✓ | | |
| | [48] | ✓ | ✓ | ✓ | |
| | [59] | ✓ | ✓ | ✓ | |
| | [49] | ✓ | ✓ | ✓ | |
| | [63] | ✓ | ✓ | ✓ | ✓ |
| | [51] | ✓ | ✓ | ✓ | ✓ |
| CORAS | [67] | ✓ | ✓ | ✓ | ✓ |
| | [52] | ✓ | ✓ | ✓ | |
| | [68] | ✓ | ✓ | ✓ | ✓ |
| Bow-Tie | [58] | ✓ | ✓ | ✓ | |
| | [71] | ✓ | ✓ | ✓ | |
| Petri-Nets | [64] | ✓ | ✓ | ✓ | |
| | [65] | ✓ | ✓ | ✓ | |
| | [66] | ✓ | ✓ | ✓ | |
| Game-Nets | [57] | ✓ | ✓ | ✓ | |
| | [69] | ✓ | ✓ | ✓ | |
| | [70] | ✓ | ✓ | | |
| | [44] | ✓ | ✓ | | |
| UML Activity Diagram | [53] | ✓ | | | |
| | [54] | ✓ | ✓ | | |
| | [55] | ✓ | ✓ | | |
| | [56] | ✓ | ✓ | | |

**Table 4.3:** The methodology applied in research articles

modeling applications.

All three (3) CORAS papers touch on asset identification, risk identification, and risk evaluation. With regards to mitigation steps, two (2) out of three (3) papers touch on mitigation steps. The paper that fails to do so, [52], focuses on elaborating how various risk analysis solutions for individual components can be combined. All ten (10) attack tree based research focus on asset and risk identification. However, only four (4) out of ten (10), representing 40%, touch on mitigation steps while seven (7) out of the total touch on risk evaluation.

### 4.2.2 Choice of Risk Modeling Technique

Section 4.2.1 presents findings on how the different modeling techniques have been used in research for security risk analysis. The criteria for selecting one of the techniques as the suitable technique to aid in identifying and understanding security risks in the smart grid requires the use of modeling techniques that do not focus on the threats themselves but rather focuses on the perspective of the attacker. A threat focused modeling technique focuses on identifying mistakes in system design and development which may translate into vulnerabilities. Thus, this category of modeling technique allows an analyst to investigate system design and development in search of design vulnerabilities [72]. An attacker focused modeling technique, on the other hand, focuses on identifying all potential entry point to the system as well as the probable objective an attacker could have.

With this requirement, CORAS is the modeling technique to be applied in this answering research question 1. This is because CORAS, compared to the other modeling techniques in Table 4.2, was specifically designed as a model-based method for security risk analysis. This gives CORAS advantages over the others which is highlighted in [4]. These advantages include:

- CORAS provides precise target system descriptions, description of security context as well as the description of relevant security features in a format that is easy to access
- CORAS makes it easy to document risk assessment results and the underlining assumptions for the results
- CORAS provides graphical presentation of information which enhances understanding, communications and interactions between parties involved in the analysis.

# Chapter 5
# CORAS Language and Tool

This chapter gives an insight into CORAS language and tools. The chapter contains three (3) sections: CORAS Terminologies, modeling language and tool.

## 5.1 Terminologies

In order to understand and appropriately use CORAS security modeling, it is paramount to understand the basic concepts used. A summary of these concepts are given below:

- **Target system:** The information system on which the security analysis is going to be performed
- **Party:** Person or organization that requests the security analysis of the target system
- **Asset:** An item, either tangible or intangible, which the party regards as valuable and thus a focus of the security analysis.
- **Vulnerability:** A weakness of the system which exposes it to the possibility of being attacked.
- **Threat:** An entity, either human or non-human that exploits vulnerability of the system
- **Unwanted Incident:** A situation that poses a danger to the asset
- **Risk:** The likelihood of an occurrence of an unwanted incident
- **Consequence:** The negative effect an unwanted incident has on an asset
- **Treatment:** The choice and implementation of risk mitigation procedures.

## 5.2 Language

The CORAS language defines the syntax and semantics of CORAS diagram which gives the diagrams meaning [4]. CORAS defines five diagrams namely: Asset Diagram, Threat Diagram, Risk overview Diagram, Treatment diagram and Treatment overview diagrams. Each of these diagrams is made up of basic components as well as relations. Since the scope of this theses is limited to risk identification, only the components and relations of Asset Diagram, Treat Diagram and Risk Overview Diagram is discussed in the subsequent sections.

### 5.2.1 Asset Overview Diagram

The asset overview diagram is constructed using two components; parties and assets, and is used to provide an overview of the assets of the target system as well as the relations between them. These two basic components are interconnected using *values* and *Harm* relations. Values connect party to assets depicting assets that the party deems important. On the other hand, Harm is used to show which assets influence another [4]. Figure 5.1 presents the components of asset diagram as well as the relations

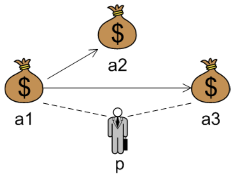


**Figure 5.1:** An overview of Asset Diagram [4]

### 5.2.2 Threat Diagram

A threat diagram is used to represent the sequence of events that pose a threat to assets. Thus, it starts with a threat and ends at the asset. A threat diagram has seven unique elements namely: deliberate threat, accidental threat, non-human threat, vulnerabilities, threat scenario, unwanted incidents and assets as shown in Figure 5.2.

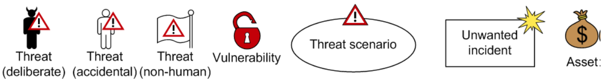


**Figure 5.2:** Basic Components of Threat Diagram [4]

Just like asset diagrams, threat diagrams are also interconnected using two relations: *LeadsTo* and *Impact*. A threat scenario is caused by a vulnerability that is exploited by a threat. When this happens the treat scenario may lead to an unwanted incident or another vulnerability that can be exploited. An unwanted incident affecting an asset impacts it. An example of a threat diagram containing all the events and relations is shown in 5.3.

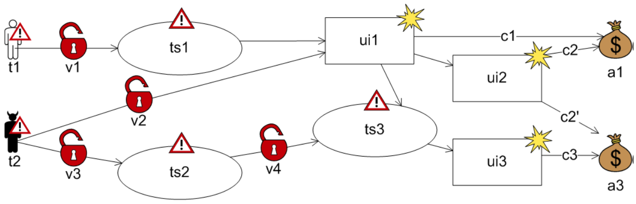


**Figure 5.3:** Initial threat diagram : A Threat Diagram example [4]

### 5.2.3 Risk Overview Diagram

A synopsis of a threat diagram is given by a risk overview diagram whereby all the risks that the threats posed to the assets are shown. These risks are given a risk value which represents its severity. A breakdown of the components of a risk diagram reveals five atomic elements namely: deliberate threats, accidental threats, non-human threats, risks, and assets [4]. These components are shown in Figure 5.4.

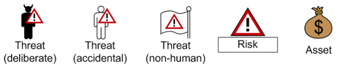


**Figure 5.4:** Basic Components of Risk Overview Diagram [4]

With regards to relations, risk overview diagram uses only one relation, *Impact*, which connects threats to risks and risks to the asset [4]. This shows which asset is impacted by which risk by which threat as seen in Figure 5.5.

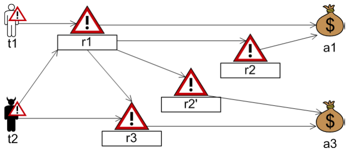


**Figure 5.5:** A Risk Overview Diagram example [4]

## 5.3 Tool

The CORAS tool[1] is an open source software which uses the graphical CORAS language. It was created to assist in performing security analysis in accordance with the CORAS methodology. This tool is developed in Java as a client-server model which allows a security analyst to create new analysis projects and generate reports among other features [39].

[1] The tool can be downloaded from http://coras.sourceforge.net

Chapter 6

# Case Study: AMI security risk modeling using CORAS

This chapter shows how CORAS can be applied to the smart grid. It presents a constructed case of AMI subsystem of the smart grid for which the security risks analysis is to be performed. This is then followed by a narrative of steps taken in analysing the risk associated with the AMI network using the CORAS method.

## 6.1 Introduction

In a small section of a fictitious country's electrical grid, a utility company, Grid Tech, has deployed a dedicated communication network to better serve their customers. Grid Tech prides themselves in the quality of service they offer to customers in terms of accurate dynamic pricing. The company installs smart meters in customer premises for more accurate billing of customers as well as to provide clients with dynamic pricing depending on demand. Each home connects to the energy grid via a Wi-Fi enabled smart meter for IoT. This allows the home area network devices (consisting of eg Washing machines, etc) to be able to communicate with the meter for pricing updates. Clients are allowed to choose between smart meters using Zigbee and WLAN for HAN. HAN A and B choose Zigbee while the others opt for WLAN.

Regardless of the wireless technology chosen for the home network, the smart meters are interconnected via a mesh network to communicate with the DCU. Each DCU, in turn, uses WiMAX to forward data readings to the control centers.

Figure 6.1 presents a high level view of the AMI network under investigation. The AMI's importance in the smart rid makes it a target for attackers. This is because it is responsible for real-time monitoring and control of the energy grid.

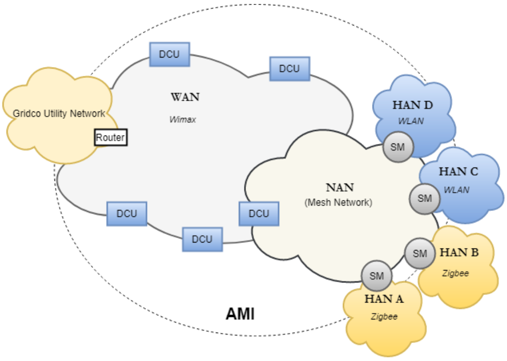


**Figure 6.1:** AMI network for Grid Tech

## 6.2 CORAS Implementation

The following sections how CORAS can be used to identify security risks in the AMI of Grid Tech

### 6.2.1 Step 1: Introduction Meeting

Defining the target system is the first thing to be done before exploring various ways it could be exploited. Defining the scope of analysis as well as the assumptions made is crucial in successfully identifying and analysing potential risks. A meeting is organized between representatives of Grid Tech company and the analysts where the utility company's representatives make a presentation explaining the target system shown in Figure 6.1. It is emphasized that, in addition to accurate billing (integrity of energy usage data), providing uninterrupted service (availability) is topmost priority.

### 6.2.2 Step 2: High-Level Analysis

The second meeting commences with the analyst providing his understanding of the target system. The high-level analysis is done to ensure that the focus and scope of the analysis are clearly understood. Assets, which include tangible and intangible objects, that Grid Tech values are clearly defined. This assists in identifying the risks associated with Grid Tech's AMI. Placing emphasis on the assets helps ensure that the scope is limited and thus the time spent in analyses focuses on identifying risks on these assets.

During the meeting, it becomes clear that accurate billing is what Grid Tech is most particular about. In addition to this, ensuring customer satisfaction by providing uninterrupted service is also of paramount importance. Furthermore, it is made clear that ensuring the privacy of customer data is not a priority. The assets of Grid Tech is presented in Figure 6.2. The threat Grid Tech is concerned about are hackers, system failure as well as communication network failure. Each asset is then taken in turn and a short brainstorming is done to identify the most important threats and vulnerabilities to each of the assets without going into details.

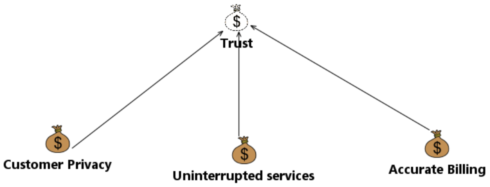


**Figure 6.2:** Asset diagram of Grid Tech's AMI

### Accurate Billing high level analysis

A high-level risk table for this asset is shown in Table 6.1. Exploiting this asset causes inaccurate energy usage records that are used in billing. This may result in a huge financial loss for Grid Tech if customers are under-billed. Alternatively, customers may be over-billed which could result in loss of customer's trust. Inaccurate energy usage records may be caused by hackers, sloppy employees or network failure as shown in Table 6.1

| **Who/What causes it** | **How? what does it affect?** | **Why is it Possible?** |
|---|---|---|
| Hacker | Breaks into system to inject or falsify billing records | Insufficient security |
| Sloppy Employee | Compromises integrity of billing records by mistakenly altering data | Carelessness |
| Network Failure | Transmission issues preventing billing records to be sent and received | Unstable connection |

**Table 6.1:** Accurate Billing High-Level Risk table

### Customer Privacy

A high-level risk table for this asset is shown in Table 6.2. Exploiting this asset provides access to customer information which allows the hacker to learn customer behaviors and patterns. This asset can be compromised by hackers or sloppy employees

| **Who/What causes it** | **How? what does it affect?** | **Why is it Possible?** |
|---|---|---|
| Hacker | Breaks into system to steal customer records | Insufficient security |
| Sloppy Employee | compromises confidentiality by leaking customer records | Carelessness |

**Table 6.2:** High-level risk table for Customer Privacy

### Uninterrupted Service

A high-level risk table for this asset is shown in Table 6.3. Exploiting this asset significantly reduces the availability of services to customers.

| **Who/What causes it** | **How? what does it affect?** | **Why is it Possible?** |
|---|---|---|
| Hacker | Breaks into system to overload the system with irrelevant data | Insufficient security |
| System Failure | System goes down making it unavailable | Hardware Fault |
| Network Failure | Transmission issues reducing availability | Unstable connection |

**Table 6.3:** High-level risk table for Uninterrupted Service

## 6.2.3 Step 3: Approval

This meeting is held between the analyst and Grid Tech representatives to ensure that all background information and documents are accurate. The documentation includes target system, risk, and scope of analysis. The result of the high-level analysis, asset value table as well as the risk evaluation criteria is sent to representatives of Grid Tech for approval.

### Asset Values

Using the asset diagram as input, each asset is ranked in order of importance to Grid Tech. This is done so that prioritization of risks associated with the assets as well as potential loses can be evaluated. Thus, an asset table is created as shown in Table 6.4.

| Asset ID | Asset Category | Asset Value |
|---|---|---|
| Customer Privacy | Information | Low |
| Accurate Billing | Information | Very High |
| Uninterrupted Services | Services | Very High |

**Table 6.4:** Grid Tech Asset Table

#### Risk Evaluation Criteria

Both parties agree on how potential risks will be evaluated. This is done so as to determine the risk level Grid Tech deems acceptable or unacceptable. The agreed criteria to determine the likelihood are given values from *Low*, *Medium* and *High* while that for consequences take on value from *Minor* , *Moderate* and *Major*. Since the scope of the analysis in this thesis does not include risk evaluation, this documentation is skipped.

### 6.2.4 Step 4: Risk Identification

This brainstorming meeting is set up to identify risks and how assets can be compromised. The analyst identifies how the vulnerabilities identified in the high-level analysis table can be exploited by the threats. Each of the assets is taken in turns and a threat diagram is developed.

#### Accurate Billing Risk Identification

Based on Table 6.1, initial threat scenario diagrams are created as starting points for further analysis. The diagrams are separated based on the threat to the asset as shown in Figure 6.3, Figure 6.4 and Figure 6.5.

The initial diagram in Figure 6.3 depicts how the assets can be compromised by a deliberate threat. An attacker who's objective is to steal energy must either prevent energy readings from being taken or modifying energy usage data while in transit to the utility. The prerequisite for energy theft to be accomplished is energy usage data modification. Exploring where and how data can be modified narrows it down to three methods:

- Interrupting measurement in smart meters so as to prevent readings from being taken
- Altering stored energy usage data in smart meter or
- Modifying data usage readings while it is being transmitted to utility companies.

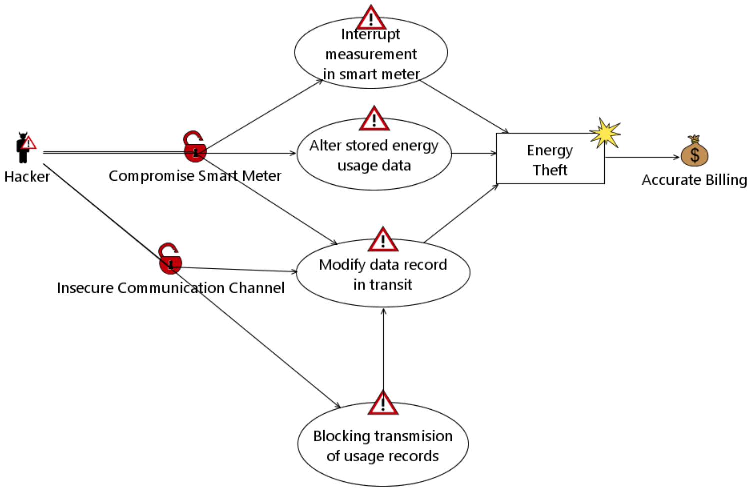

Interrupt measurement in smart meter
Hacker
Compromise Smart Meter
Alter stored energy usage data
Energy Theft
Accurate Billing
Insecure Communication Channel
Modify data record in transit
Blocking transmision of usage records

**Figure 6.3:** Initial threat diagram : Deliberate threats

The initial diagram in Figure 6.4 shows how the assets can be compromised by an accidental threat. An employee having write-access to energy record data may alter it either knowingly or unknowingly thereby resulting in compromising the integrity of data due to inaccurate data.

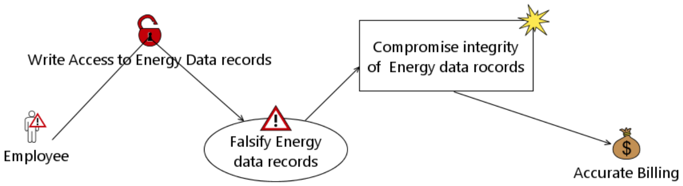

Write Access to Energy Data records
Compromise integrity of Energy data rocords
Employee
Falsify Energy data records
Accurate Billing

**Figure 6.4:** Initial threat diagram : Accidental threats

In addition to threats posed by humans, there are inanimate threats to this asset. The inanimate threats take the form of communication network failure as shown in Figure 6.5. Network instability is a vulnerability that can cause dropped packets thereby compromising the integrity of the energy data records.

### Customer Privacy

Using Table 6.2 as input, initial threat scenario diagrams shown in Figure 6.6 and Figure 6.7 are created as starting points for further analysis.

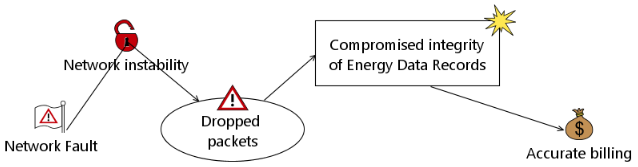


**Figure 6.5:** Initial threat diagram : Inanimate threats

The initial threat scenarios in Figure 6.6 depicts how the deliberate actions of persons affect this asset. An eavesdropper may attain customer data as a result of the use of an insecure communication medium. Alternatively, a hacker may exploit vulnerabilities in the security infrastructure to gain access to the network. Once inside, he could launch a variety of network attacks to obtain access to client information thereby compromising confidentiality.

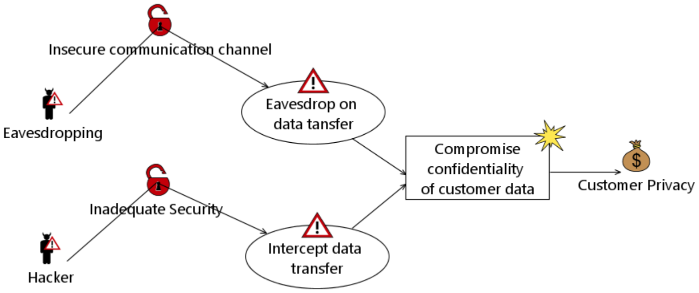

Insecure communication channel
Eavesdropping
Eavesdrop on data tansfer
Compromise confidentiality of customer data
Customer Privacy
Inadequate Security
Hacker
Intercept data transfer

**Figure 6.6:** Initial threat diagram : Deliberate threats

Figure 6.7 follows the path an accidental treat takes to compromise the asset. An employee of Grid Tech may unintentionally leak customer data due to either a lack of sufficient training or due to careless on the part of the employee.

### Uninterrupted Service

The analyst uses Table 6.3 and provides initial threat diagrams for this asset. Figure 6.8 shows how an attacker affects the asset. He exploits inadequate security deployments in the wireless communication medium used in the AMI to launch various attacks that deplete network resources thereby services unavailable.

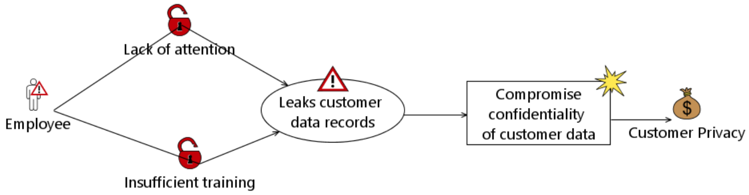

Lack of attention
Employee
Insufficient training
Leaks customer data records
Compromise confidentiality of customer data
$
Customer Privacy

**Figure 6.7:** Initial threat diagram : Accidental threats

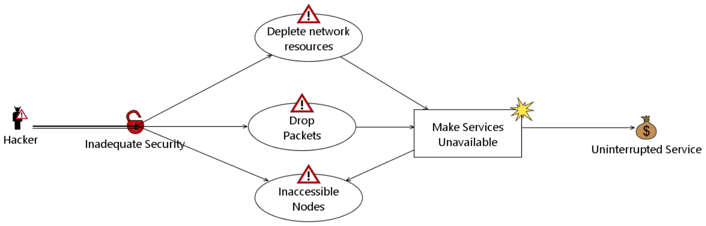


**Figure 6.8:** Initial threat diagram : Deliberate threats

This asset may also be compromised by non-human treats as shown in Figure 6.9. Network failure due to an unstable network can result in severe packet drops rendering the system services unavailable. Furthermore, services may also be unavailable due to hardware faults

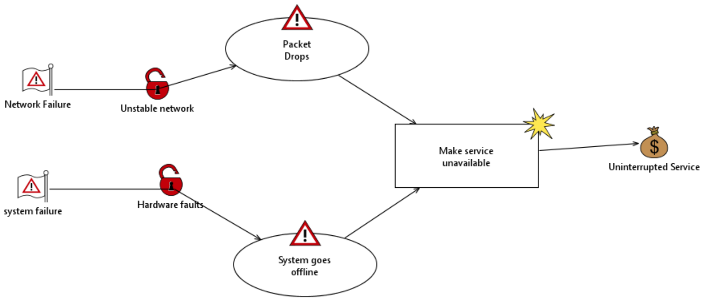


**Figure 6.9:** Initial threat diagram : Non-Human Threats

## 6.3 Findings & Analysis

The CORAS method is used to present the security risks of the AMI section of the smart grid. The resulting diagrams are analysed in the following subsections to get a deeper understanding of the associated risks

### 6.3.1 Threats

Applying the CORAS modeling technique to the AMI reveals the relations between threat scenarios and the resulting unwanted events. The identified assets align with the security requirements discussed in section 2.3.

#### Attacker Types

The results for risk identification reveals how the threats can cause unwanted scenarios which could compromise the assets. In order to gain a better understanding as to which exploits the threats can employ, the different types of threats and their motivation need to be explored. The deliberate threats against the AMI consist of customers, utility insiders, organized crime and enemy state. A summary is of the individual groups under deliberate threat is presented in Table 6.5.

| **Attacker** | **Attacker Type** | **Motivation** |
|---|---|---|
| Customers | Physical Attacker | Reduce utility cost |
| Utility insiders | Administrator | Varied |
| Organized Crime | Network Attacker, Software Attacker, Physical Attacker | Monetary gains, Denial of service or terrorist goals |
| Enemy state | Network attacker, Software attacker | Sabotage, Denial of service |

**Table 6.5:** Attacker types, motivation and Tools

The first group of perpetrators identified are customers whose homes receive energy supplied by the utility company. Customers have direct access to smart meters installed in their homes. With this direct access, exploiting of the smart meter can be achieved as these nodes cannot be physically monitored by the utility providers or security personnel. It can be argued that customers who attempt to compromise smart meters installed on their premises, predominantly do so to engage in energy theft as this aligns with their motivation. Their motivation, for the most part, is to reduce the amount paid for energy usage hence engage in energy theft. Furthermore, the likelihood that this group would be driven by the desire to interrupt service or steal other clients information is very low compared to other groups. Customers were able to achieve this easily with traditional analog meters. Smart meters are equipped to detect and relay information when tempered with. As such, successfully pulling this off requires some technical skills. The implication of this is that successfully avoiding energy bills is more difficult to achieve for this group compared to the other group of attackers due to their limited technical skills. Thus, in terms of resource and skill-set, the average end user is typically the least resourceful group of attackers and have limited technical ability to pull any of the attacks.

Another group of attackers with limited hacking skills is a small section of an employee of utility companies who are corrupt or dishonest. These employees may be working alone or recruited by an organized crime or enemy states. With this premise, their motivation for embarking on an attack is not definite. In fact, there is very limited information in literature to identify their motivations. One of the probable desire could be acquiring wealth. Other motivations could be aligned with the motivations of the groups that recruited them. What makes enables this group of adversaries to effectively compromise assets is the privileges assigned to them that allows them to access or tamper with data records, tamper with node configurations or install malware on systems to attain their goal. Another set of persons that belong to this group are sloppy employees. These individuals are not motivated to perform any attacks directly but may, as a result of insufficient training or lack of attention, fall prey to social engineering attacks. This results in leaking or exposing data records which are picked up by other groups for exploitation.

The next group of attackers is the organized crime group. A case can be made to say that this group has motivations in embarking on attacks against accurate billing and customer privacy as a result of the potential wealth they can rake in pulling off the attacks. This makes them more resourceful and grants them the means to attain the services of professional hackers who explore vulnerabilities as well as develop tools that exploit these vulnerabilities. Compromising customer privacy gives this group knowledge of customers' routine. This is useful in predicting when a customer would be away from home so as to perform burglaries.

The last group of attackers comes in the form of enemy states. This group of adversaries has the resources and technical abilities to pull off all the attacks. When it comes to motivation for attacking each asset, they have little motivated to pull off attacks against accurate billing as well as customer privacy but are more likely to engage in attacks to disrupt services.

Chapter 7

# Smart Grid Attacks

This chapter contains attacks that pose a threat to the smart grid. It presents the findings from the literature review on smart grid attacks. The chapter contains findings with 5 main sections according to the category used in the grouping of attacks: publication year, research type, security requirement, individual attacks. The chapter concludes with a presentation of attack trees for the findings.

## 7.1 Findings and Analysis

The steps presented in Section 3.1.3 is applied to relevant literature so as to answer research question 2. In the past ten years, there have been numerous publications on attacks that can be used to compromise security requirements of the smart grid including confidentiality, integrity, and availability. However, with focus on publications in the last three years (from 2015 to early 2018), the latest trend in attacks against the smart grid is identified. These are discussed in the subsequent sections.

### 7.1.1 Publication Year

Table 7.1 presents the grouping of the relevant publications according to the year of publication. It can be seen that the number increases from year to year starting from 21 in 2015 which represents 25%, followed by 25 in 2016 representing 29.76% and 33 in 2017 representing 39.29%. 2018 had 5 articles representing 5.95% but since the results for 2018 only accounts for the publications made between January and April, it will be interesting to see if the trend continues. The upward trend can be argued to depict the increase in interest in ensuring the security of the smart grid by finding and testing solutions that mitigate the probable attacks.

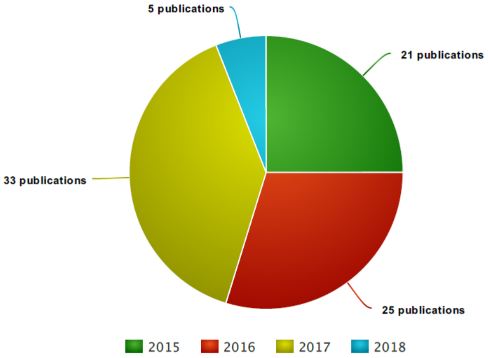


**Figure 7.1:** Percentage share of publications on smart grid attacks

| Year | References | Number |
|---|---|---|
| 2015 | [73] [74] [75] [76] [77] [78] [79] [80] [81] [82] [83] [84] [85] [86] [87] [88] [89] [90] [91] [92] [93] | 21 |
| 2016 | [94], [95], [96], [97], [98], [99], [100], [101], [102], [103], [104], [105], [106], [107], [108], [109], [110], [111], [112], [113], [114] [115] [116] [117], [118] | 25 |
| 2017 | [119], [120], [121], [122], [123], [124], [125], [126], [127], [128], [129], [130], [131], [132], [133], [134], [135], [136], [137], [138], [139], [140], [141], [142], [143], [144], [145], [146], [147], [148], [149], [150], [151] | 33 |
| 2018 | [152], [153], [154], [155], [156] | 5 |

**Table 7.1:** Publication Year of research articles using modeling techniques

### 7.1.2 Research Type

Table 7.2 and Figure 7.2 shows the classification of research based on the research type: Modeling/Simulation or Survey/Review. The majority of research fall under the modeling (simulation) group. Modeling focused research comprises 89.29% of the total while those focused on review makes up 10.71%. It is not a surprise as more and more researchers are focused on finding, proposing and improving upon solutions to security threats to the smart grid.

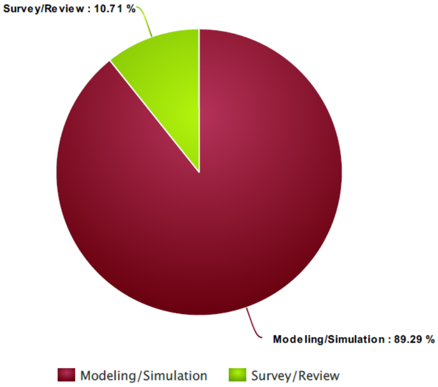


**Figure 7.2:** Classification based on research type

| **Research Type** | **Reference** | **Number** |
|---|---|---|
| Modeling / Simulation | [73], [74], [75], [76], [77], [86], [82], [88], [85], [94], [95], [96], [97], [98], [99], [100], [101], [102], [103], [104], [105], [106], [107], [108], [111], [112], [113], [114], [116], [117], [118], [119], [120], [121], [122], [123], [124], [125], [126], [128], [129], [127], [131], [132], [130], [135], [133], [134], [136], [137], [138], [139], [140], [141], [142], [143], [144], [146], [147], [148], [149], [150], [145], [151], [152], [156], [155], [154], [89], [90], [80], [87], [92], [91], [78] | 75 |
| Survey/Review | [79], [109], [110], [115], [84], [83], [81], [93], [153] | 9 |

**Table 7.2:** Classification according to research type

### 7.1.3 Security Requirement

Table 7.3 shows the groupings according to security requirements while Figure 7.3 shows the corresponding percentage shares. Publications touching on attacks against data integrity have been the most dominant in smart grid over the last 4 years with a

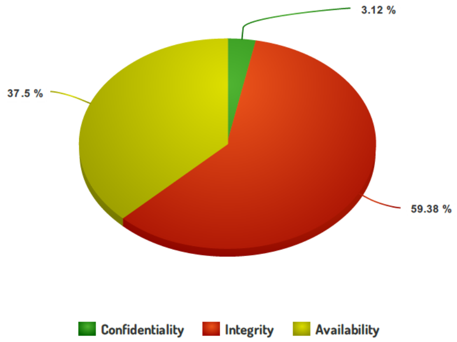


**Figure 7.3:** Percentage share of publications touching on each security requirements

share of 59.38%. Data integrity comprises the integrity of control information as well as billing information. Publications touching on availability also had a relatively high percentage share with 37.5% while those on confidentiality had a meager percentage share of 3.12%.

| **Security Requirement** | **References** | **Number** |
|---|---|---|
| Privacy/Confidentiality | [113], [115] [74] | 3 |
| Accurate Billing (Data integrity) | [74] [77] [80] [92], [85], [94], [95], [97], [100], [101], [102], [103], [104], [105], [106], [107], [108], [109], [110], [113], [115], [114], [118], [119], [122], [125], [127], [128], [131], [133], [134], [135], [136], [139], [141], [142], [144], [145], [146] [147], [148], [149], [151], [152], [154], [156], [155] [89] [90] [91] [86] [83] [81] [93] [79] [78] [75] | 57 |
| Uninterrupted Services (Availability) | [73] [88] [96], [98], [99], [109], [110], [111], [112], [113], [115], [116], [117], [120], [121], [123], [124], [125], [126], [127], [129], [130], [132], [137], [138], [140], [141], [143], [150], [153], [154] [87] [84] [82] [79] [76] | 36 |

**Table 7.3:** Classification based on security requirements

| Attacks | References | Number |
|---|---|---|
| False Data Injection | [75], [77], [80], [93], [92], [81], [86], [91], [85], [151], [90], [155], [156], [152], [97], [100], [102], [94], [103], [104], [108], [110], [109], [114], [118], [119], [122], [128], [129], [131], [134], [135], [136], [139], [141], [142], [146], [154], [145], [147], [148] | 41 |
| Opportunistic attack | [105] | 1 |
| Bid Modification attack | [133] | 1 |
| Malware | [115] | 1 |
| Spoofing | [144], [74], [113] | 3 |
| line-removing attack | [146] | 1 |
| Black-Hole/Sinkhole | [74], [89] | 2 |
| Man-in-the-the-middle | [83] | 1 |

**Table 7.4:** Individual attacks that compromise integrity

| Attacks | References | Number |
|---|---|---|
| Compromised meter | [113] | 1 |
| Unauthorized Access | [115] | 1 |
| Traffic analysis | [115] | 1 |
| sinkhole | [74] | 1 |

**Table 7.5:** Individual attacks that compromise availability

### 7.1.4 Individual Attacks

Tables 7.4 to 7.6 show individual attacks that can be used to compromise each of the security requirements.

#### Integrity

It can be seen from Table 7.4 that false data injection attacks constitute the majority of attacks against integrity. False data injection attack, as the name implies, is an attack that seeks to secretly compromise measurement data from sensors in the smart grid to cause errors in state estimation; a tool for a system operator to obtain the current snapshot of power system operation [133]. In [75], false data injection attacks

| Attacks | References | Number |
|---|---|---|
| Switching Attacks | [98], [109], [116], [82], [76] | 5 |
| DoS | [87], [153], [154], [150], [110], [143], [109], [112], [126], [115], [121] | 11 |
| Distributed DoS | [120], [141], [123], [124] | 4 |
| Compromised Node | [111], [117] | 2 |
| Malicious software (Malware) | [112], [115], [96] | 3 |
| Replay | [115] [138] [140] | 4 |
| Packet dropping | [132] | 1 |
| Dynamic load altering attack | [137], [84] | 2 |

**Table 7.6:** Individual attacks that compromise availability

against SCADA are implemented using sparse attack vector construction methods. Sparse attack vector deals with finding the smallest number of sensors to compromise so as to be successful at launching an attack [94].

Opportunistic attacks, man-in-the-middle attacks, and line-removing attack are other ways with which an attacker can compromise integrity in the smart grid as shown in Table 7.4. Opportunistic attacks aim at manipulating electricity prices by targeting devices in-charge of real-time pricing. Compromising these devices result in shifting the normal demand-supply relation which in turn affects pricing at the local bus. With the help of utility insiders, the attacker can rake in huge profits as a result of the fluctuations in prices [105].

Man-in-the-middle attack is the general term describing attacks involving an attacker placing himself in the communication path between two parties who intend to communicate with each other. The attacker does so discreetly thereby tricking the two parties to think they are communicating with each other directly. After successfully planting himself in this position, the attacker can decide to relay messages to other destinations or alter the contents of the original message. Utilizing this attack can also result in compromising confidentiality as well as availability depending on the goal of the attacker. Thus, depending on his goal, he adopts variations of this attack. With line-removing attack, an attacker can generate fake outage event so as to trick the operation center to make wrong dispatches which could end up in system instability [146].

### Availability

With regards to availability, DoS contributes the most researched about attack. DoS is defined in [87] as *"Inundation of a system or network with detrimental traffic to inhibit the benign users of the service offered by the network or the system itself by a source using either of the flooding techniques"*. With this definition, all other attacks but switching attacks in Table 7.6 can be considered as ways to implement DoS.

Switching attacks (cyber switching attacks) is an attack whereby a target generator is made unstable and thus isolated from the network as a result of compromising switches [98]. Switching attacks can lead to blackouts thereby compromising availability. Other attacks that affect availability include DDoS and malware. DDoS is an implementation of DoS through enormous number of sources.

Malware is a term coined from two words: Malicious and Software. It can be explained as a software running on a target system that is designed to intentionally cause harm to the system. There are various types of malware including Ransomware, virus, Trojan horse, Worm, Sniffer and Botnet. [157] defines categories of malware depending on the goal. 3 of the defined categories can be used to achieve an attackers goal without human actions. These are:

- Espionage: breaching confidentiality by stealing data from the target system. The data may be user data such as billing information or system data such as account credentials.
- Sabotage: breaching availability by either altering system functionality or by destroying the system. Sabotage may also affect integrity by manipulating the system to cause inaccurate behaviour.
- Hijacking: breaching availability by taking control of the system to act as botnets for DoS or DDoS. They may also be used to forward messages to an attacker which compromises confidentiality.

### Confidentiality

With regards to privacy, there are only a few attacks that have been used in literature to compromise privacy. These include traffic analysis and sinkhole attacks. With Black-hole/Sinkhole attacks, the attacker plants a malicious node in the communication path between the communicating nodes. This node advertises itself to be a legitimate route to forward traffic and upon succeeding, receives the desired packets. The attacker then chooses to drop the traffic pertaining to the desired smart meter or modify the data and forwarding it. In order to mask his activity, the attacker may forward traffic from other nodes unmodified.

## 7.2 Attack Tree

The results obtained in Table 7.4 to 7.6 is used in completing the attack trees for each of the security requirements. The attack trees for confidentiality, integrity and availability are shown in Figure 7.4 , 7.5 and 7.6 respectively. Since all sub-attacks are alternate ways to achieve an attack, a simplified attack tree is presented by removing the Boolean ’OR’ operator.

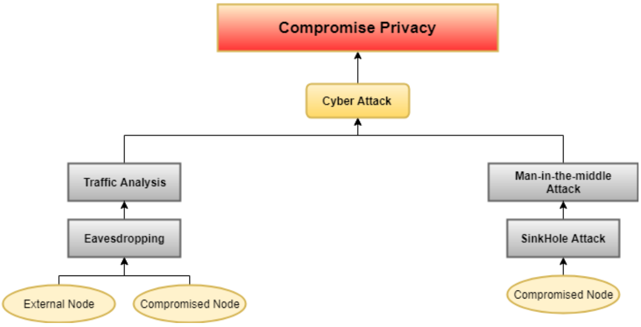


**Figure 7.4:** Attack tree for compromising privacy in smart grid

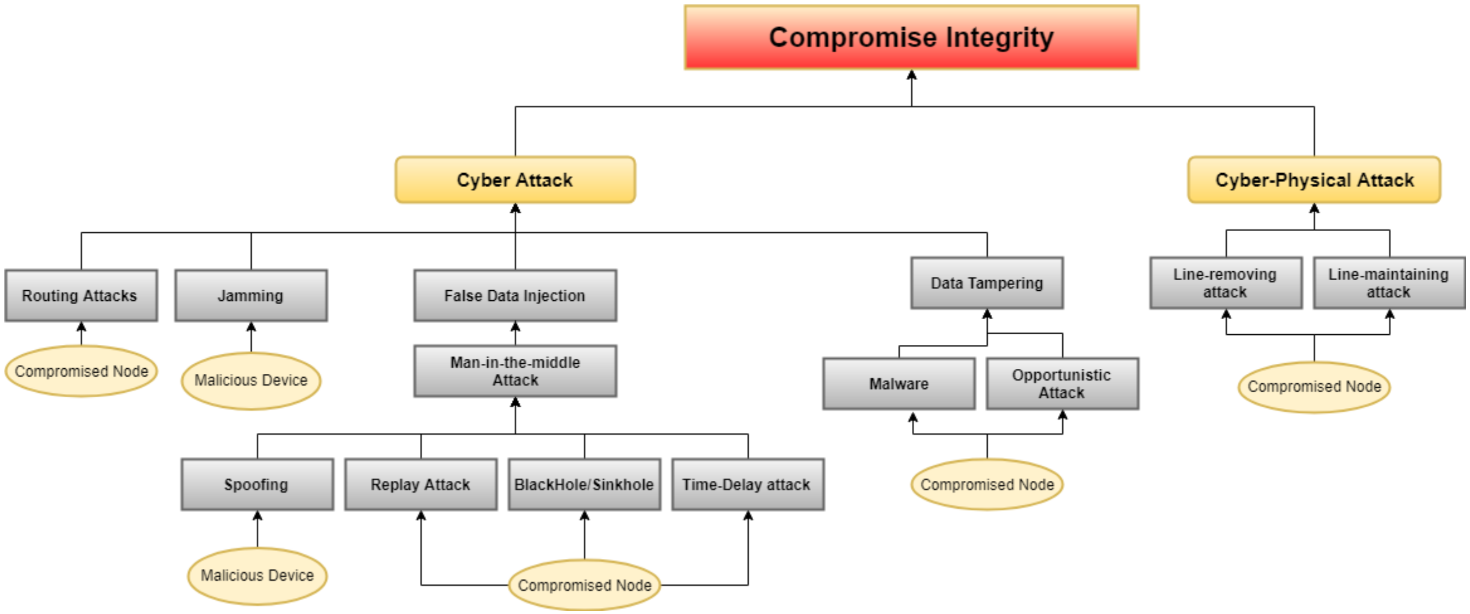


**Figure 7.5:** Attack tree for compromising integrity in smart grid

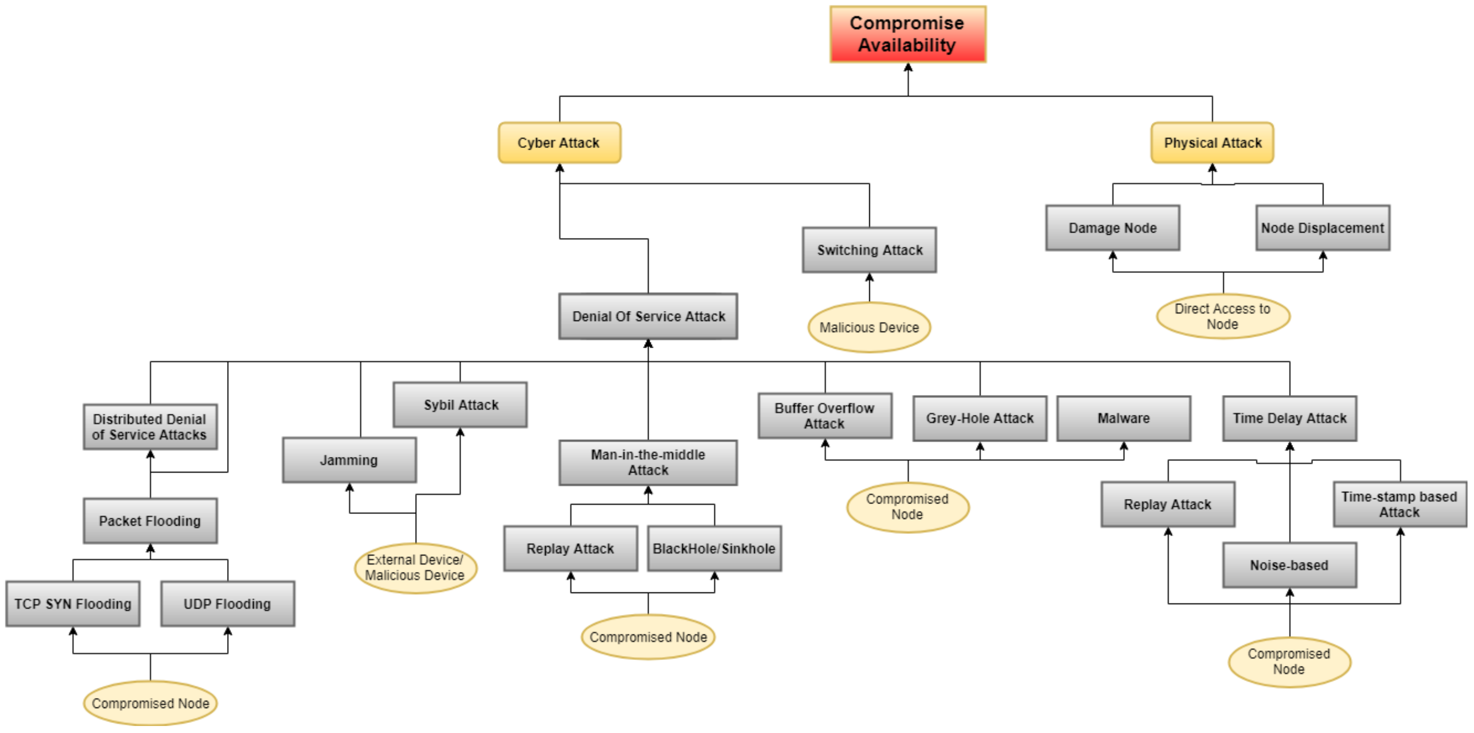


**Figure 7.6:** Attack tree for compromising availability in smart grid

# Chapter 8 Analysis and Discussion

The purpose of the thesis is to investigate and apply a suitable security modeling technique to explore the security risks associated with the smart grid as well as investigate smart grid attacks. This chapter contains two (2) main sections: Security Risk Modeling techniques and Attacks. The contents of these sections discuss the results of the review of modeling techniques, results obtained from the chosen technique as well as results of the individual attacks that can affect the smart grid.

## 8.1 Security Risk Modeling Techniques

As mentioned earlier, understanding real-world systems can prove difficult and as such, there has been increased interest in methods that can aid in the understanding of these systems. Visualization is one of the popular ways of presenting and understanding complex systems resulting in the development of numerous visualization techniques. However, with a special focus on security risk analysis, the number of viable techniques that can be applied to analyse security risk of the smart grid can be narrowed. With this in mind, it is very important to review and document the viable techniques in such a way that can help understand how they can be applied to the smart grid. By doing this, research question 1 can be answered. The findings of the literature review of security risk modeling techniques presented in section 4.2.1 are discussed below:

- **Aim of the security related research conducted**
  According to the result in Table 4.1, the difference between the percentages of the two categories is relatively small. The result is unexpected and particularly interesting because you would expect it to be much easier and feasible to apply an established method as compared to developing and implementing extensions. The argument for the above statement is that it generally takes more time and effort to develop a novel method or an extension to an existing method as compared to simply applying the method in security risk analysis. The results can be interpreted to say that the base models are not fully equipped to

tackle the growing need for more secure systems hence the need for alternative methods or extensions to the established methods.

- **Modeling techniques used**:
  Table 4.2 shows attack trees are the most used modeling technique. Looking at security risks visualization results of target systems using the different techniques, it is easy to understand why this is so. Firstly, attack trees are popular among security professionals due to their experience with fault trees. Secondly, attack tree is the simplest to create because of the simplified semantics and the visualization this technique produces describe attacks in an intuitive visual way using the simple semantics. However, the consequence of having a simplified semantics is that it limits the applications. This argument is in line with arguments presented by Mirembe and M. Muyeba in [72] that attack tree's semantics have limited internal structure, and this makes it inadequate for providing logical reasoning. Thus, Attack trees tend to be biased and present visualizations based on the perception and understanding of the author of the tree.

- **Application of modeling technique**
  All the security modeling techniques can be used in performing asset identification and risk identification. How they achieve this can be grouped into two: mathematical modeling and non-mathematical modeling. Two of the lot, Petri-nets, and game-nets require the use of mathematical modeling in the construction of visualization while the others do not. With this, Petri-nets and game-nets provide logical reasoning which is lacking in attack trees. They achieve this by presenting a deviation from attacker focused modeling by presenting a distinction between events and goals. This clear distinction is advantageous as it provides a much more in-depth description which allows atomic components on an attack to be investigated. However, these two modeling techniques require a higher level of expertise to model the target system as compared to the rest.

  Activity diagrams, from the result, have the least application in security risk modeling. They have been limited to only risk identification. The reason for this limited application can be argued to be due to what makes activity diagrams different from the rest; activity diagrams being based on process modeling. As such, their limited focus is on how a user traverses various use cases of the system. Thus, they view the system from the perspective of user interactions. Petri-nets, game-nets, and bow-tie models are found to extend the application of activity diagram to only cover risk evaluation while CORAS and attack trees are further used in performing mitigation steps. Performing a qualitative analysis is relatively straightforward for both game-nets and petri-nets as the use mathematical modeling from the get-go.

With the aim of identifying a suitable security risk modeling technique that can be used in analysing the security risks in smart grid and demonstrating its applicability using a qualitative analysis, employing a mathematically based modeling ( petri-nets and game-nets) could have been a viable option. However, using these techniques pose a challenge. This is because aside from having complex analysis algorithms, the results obtained are very dependent on the abstractions made during the modeling stages [58]. Thus, this reduces the options of suitable techniques for visualizing the security risks in the smart grid to bow-tie, CORAS and attack tree. Among these, only CORAS provides a framework to assist in performing risk analysis. Its methodology provides a walk-through to risk assessment. The results of applying CORAS confirm arguments presented in section 4.2.2. Thus, with CORAS, a detailed and unambiguous description of the AMI and assets is provided. Furthermore, the effortless way with which the results of analysis are documented and visualized enhances the understanding of the security risks in the AMI section of the smart grid.

### 8.1.1 CORAS Application

In this section, the findings of the application of CORAS in the AMI use case obtained in section 6.3 are discussed. The use of the seven unique elements (deliberate threat, accidental threat, non-human threat, vulnerabilities, threat scenario, unwanted incidents, and assets) provided by CORAS aided in identifying security risks in the AMI. Thus, with the use of the CORAS methodology defined in section 3.1.2, identification and documentation of three direct assets, as well as three unwanted incidents (energy theft, privacy breach, and unavailable service) in step four, is done. Exploring how each asset can be compromised by using the three distinct threats defined by CORAS is key to identifying how each threat exploit a vulnerability to create a threat scenario which may result in an unwanted incident. The following sections discuss how the unwanted incidents identified can be reached by the threats.

– **Energy Theft**
  The results for deliberate threats against accurate billing presents three different ways an attacker can achieve his goal. The first threat scenario, interrupting measurement from being taken in the smart meter, is more difficult to achieve compared to the traditional meter. The traditional meter lacks sensors or detection mechanisms that detect whenever the meter is disconnected or psychically tempered. This results in allowing customers to engage in energy theft using various schemes (Table 8.1). Rashed et al discussed in [8] the various

tampering schemes possible with the traditional meter. These include bypassing the meter by direct connection to the distribution lines and grounding the neutral wire. However, these theft techniques are not possible in the case of smart meters as there are sensors that detect and record logs whenever power is disconnected from the meter. Therefore to accomplish energy theft without the knowledge of utility companies, the perpetrators need to go one step further by deleting these logs either in the meter or while the readings are in transmission to the utility. In order to delete the logs saved in the meter, the adversary needs to obtain the credentials to be able to log into the smart meter.

| **Theft Method** | **Smart Meter Counter measure** |
|---|---|
| Direct connection to distribution lines | Recording 'zero' readings and informing utility provider through AMI |
| Grounding the neutral wire | Recording 'zero' readings and informing utility provider through AMI |

**Table 8.1:** Traditional meter theft schemes and countermeasures in smart meter (adapted from [8])

The second threat scenario involves altering stored energy usage data in the smart meter. In order for an attacker to do this, the attacker must obtain valid credentials to gain access to the stored data. The attacker can attempt to reverse engineer the firmware so as to find vulnerabilities to attain passwords and encryption keys. In the case whereby the customer's smart meter serves as an aggregation unit for reports from other meters, the attacker may opt to split his consumption data and use it as a top up to the consumption records of others. In that way, he can mask his activities from the utility company.

The last threat scenario is to modify energy data while it is in transit to the utility. To accomplish this, an attacker needs to primarily do 2 things; i) prevent original traffic from reaching the utility by intercepting traffic from the meter and ii) modify the energy data or inject falsified records. The second step is necessary for the attacker's activity to stand a chance of going unnoticed by Grid Tech. By implementing attacks against the network layer, an attacker can implement either the first step or both of the steps. Some of the attacks require the attacker to implant a malicious node into the network. How the attacker goes about this is dependent on how authentication and integrity checks are implemented.

- **Privacy Breach**
  The results in figure 6.6 shows that an attacker can attain this goal in two

different ways using cyber attacks. The first threat scenario involves eavesdropping on the communication channel. An attacker can do so either actively or passively depending on how secure the network channel is. In fact, eavesdropping is often the starting point for other forms of attacks that compromise the assets. Eavesdropping against wireless channel has been researched and Li et. al. show how this is possible from the perspective of the attacker in [158].

The alternate threat scenario shows that intercepting the data by means of network attacks also leads to the unwanted scenario. An attacker leverages security vulnerabilities in the communication network to gain access to data. The attacks that can be used to modify data to accomplish energy theft may also be used here since the data needs to be first intercepted before modification.

In addition to these two ways, an attacker may decide to employ a physical attack by way of physical theft of the smart meter so as to access the stored data. This type of attack requires the attacker to be on customer premises to accomplish. It also requires that the attacker has the necessary know how to access the contents of the stored data. It is also interesting to note that the asset can be compromised by accidental acts by utility employees. This is made possible by use of social engineering techniques to exploit employees lack of attentiveness or insufficient training.

- **Uninterrupted Services**
  Uninterrupted service can be accomplished in three ways. Firstly, nodes going offline as a result of hardware faults, software faults or an attacker's activities which can result in an adverse effect on service availability. Attackers, thus, need to compromise the nodes in order to take them down. Secondly, severe packet drops as a result of network instability or an attacker's activities may also lead to interrupted services. An attacker could accomplish this by either using a rogue device or a compromised node. Lastly, an attacker can accomplish this goal by the use of a variety of DoS attacks that aim to consume network resources thereby making services unavailable for legitimate nodes

## 8.2 Attacks

As presented earlier, the smart grid's communication network makes it a target for attacks which can result in significant losses if successful. In this regard, there has been significant research in simulating and implementing attacks as well as the efficacy of defense mechanisms to detect the attacks against the smart grid. As such, it is important to identify, review and thoroughly document the attacks that have been presented in literature. This can help identify the areas of significant research as well as areas of future research direction. Research question 2 aims at addressing the above-mentioned needs. The findings of the literature review of smart grid attacks are presented in 7.1. The findings are discussed below:

- **Security Requirement**
  In table 7.3, it can be seen that most of the reviewed literature is related to integrity in the smart grid while that on confidentiality occupies a very small percentage of research. A plausible reason as to why this is so can be drawn from the effects of integrity attacks. Some attacks against integrity such as false data injection can directly result in compromising availability. For example, data injection attacks can corrupt PMU data and if this goes undetected by the power grid's detection mechanisms, it can result in incorrect operational decisions that lead to blackouts [117]. Furthermore, other attacks such as man-in-the-middle and blackhole/sinkhole attack can be tweaked to compromise availability. These arguments justify why significant portions of the reviewed literature focused on integrity attacks.

  The percentage share of confidentiality related publications reviewed shows that protecting confidentiality is the least concern in the smart grid. The meager percentage share could be attributed to the significance or impact threats against confidentiality pose to the smart grid. Effects of a breach in confidentiality tend not to affect operations in the smart grid on its own. Thus, a breach in confidentiality of customer data affects end users instead of the grid itself whereas that of operational/control data does not affect the grid also. However, a breach in confidentiality of control data is used in the reconnaissance stage of attacks by attackers who aim to compromise the other security requirements. Thus, in order to impact operations, other attacks have to be employed.

- **Individual Attacks**
  The results of the literature review show the various attacks that can be used in compromising the smart grid in terms of integrity, availability, and confidentiality. False data injection attacks is found in Table 7.4 to be the most researched attack against integrity whereas DoS, from table 7.6 is the most researched attack against availability. The results of the attack trees present an overview of all attacks against the security requirements.

  Analysing all the attack trees, it can be seen that man-in-the-middle attack is common to all security requirements and requires the use of an external malicious node. Man-In-The-Middle, one of the primary threats against the security of a wireless network, is described in [159] as *"the most successful attack that is launched for gaining control over the transferred sensitive end-users data"*. This attack is possible in the smart grid because of the use of communication technologies such as Wi-Fi and Zigbee, which have been shown to be susceptible to man-in-the-middle attacks. The authors of [159] show how feasible it is to intercept packets in Zigbee networks that do not use encryption by using passive eavesdropping. A countermeasure to prevent passive eavesdropping could be the use of a protocol for encryption such as OSGP which, in turn, require the attacker to employ active eavesdropping in order to be able to intercept the messages. Unfortunately, OSGP has been shown to have a weakness which makes active eavesdropping as well as other variations of the man-in-the-middle attack possible. After successfully intercepting the messages using man-in-the-middle attack, the attacker can go a step further to either modify the intercepted messages thereby compromising the integrity of the data or destroying the messages thereby compromising the availability of service.

Figure 7.6 shows that DoS can be achieved in a plethora of ways. One such way is the use of flooding packets and this is demonstrated in [73] whereby UDP flooding is implemented on time-critical communications in WLAN and its effects analysed. Another demonstration is achieved in [87] where the authors use an external hardware to perform TCP SYN flooding in order to achieve DoS. Thus, DoS can be achieved by using either an external node or compromising a legitimate node. In fact, these two nodes are the attack sources for almost all attacks.

An external malicious node can be used for both passive and active attacks. Using the external node for passive attacks is done by way of sniffing or eavesdropping on the wireless communication channel used in the smart grid. Doing this alone is sufficient for compromising customer privacy if the data being sent is not encrypted. Furthermore, the external malicious nodes can be used for active attacks. For this to be possible, the attacker needs to clandestinely integrate the malicious node into the communication channel. This can be done by way of using rogue access points or by ARP spoofing.

The second entry point for an attack, compromising nodes such as smart meters, DCU, and PMU, can be achieved by launching physical or cyber attacks. The first group of attacks, physical attacks, involves attacks against the life cycle of the node. One way the attacker can go about this is to replace dedicated Integrated Circuits (ICs) which are responsible for measurement with fake or compromised ICs. These fake ICs could be programmed by the attacker to do whatever the attacker desires such as sharing the encryption key or customer details with the attacker. An attacker who lacks the technical know-how to pull this off may rather opt to replace the entire node with fake ones. For cyber attacks, the attacker may clone the node's software or compromise it using malware.

# Chapter 9 Conclusion and Future Works

In this chapter, the conclusions drawn from the results obtained in this thesis as well as recommendations for future works are provided. The chapter is organized according to the research questions.

**Research Question 1: What different modeling techniques are used in security risk analysis and which of the techniques better aids in identifying and understanding the security risks in a smart grid?**

With the incorporation of a communication network to the traditional grid, the smart grid is a possible target for attackers. To effectively develop and implement adequate security measures, security risk analysis has to be done. As such, in order to answer research question 1, the thesis aimed to report the results of a literature review of security modeling techniques. A set of modeling techniques were identified and analysed with regards to how they were applied in security risk analysis in order to provide information about the recent state of security modeling techniques. The search began with 11,346 articles and specific selection criteria were applied. This resulted in a filtering the initial pool of papers to 26 articles. The information obtained from the 26 articles resulted in the below conclusions:

- The results of the literature review show that the modeling techniques used in security risks can be classified into two groups: implementation of base model and implementation of extensions to base model. Research that used implementation of base model appear to be more popular, albeit rather marginally. This shows that the base models are not fully adequate to tackle security risk analysis because of the significantly high percentage of implementation of extensions to the base models.
- The review enabled the identification of different modeling techniques that have been used in security risk analysis: UML activity diagram, attack trees, bow-tie, CORAS, petri-nets and game-nets as modeling techniques. Among

these techniques, the review reveals that attack tree is the most popular used technique in security risk analysis

- A comparative analysis of how the modeling techniques are used in literature shows that the techniques can be evaluated based on four (4) desired applications: "Asset identification", "Risk identification", "Risk evaluation" and "mitigation steps". The findings shows that UML activity were only used in asset identification and risk identification. Petri-nets, game-nets and Bow-tie extend the application of UML activity diagram to risk evaluation but failed to touch on mitigation steps. Only CORAS and attack trees have been used in all four (4) applications.

- The results of using CORAS as the suitable technique in security risk analysis of the AMI reveals three (3) assets as well as various threat scenarios that can be used to compromise the assets. In addition, how threats exploit vulnerabilities to result in threat scenarios were identified. Thus, the application of CORAS methodology provided a step-by-step walk-through which aided in identifying the security threats. Documenting and visualization using the CORAS tool paints a vivid picture of the risks in this section of the smart grid. This shows that the CORAS's language, tool and methodology for risk analysis is easy to use, straight forward and provides guides for asset identification and risk analysis. Thus, the findings reiterates arguments made for choosing CORAS as the suitable modeling technique made in section 4.2.2

**Research Question 2: What attacks can be used to compromise the smart grid?**

For research question 2, attack trees are used in presenting an overview of attacks against the smart grid. The individual attacks that are plausible in the smart grid was obtained by a literature study of smart grid attacks. With a pool of 750 articles obtained from the initial search, 2 filter criteria were used to limit the study to 84 articles. From the results obtained, the following conclusions can be made:

- The results of the literature review of attacks the smart grid is susceptible to can be classified based on the three main security requirements: confidentiality, integrity and availability. Research on attacks that compromise integrity are the most popular whereas research on attacks that compromise confidentiality are the least popular in literature. The reason for this is that majority of attacks against integrity, particularly those that affect integrity of control data, can have cascading effect on the smart grid resulting in loss of availability.

- Analyses of the attack tree for each requirement revealed thirteen (13) attacks that can be coordinated to compromise integrity, four (4) attacks for compromising confidentiality and eighteen (18) attacks that are correlated with compromising availability. Furthermore, with regards to attacks common to the smart grid security requirements, the results show that Man-in-the-middle and blackhole/sinkhole attacks are common to compromising confidentiality, integrity and availability whereas jamming and replay attacks can be used to compromise both integrity and availability in the smart grid. Finally, all the identified attacks that aim to compromise the security requirements stem from either compromising legitimate nodes or using external devices.

## 9.1 Future Work

In this section, a presentation of recommendations for extending the research done in this thesis:

- **Risk Evaluation and Mitigation Steps using CORAS**
  This thesis demonstrated the applicability of CORAS in identifying security risks in AMI. It limited CORAS application to asset and risk identification. Implementing risk evaluation and mitigation steps using CORAS would provide an in-dept understanding into the solutions for improving the security of the smart grid. To do this, research into defining a formal evaluation criteria for security risks in the smart grid needs to be done. Furthermore, to attain a complete overview of security risks in the smart grid, CORAS should be applied in analysing security in SCADA and WAMS

- **Formal assessment for security risk modeling techniques**
  This thesis presented a way to compare risk modeling techniques based on the research questions and limited the comparison to six techniques. However, with the emergence of various extensions to modeling techniques as well as new techniques for security assessment, it is paramount to formally define an evaluation criteria for each of them so as to assess the strengths and shortcomings of each of the techniques. Thus, future work could concentrate on developing and implementing an assessment tool for all the techniques.

# References

[1] Y. Kabalci, “A survey on smart metering and smart grid communication,” *Renewable and Sustainable Energy Reviews*, vol. 57, pp. 302–318, 2016.

[2] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, “Cyber-security in smart grid: Survey and challenges,” may 2018.

[3] S. Sheuly, “a Systematic Literature Review on Agile Project Management,” pp. 1–70, 2013.

[4] F. den Braber, G. Brændeland, H. E. I. Dahl, I. Engan, I. Hogganvik, M. S. Lund, B. Solhaug, K. Stølen, and F. Vraalsen, “The CORAS model-based method for security risk analysis,” *SINTEF, Oslo*, no. September, 2006.

[5] J. Zhou, “Petri-net based safety analysis of process systems,” *IEEE International Conference on Industrial Engineering and Engineering Management*, vol. 2017-Decem, pp. 1217–1221, 2018.

[6] R. Kaur, N. Kaur, and S. K. Sood, “Security in IoT network based on stochastic game net model,” *International Journal of Network Management*, vol. 27, no. 4, pp. 1–19, 2017.

[7] H. Abdo, M. Kaouk, J. Flaus, and F. Masse, “A safety / security risk analysis approach of Industrial Control Systems : A cyber bowtie – combining new version of attack tree with bowtie,” *Computers & Security*, vol. 72, pp. 175–195, 2018.

[8] R. Rashed Mohassel, A. Fung, F. Mohammadi, and K. Raahemifar, “A survey on Advanced Metering Infrastructure,” *International Journal of Electrical Power & Energy Systems*, vol. 63, pp. 473–484, dec 2014.

[9] L. Kotut and L. A. Wahsheh, “Survey of cyber security challenges and solutions in smart grids,” in *2016 Cybersecurity Symposium (CYBERSEC)*, pp. 32–37, April 2016.

[10] R. Aggarwal and M. Lal Das, “RFID Security in the Context of “ Internet of Things ”,” *SecurIT ’12 Proceedings of the First International Conference on Security of Internet of Things*, pp. 51–56, 2012.

[11] D. Evans, “The Internet of Things - How the Next Evolution of the Internet is Changing Everything,” *CISCO white paper*, no. April, pp. 1–11, 2011.

[12] X. Chen, J. Liu, and X. Li, “Integration of IOT with smart grid,” *IET International Conference on Communication Technology and Application (ICCTA 2011)*, no. 1, pp. 723–726, 2011.

[13] B. S. E. Collier, “The Emerging Enernet,” no. April 2017, pp. 12–16, 2016.

[14] S. Jain, K. N. Vinoth, A. Paventhan, V. Kumar Chinnaiyan, V. Arnachalam, and M. Pradish, “Survey on smart grid technologies-smart metering, IoT and EMS,” *2014 IEEE Students’ Conference on Electrical, Electronics and Computer Science, SCEECS 2014*, 2014.

[15] J. Liu, X. Li, X. Chen, Y. Zhen, and L. Zeng, “Applications of Internet of Things on Smart Grid in China,” *2011 13th International Conference on Advanced Communication Technology (ICACT)*, pp. 13–17, 2011.

[16] P. S. Moura, G. López, and J. I. Moreno, “The role of Smart Grids to foster energy efficiency,” vol. 6, no. May 2014, pp. 621–639, 2013.

[17] C. Greer, D. A. Wollman, D. E. Prochaska, P. A. Boynton, J. A. Mazer, C. T. Nguyen, G. J. FitzPatrick, T. L. Nelson, G. H. Koepke, A. R. Hefner Jr, V. Y. Pillitteri, T. L. Brewer, N. T. Golmie, D. H. Su, A. C. Eustis, D. G. Holmberg, and S. T. Bushby, “NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0,” 2014.

[18] S. Tan, D. De, W. Z. Song, J. Yang, and S. K. Das, “Survey of Security Advances in Smart Grid: A Data Driven Approach,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 397–422, 2017.

[19] E. Bou-Harb, C. Fachkha, M. Pourzandi, M. Debbabi, and C. Assi, “Communication security for smart grid distribution networks,” *IEEE Communications Magazine*, vol. 51, no. 1, pp. 42–49, 2013.

[20] Q.-D. Ho, Y. Gao, G. Rajalingham, and T. Le-Ngoc, “Wireless Communications Networks for the Smart Grid,” pp. 15–31, 2014.

[21] G. Di Leo, C. Liguori, V. Paciello, A. Pietrosanto, and P. Sommella, “Towards visual smart metering exploiting wM-Bus and DLMS/COSEM,” *2015 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications, CIVEMSA 2015*, 2015.

[22] K. Kursawe and C. Peters, “Structural weaknesses in the open smart grid protocol,” *Proceedings - 10th International Conference on Availability, Reliability and Security, ARES 2015*, pp. 1–10, 2015.

[23] S. Goel, Y. Hong, V. Papakonstantinou, and D. Kloza, *Smart Grid Security.* 2015.

[24] J. Liu, Y. Xiao, and J. Gao, "Achieving accountability in smart grid," *IEEE Systems Journal*, vol. 8, no. 2, pp. 493–508, 2014.

[25] J. Cuellar, *Smart Grid Security: Second International Workshop, SmartGridSec 2014 Munich, Germany, February 26, 2014 Revised Selected Papers.* 2014.

[26] Z. L. Z. Lu, X. L. X. Lu, W. W. W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," *Military Communications Conference, 2010 - Milcom 2010*, pp. 1830–1835, 2010.

[27] Alan Bryman, S. E. Baker, R. Edwards, R. Belk, a. Bryman, U. Flick, G. Isouard, J. a. Maxwell, J. Pape, E. Publishing, B. Collection, L. Spencer, J. Ritchie, J. Lewis, L. Dillon, M. S. Sridhar, The Wallace Foundation, J. White, S. Drew, and T. Hay, "Handbook of qualitative research methods in marketing," *Qualitative Research Journal*, vol. 41, no. 1, pp. 295–312, 2007.

[28] Glenn A. Bowen and G. A. Bowen, "Document analysis as a qualitative research method," *Qualitative research journal*, vol. 9, no. 2, pp. 27–40, 2009.

[29] R. H. Fletcher, S. W. Fletcher, V. Jiménez, S. Díaz De Salas, V. Mendoza, C. Porras, K. M. Eisenhardt, B. Flyvbjerg, R. K. Yin, C. Study, W. Tellis, J. Gerring, Z. Zainal, L. M. Dooley, and K. B. M. Noor, "Case study as a research method," *Academy of Management Review*, vol. 5, no. 2, pp. 301–316, 1997.

[30] J. K. Khalid S Khan, Regina Kunz, "Five steps to conducting a systemstic review.," *Journal of the royal society of medicine*, vol. 96, 2003.

[31] M. Khan and S. Khan, "Data and information visualization methods, and interactive mechanisms: A survey," *International Journal of Computer Applications*, vol. 34, no. 1, pp. 1–14, 2011.

[32] J. Bau and J. C. Mitchell, "Security modeling and analysis," *IEEE Security and Privacy*, vol. 9, no. 3, pp. 18–25, 2011.

[33] F. Meng, D. Chu, and D. Zhan, "Transformation from data flow diagram to UML2.0 activity diagram," *Proceedings of the 2010 IEEE International Conference on Progress in Informatics and Computing, PIC 2010*, vol. 2, pp. 1010–1014, 2010.

[34] S. Ouchani and A. Otmane, "A Security Risk Assessment Framework for SysML Activity Diagrams," 2013.

[35] O. O. Mwambe and I. Echizen, "Security Oriented Malicious Activity Diagrams to Support Information Systems Security," 2017.

[36] B. Schneier, "Attack Trees," *Dr. Dobb's Journal of Spftware Tools*, vol. 24, no. 12, p. 60, 1999.

[37] V. Saini, Q. Duan, and V. Paruchuri, "Threat modeling using attack trees," *Journal of Computing Sciences in Colleges*, vol. 23, no. 4, pp. 124–131, 2008.

[38] S. Y. Esayas, “Structuring compliance risk identification using the CORAS approach: Compliance as an asset,” *Proceedings - IEEE 25th International Symposium on Software Reliability Engineering Workshops, ISSREW 2014*, pp. 281–286, 2014.

[39] F. Vraalsen, F. den Braber, M. S. Lund, and K. Stølen, “The CORAS Tool for Security Risk Analysis.,” *iTrust*, vol. 3477, pp. 402–405, 2005.

[40] B. Solhaug and K. Stølen, “The CORAS Language – Why it is Designed the Way it is,” *Safety, Reliability, Risk and Life-Cycle Performance of Structures and Infrastructures*, pp. 3155–3162, 2013.

[41] J. Zhou, G. Reniers, and L. Zhang, “A weighted fuzzy Petri-net based approach for security risk assessment in the chemical industry,” *Chemical Engineering Science*, vol. 174, pp. 136–145, 2017.

[42] O. Tariq, J. Sang, K. Gulzar, and H. Xiang, “Automated Analysis of UML Activity Diagram using CPNs,”

[43] C. Zhang, Y. Ma, X. Wang, and R. Wang, “Software Architecture Modeling and Reliability Evaluation Based on Petri Net,” pp. 51–56, 2017.

[44] K. Meng, Y. Wang, J. Lv, C. Lin, and J. Li, “Security Analysis for Web Service Behaviors Based on Hierarchical Stochastic Game Model,” *Chinese Journal of Electronics*, vol. 24, no. 3, pp. 449–454, 2015.

[45] J. Lv and J. Rong, “Virtualisation security risk assessment for enterprise cloud services based on stochastic game nets model,” *IET Information Security*, vol. 12, no. 1, pp. 7–14, 2018.

[46] N. Khakzad, F. Khan, and P. Amyotte, “Dynamic risk analysis using bow-tie approach,” *Reliability Engineering and System Safety*, vol. 104, pp. 36–44, 2012.

[47] H.-K. Kong, M. K. Hong, and T.-S. Kim, “Security risk assessment framework for smart car using the attack tree analysis,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 0, no. 0, p. 0, 2017.

[48] C. Wongvises, A. Khurat, D. Fall, and S. Kashihara, “Fault tree analysis-based risk quantification of smart homes,” *2017 2nd International Conference on Information Technology (INCIT)*, pp. 1–6, 2017.

[49] R. Kumar and M. Stoelinga, “Quantitative security and safety analysis with attack-fault trees,” *Proceedings of IEEE International Symposium on High Assurance Systems Engineering*, pp. 25–32, 2017.

[50] X. Ji, H. Yu, G. Fan, and W. Fu, “Attack-defense trees based cyber security analysis for CPSs,” *2016 IEEE/ACIS 17th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD 2016*, pp. 693–698, 2016.

[51] P. Wang, H. Lin, T. C. Wang, W. Lin, and P. Kuo, "Threat Risk Analysis for Cloud Security based on Attack-Defense Trees," *International Journal of Advancements in Computing Technology*, vol. 4, no. 17, pp. 607–617, 2012.

[52] J. Viehmann, "Reusing risk analysis results - An extension for the CORAS risk analysis method," *Proceedings - 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust and 2012 ASE/IEEE International Conference on Social Computing, SocialCom/PASSAT 2012*, pp. 742–751, 2012.

[53] S. Almutairi, G. Bella, and A. Abu-samaha, "System Using UML," pp. 259–265, 2012.

[54] S. J. Lincke, T. H. Knautz, and M. D. Lowery, "Designing system security with UML misuse deployment diagrams," *Proceedings of the 2012 IEEE 6th International Conference on Software Security and Reliability Companion, SERE-C 2012*, pp. 57–61, 2012.

[55] J. Jürjens, J. Schreck, and P. Bartmann, "Model-based security analysis for mobile communications," *Proceedings of the 13th international conference on Software engineering - ICSE '08*, vol. 2, p. 683, 2008.

[56] J. Jurjens, "Modelling audit security for smart-card payment schemes with UML-SEC," pp. 93–107, 2001.

[57] Y. Wang, C. Lin, S. Member, K. Meng, and H. Yang, "Security Analysis for Online Banking System Using Hierarchical Stochastic Game Nets Model," no. 5, 2009.

[58] A. Badreddine and N. Ben Amor, "A new approach to construct optimal bow tie diagrams for risk analysis," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 6097 LNAI, no. PART 2, pp. 595–604, 2010.

[59] S. Du and Z. Haojin, "Security Assessment in Vehicular Networks," p. 49, 2013.

[60] D. Kim, D. Shin, D. Shin, and Y. H. Kim, "Attack Detection Application with Attack Tree for Mobile System using Log Analysis," *Mobile Networks and Applications*, pp. 1–9, 2018.

[61] K. Edge, R. Raines, M. Grimaila, R. Baldwin, R. Bennington, and C. Reuter, "The use of attack and protection trees to analyze security for an online banking system," *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 1–8, 2007.

[62] L. Yao, P. Dong, T. Zheng, H. Zhang, X. Du, and M. Guizani, "Network security analyzing and modeling based on Petri net and Attack tree for SDN," *2016 International Conference on Computing, Networking and Communications, ICNC 2016*, no. 61232017, pp. 3–7, 2016.

[63] K. S. Edge, G. C. Dalton, R. A. Raines, and R. F. Mills, “Using attack and protection trees to analyze threats and defenses to homeland security,” *Proceedings - IEEE Military Communications Conference MILCOM*, pp. 1–7, 2007.

[64] L. Yao, P. Dong, X. Du, and H. Zhang, “Security analysis based on Petri net for separation mechanisms in smart identifier network,” *2017 26th International Conference on Computer Communications and Networks, ICCCN 2017*, 2017.

[65] S. A. Alsuhibany and A. P. A. van Moorsel, “Modelling and Analysis of Release Order of Security Algorithms Using Stochastic Petri Nets,” *Ares*, pp. 437–445, 2013.

[66] Y. Fu, J. Zhu, and S. Gao, “CPS Information Security Risk Evaluation System Based on Petri Net,” *2017 IEEE Second International Conference on Data Science in Cyberspace (DSC)*, pp. 541–548, 2017.

[67] T. Dimitrakos and B. Ritchie, “Model based Security Risk Analysis for Web Applications : The CORAS approach,” *Security*, pp. 1–13, 2002.

[68] F. Ya-Ping, F. Kwo-Jean, and Y. Chung-Huang, “CORAS for the research of ISAC,” *Proceedings - 2008 International Conference on Convergence and Hybrid Information Technology, ICHIT 2008*, pp. 250–256, 2008.

[69] Y. Wang, C. Lin, S. Member, Y. Wang, and K. Meng, “Security Analysis of Enterprise Network Based on Stochastic Game Nets Model,” no. 60803123, 2009.

[70] A. E. Bouchti and T. Nahhal, “Cyber security modeling for SCADA systems using stochastic game nets approach,” *5th International Conference on Future Generation Communication Technologies, FGCT 2016*, pp. 42–47, 2016.

[71] K. Bernsmed, C. Frøystad, P. H. Meland, D. A. Nesheim, and Ø. J. Rødseth, “Visualizing cyber security risks with bow-tie diagrams,” in *Graphical Models for Security* (P. Liu, S. Mauw, and K. Stolen, eds.), (Cham), pp. 38–56, Springer International Publishing, 2018.

[72] D. P. Mirembe and M. Muyeba, “Threat modeling revisited: Improving expressiveness of attack,” *Proceedings - EMS 2008, European Modelling Symposium, 2nd UKSim European Symposium on Computer Modelling and Simulation*, pp. 93–98, 2008.

[73] Q. Li, C. Ross, J. Yang, J. Di, J. C. Balda, and H. A. Mantooth, “The effects of flooding attacks on time-critical communications in the smart grid,” *2015 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2015*, pp. 1–5, 2015.

[74] C. Taylor, “Strong Authentication Countermeasures Using Dynamic Keying for Sinkhole and Distance Spoofing Attacks in Smart Grid Networks,” pp. 1835–1840, 2015.

[75] J. Hao, S. Member, R. J. Piechocki, D. Kaleshi, W. H. Chin, S. Member, and Z. Fan, "and Defense Mechanisms in Smart Grids," vol. 11, no. 5, pp. 1198–1209, 2015.

[76] J. Yan, Y. Tang, Y. Zhu, H. He, and Y. Sun, "Smart grid vulnerability under cascade-based sequential line-switching attacks," *2015 IEEE Global Communications Conference, GLOBECOM 2015*, 2015.

[77] A. Sanjab and W. Saad, "Smart grid data injection attacks: To defend or not?," *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 380–385, 2015.

[78] M. Basharat, W. Ejaz, and S. H. Ahmed, "Securing cognitive radio enabled smart grid systems against cyber attacks," *2015 1st International Conference on Anti-Cybercrime, ICACC 2015*, 2015.

[79] K. Tazi and F. Abdi, "Review on Cyber-Physical Security of the Smart Grid : Attacks and Defense Mechanisms," 2015.

[80] S. Li, Y. Yilmaz, and X. Wang, "Quickest Detection of False Data Injection Attack in Wide-Area Smart Grids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2725–2735, 2015.

[81] Z. Hu and Y. Wang, "False Data Injection Attacks Identification for Smart Grids," pp. 139–143, 2015.

[82] A. Farraj and D. Kundur, "On using energy storage systems in switching attacks that destabilize smart grid systems," pp. 1–5, 2015.

[83] I. Darwish, O. Igbe, and T. Saadawi, "Experimental and theoretical modeling of DNP3 attacks in smart grids," *2015 36th IEEE Sarnoff Symposium*, pp. 155–160, 2015.

[84] S. Amini, H. Mohsenian-Rad, and F. Pasqualetti, "Dynamic load altering attacks in smart grid," *2015 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2015*, pp. 1–5, 2015.

[85] J. Zhao, S. Member, G. Zhang, M. L. Scala, Z. Y. Dong, S. Member, C. Chen, J. Wang, and S. Member, "Short-Term State Forecasting-Aided Method for Detection of Smart Grid General False Data Injection Attacks," vol. 8, no. 4, pp. 1–11, 2015.

[86] D. B. Rawat and C. Bajracharya, "Detection of False Data Injection Attacks in Smart Grid Communication Systems," *Ieee Signal Processing Letters*, vol. 22, no. 10, pp. 1652–1656, 2015.

[87] J. Jayachandrabensam and J. D. Anunciya, "Implementation Against DoS Attacks," 2015.

[88] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, “A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids,” *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2659–2668, 2015.

[89] F. A. Author, S. B. Author, and T. C. Author, “Lethal Attacks in the Smart Grid : Spatial and Temporal Based Detections,” pp. 1–6, 2015.

[90] J. Yang, R. Yu, Y. Liu, S. Xie, and Y. Zhang, “A two-stage attacking scheme for low-sparsity unobservable attacks in smart grid,” *IEEE International Conference on Communications*, vol. 2015-September, pp. 7210–7215, 2015.

[91] J. Wang, L. C. Hui, and S. M. Yiu, “Data framing attacks against nonlinear state estimation in smart grid,” *2015 IEEE Globecom Workshops, GC Wkshps 2015 - Proceedings*, 2015.

[92] Z.-H. Yu and W.-L. Chin, “Blind False Data Injection Attack Using PCA Approximation Method in Smart Grid,” *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1219–1226, 2015.

[93] T. Ryutov, A. Almajali, and C. Neuman, “Modeling security policies for mitigating the risk of load altering attacks on smart grid systems,” *2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2015 - Held as Part of CPS Week, Proceedings*, no. 1, 2015.

[94] Q. Yang, R. Min, D. An, W. Yu, and X. Yang, “Towards optimal PMU placement against data integrity attacks in smart grid,” *2016 50th Annual Conference on Information Systems and Sciences, CISS 2016*, pp. 54–58, 2016.

[95] X. Yang, X. Zhang, J. Lin, W. Yu, and P. Zhao, “A Gaussian-Mixture Model Based Detection Scheme against Data Integrity Attacks in the Smart Grid,” vol. 4, no. i, pp. 147–161, 2016.

[96] V. Kumar Singh, A. Ozen, and M. Govindarasu, “Stealthy cyber attacks and impact analysis on wide-area protection of smart grid,” *NAPS 2016 - 48th North American Power Symposium, Proceedings*, 2016.

[97] Y. He, G. J. Mendis, and J. Wei, “Real-time Detection of False Data Injection Attacks in Smart Grids: A Deep Learning-Based Intelligent Mechanism,” *submitted to IEEE Transactions on Smart Grid*, vol. 3053, no. c, pp. 1–12, 2016.

[98] H. Karbouj and S. Maity, “On using TCBR against cyber switching attacks on smart grids,” *IEEE PES Innovative Smart Grid Technologies Conference Europe*, pp. 665–669, 2016.

[99] N. Boumkheld, M. Ghogho, and M. El Koutbi, “Intrusion detection system for the detection of blackhole attacks in a smart grid,” *2016 4th International Symposium on Computational and Business Intelligence, ISCBI 2016*, pp. 108–111, 2016.

[100] K. Khanna, B. K. Panigrahi, and A. Joshi, "Feasibility and Mitigation of False Data Injection Attacks in Smart Grid," *2016 Ieee 6Th International Conference on Power Systems (Icps)*, 2016.

[101] V. B. Krishna, K. Lee, G. A. Weaver, R. K. Iyer, and W. H. Sanders, "F-DETA: A framework for detecting electricity theft attacks in smart grids," *Proceedings - 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2016*, pp. 407–418, 2016.

[102] A. Abdallah and X. S. Shen, "Efficient prevention technique for false data injection attack in smart grid," *2016 IEEE International Conference on Communications, ICC 2016*, 2016.

[103] B. Tang, J. Yan, S. Kay, and H. He, "Detection of False Data Injection Attacks in Smart Grid under Colored Gaussian Noise," 2016.

[104] J. Yan, B. Tang, and H. He, "Detection of false data attacks in smart grid with supervised learning," *Proceedings of the International Joint Conference on Neural Networks*, vol. 2016-October, pp. 1395–1402, 2016.

[105] B. Li, R. Lu, W. Wang, and K. K. R. Choo, "DDOA: A Dirichlet-Based Detection Scheme for Opportunistic Attacks in Smart Grid Cyber-Physical System," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 11, pp. 2415–2425, 2016.

[106] X. Yang, X. Zhang, J. Lin, W. Yu, X. Fu, and W. Zhao, "Data integrity attacks against the distributed real-time pricing in the smart grid," *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*, pp. 1–8, 2016.

[107] K. Khanna, B. K. Panigrahi, and A. Joshi, "Data integrity attack in smart grid: optimised attack to gain momentary economic profit," *IET Generation, Transmission & Distribution*, vol. 10, no. 16, pp. 4032–4039, 2016.

[108] A. Sanjab and W. Saad, "Data Injection Attacks on Smart Grids with Multiple Adversaries: A Game-Theoretic Perspective," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 2038–2049, 2016.

[109] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[110] Y. Zhou and Z. Miao, "Cyber attacks, detection and protection in smart grid state estimation," *NAPS 2016 - 48th North American Power Symposium, Proceedings*, pp. 1–6, 2016.

[111] C. Konstantinou, M. Sazos, and M. Maniatakos, "Attacking the smart grid using public information," *2016 17th Latin-American Test Symposium (LATS)*, pp. 105–110, 2016.

[112] A. G. Wermann, M. C. Bortolozzo, E. Germano Da Silva, A. Schaeffer-Filho, L. P. Gaspary, and M. Barcellos, “ASTORIA: A framework for attack simulation and evaluation in smart grids,” *Proceedings of the NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, no. Noms, pp. 273–280, 2016.

[113] L. Langer, P. Smith, M. Hutle, and A. Schaeffer-Filho, “Analysing cyber-physical attacks to a Smart Grid: A voltage control use case,” *2016 Power Systems Computation Conference (PSCC)*, pp. 1–7, 2016.

[114] M. G. Kallitsis, S. Bhattacharya, S. Stoev, and G. Michailidis, “Adaptive statistical detection of false data injection attacks in smart grids,” *2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pp. 826–830, 2016.

[115] S. A. Yadav, S. R. Kumar, S. Sharma, and A. Singh, “A review of possibilities and solutions of cyber attacks in smart grids,” *2016 1st International Conference on Innovation and Challenges in Cyber Security, ICICCS 2016*, no. Iciccs, pp. 60–63, 2016.

[116] A. Farraj, E. Hammad, A. A. Daoud, and D. Kundur, “A Game-Theoretic Analysis of Cyber Switching Attacks and Mitigation in Smart Grid Systems,” *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1846–1855, 2016.

[117] P. Srikantha, S. Member, and D. Kundur, “A DER Attack-Mitigation Differential Game for Smart Grid Security Analysis,” vol. 7, no. 3, pp. 1476–1485, 2016.

[118] J. Wei and G. J. Mendis, “A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids,” *IEEE Proceedings of the 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids, CPSR-SG 2016 - This Workshop is Part of the CPS Week 2016*, pp. 1–6, 2016.

[119] Q. Yang, D. Li, W. Yu, Y. Liu, D. An, X. Yang, and J. Lin, “Power Flow in Smart Grid,” vol. 4, no. 5, pp. 1726–1738, 2017.

[120] K. Wang, M. Du, S. Maharjan, and Y. Sun, “Strategic Honeypot Game Model for Distributed Denial of Service Attacks in the Smart Grid,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2474–2482, 2017.

[121] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, S. Sargolzaei, and B. Carbunar, “SPECIAL SECTION ON ANALYSIS AND SYNTHESIS OF TIME-DELAY SYSTEMS Resilient Design of Networked Control Systems Under Time Delay Switch Attacks, Application in Smart Grid,” vol. 5, 2017.

[122] Q. Jiang, H. Chen, L. Xie, and K. Wang, “Real-time Detection of False Data Injection Attack Using Residual Prewhitening in Smart Grid Network,” no. October, pp. 83–88, 2017.

[123] R. C. Diovu and J. T. Agee, “Quantitative Analysis of Firewall Security under DDoS Attacks in Smart Grid AMI Networks,” pp. 1–6, 2017.

[124] R. C. Diovu and J. T. Agee, “A CLOUD-BASED OPENFLOW FIREWALL FOR MITIGATION AGAINST DDoS ATTACKS IN SMART GRID AMI NETWORKS .,” pp. 28–33, 2017.

[125] A. Farraj, E. Hammad, and D. Kundur, “A Distributed Control Paradigm for Smart Grid to Address Attacks on Data Integrity and Availability,” *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. c, pp. 1–1, 2017.

[126] N. Renewable, “A Distributed Middleware Architecture for Attack-Resilient Communications in Smart Grids,” 2017.

[127] G. S. Dhunna and I. Al-anbagi, “A Low Power Cybersecurity Mechanism for WSNs in a Smart Grid Environment,” 2017.

[128] Y. Wang, M. Amin, J. Fu, and H. Moussa, “A Novel Data Analytical Approach for False Data Injection Cyber-Physical Attack Mitigation in Smart Grids,” *IEEE Access*, vol. 5, 2017.

[129] Z. Ni and S. Paul, “A Reinforcement Learning Approach for Sequential Decision-Making Process of Attacks in Smart Grid,” 2017.

[130] Dong Liu, X. Zhang, and C. K. Tse, “A stochastic model for cascading failures in smart grid under cyber attack,” *2017 IEEE 3rd International Future Energy Electronics Conference and ECCE Asia (IFEEC 2017 - ECCE Asia)*, pp. 783–788, 2017.

[131] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, “Achieving Efficient Detection Against False Data Injection Attacks in Smart Grid,” *IEEE Access*, vol. 5, pp. 13787–13798, 2017.

[132] D. Velusamy, “An Effective Trust Based Defense Mechanism to thwart Malicious Attack in Smart Grid Communication Network,” 2017.

[133] K. Khanna, B. K. Panigrahi, and A. Joshi, “Bid modification attack in smart grid for monetary benefits,” *Proceedings - 2016 IEEE International Symposium on Nanoelectronic and Information Systems, iNIS 2016*, pp. 224–229, 2017.

[134] R. Deng, P. Zhuang, and H. Liang, “CCPA: Coordinated Cyber-Physical Attacks and Countermeasures in Smart Grid,” *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2420–2430, 2017.

[135] S. Waghmare, F. Kazi, and N. Singh, “Data driven approach to attack detection in a cyber-physical smart grid system,” *2017 Indian Control Conference (ICC)*, no. Icc, pp. 271–276, 2017.

[136] J. Jiang and Y. Qian, “Defense Mechanisms against Data Injection Attacks in Smart Grid Networks,” no. October, pp. 76–82, 2017.

[137] A. Patel, “Destabilizing Smart Grid by Dynamic Load Altering Attack Using PI Controller,” pp. 354–359, 2017.

[138] J. Zhao, J. Wang, and L. Yin, "Detection and control against replay attacks in smart grid," *Proceedings - 12th International Conference on Computational Intelligence and Security, CIS 2016*, pp. 624–628, 2017.

[139] S. A. Foroutan and F. R. Salmasi, "Detection of false data injection attacks against state estimation in smart grids based on a mixture Gaussian distribution learning method," *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 4, pp. 161–171, 2017.

[140] T. Irita and T. Namerikawa, "Detection of replay attack on smart grid with code signal and bargaining game," *Proceedings of the American Control Conference*, pp. 2112–2117, 2017.

[141] O. Igbe, I. Darwish, and T. Saadawi, "Deterministic Dendritic Cell Algorithm Application to Smart Grid Cyber-Attack Detection," *Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017*, pp. 199–204, 2017.

[142] J. R. K. R and B. Sikdar, "Efficient Detection of False Data Injection Attacks on AC State Estimation in Smart Grids," pp. 411–415, 2017.

[143] T. Shen and M. Ma, "Enhanced Security Functionality for Communication Networks in," pp. 19–22, 2017.

[144] P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore, and R. S. Blum, "GPS spoofing attack characterization and detection in smart grids," *2016 IEEE Conference on Communications and Network Security, CNS 2016*, vol. 0, pp. 391–395, 2017.

[145] R. B. Sandeep Kumar Singh and A. Joshi, "Joint-Transformation-Based Detection of False Data Injection Attacks in Smart Grid," *IET Cyber-Physical Systems: Theory & Applications*, vol. 2, no. 3, pp. 143–151, 2017.

[146] H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung, and C.-K. Wen, "Local Cyber-physical Attack with Leveraging Detection in Smart Grid," no. October, pp. 461–466, 2017.

[147] H. Karimipour and V. Dinavahi, "On false data injection attack against dynamic state estimation on smart power grids," *2017 IEEE International Conference on Smart Energy Grid Engineering (SEGE)*, pp. 388–393, 2017.

[148] Q. Yang, D. An, R. Min, W. Yu, X. Yang, and W. Zhao, "On optimal PMU placement-based defense against data integrity attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 7, pp. 1735–1750, 2017.

[149] S. Mishra, X. Li, T. Pan, A. Kuhnle, M. T. Thai, and J. Seo, "Price Modification Attack and Protection Scheme in Smart Grid," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1864–1875, 2017.

[150] P. Wood, S. Bagchi, and A. Hussain, "Profiting from attacks on real-time price communications in smart grids," *2017 9th International Conference on Communication Systems and Networks, COMSNETS 2017*, pp. 158–165, 2017.

[151] C. Wickramaarachchi, C. Chelmis, R. Kannan, and V. K. Prasanna, "Protecting critical buses in power-grid against data attacks: Adaptive protection schemes for smart cities," *FTC 2016 - Proceedings of Future Technologies Conference*, no. December, pp. 1047–1056, 2017.

[152] K. Khanna, B. K. Panigrahi, and A. Joshi, "AI-based approach to identify compromised meters in data integrity attacks on smart grid," *IET Generation, Transmission & Distribution*, vol. 12, no. 5, pp. 1052–1066, 2018.

[153] M. Imran, F. A. Khan, H. Abbas, and M. Iftikhar, "Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks," pp. 217–226, 2018.

[154] M. N. Kurt, Y. Yilmaz, and X. Wang, "Distributed Quickest Detection of Cyber-Attacks in Smart Grid," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2015–2030, 2018.

[155] K. Hamedani, L. Liu, R. Atat, J. Wu, and Y. Yi, "Reservoir Computing Meets Smart Grids: Attack Detection Using Delayed Feedback Networks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 734–743, 2018.

[156] S. Tan, W.-Z. Song, M. Stewart, J. Yang, and L. Tong, "Online Data Integrity Attacks Against Real-Time Electrical Market in Smart Grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 313–322, 2018.

[157] H. Dornhackl, K. Kadletz, R. Luh, and P. Tavolato, "Malicious Behavior Patterns,"

[158] X. Li, J. Xu, H.-N. Dai, Q. Zhao, C. F. Cheang, and Q. Wang, "On modeling eavesdropping attacks in wireless networks," *Journal of Computational Science*, vol. 11, pp. 196 – 204, 2015.

[159] O. Olawumi, K. Haataja, M. Asikainen, N. Vidgren, and P. Toivanen, "Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned," *2014 14th International Conference on Hybrid Intelligent Systems, HIS 2014*, no. May, pp. 199–206, 2003.