Key Management Scheme for Smart Grid

Bashar Ahmed Alohali

A thesis submitted in partial fulfilment of the requirements of Liverpool John Moores University for the degree of Doctor of Philosophy

August, 2016

Acknowledgements

First, great thanks to my Almighty God, Allah, the most merciful and the most beneficent, for his blessings—which have given me the ability, strength and determination to complete a PhD at this prestigious institution—and for everything else he has given me.

I would like to take this opportunity to give thanks to many people for their help, in completing this thesis. Without their support and contributions, the successful completion of my thesis would not have been possible. I would like to express special thanks and gratitude for my director of studies, Dr Kashif Kifayat, for his continuous support, excellent supervision, significant feedback and encouragement, as well as for allowing me to share in his experience.

I would also like to give special thanks to my second supervisor, Professor Qi Shi, for his significant feedback and for the valuable time he spent helping me during many stages of my research. Furthermore, I am deeply thankful to my third supervisor, Dr William Hurst, for his kind support and advice during my PhD studies.

I would also like to express my appreciation to my previous director of studies, Professor Madjid Merabti, the Dean of the College of Sciences at University of Sharjah. I gratefully acknowledge his enthusiastic supervision, support, encouragement and invaluable suggestions during this research.

My thanks also go to the researchers, administration staff and technicians in the School of Computing and Mathematical Sciences at Liverpool John Moores University for their support over the past years.

I am grateful and appreciative toward the government of Saudi Arabia for supporting me financially during my PhD; this allowed this research to continue unimpeded. This support is gratefully acknowledged.

I am also very thankful to my beloved mother, brothers, sisters and wife; their prayers, encouragement and unconditional support enabled me to successfully complete my PhD.

I want to dedicate this thesis to dearly beloved mother; to the spirit of my father (may Allah have mercy on him); and to my wife.

Abstract

A Smart Grid (SG) is a modern electricity supply system. It uses information and communication technology (ICT) to run, monitor and control data between the generation source and the end user. It comprises a set of technologies that uses sensing, embedded processing and digital communications to intelligently control and monitor an electricity grid with improved reliability, security, and efficiency.

SGs are classified as Critical Infrastructures. In the recent past, there have been cyber-attacks on SGs causing substantial damage and loss of services. A recent cyber-attack on Ukraine's SG caused over 2.3 million homes to be without power for around six hours. Apart from the loss of services, some portions of the SG are yet to be operational, due to the damage caused. SGs also face security challenges such as confidentiality, availability, fault tolerance, privacy, and other security issues. Communication and networking technologies integrated into the SG require new and existing security vulnerabilities to be thoroughly investigated.

Key management is one of the most important security requirements to achieve data confidentiality and integrity in a SG system. It is not practical to design a single key management scheme/framework for all systems, actors and segments in the smart grid, since the security requirements of various sub-systems in the SG vary. We address two specific sub-systems categorised by the network connectivity layer – the Home Area Network (HAN) and the Neighbourhood Area Network (NAN). Currently, several security schemes and key management solutions for SGs have been proposed. However, these solutions lack better security for preventing common cyber-attacks such as node capture attack, replay attack and Sybil attack. We propose a cryptographic key management scheme that takes into account the differences in the HAN and NAN segments of the SG with respect to topology, authentication and forwarding of data. The scheme complies with the overall performance requirements of the smart grid.

The proposed scheme uses group key management and group authentication in order to address end-to-end security for the HAN and NAN scenarios in a smart grid, which fulfils data confidentiality, integrity and scalability requirements. The security scheme is implemented in a multi-hop sensor network using TelosB motes and ZigBee OPNET simulation model. In addition, replay attack, Sybil attack and node capture attack scenarios have been implemented and evaluated in a NAN scenario. Evaluation results show that the

scheme is resilient against node capture attacks and replay attacks. Smart Meters in a NAN are able to authenticate themselves in a group rather than authenticating one at a time. This significant improvement over existing schemes is discussed with comparisons with other security schemes.

Abbreviations

AMI	Advanced Metering Infrastructure
AES	Advanced Encryption Standard
BAN	Business Area Network
CA	Certificate Authority
CoT	Cloud of Things
DER	Distributed Energy Resources
DR	Demand Response
DoS	Denial of Service
ECC	Elliptic Curve Cryptography
ESI	Energy Service Interface
FAN	Field Area Network
HAN	Home Area Network
HMS	Home Management System
HMI	Human Machine Interface
ICT	Information and Communication Technology
IAN	Industrial Area Network
IED	Intelligent Electronic Devices
IoT	Internet of Things
PK	Public Key
QoS	Quality of Service
RTT	Round Trip Time or Ping
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SG	Smart Grid
SM	Smart Meter
MDMSs	Meter Data Management Systems
MTU	Master Terminal Unit
SHA	Secure Hash Algorithm
LMN	Last Mile Network
MITM	Man-in-the-middle attack
MAC	Message Authentication Codes
MDMSs	Meter Data Management Systems
NAN	Neighbor Area Network

NCA	Node Capture Attack
VPP	Virtual Power Plant
WAN	Wide Area Network
WAMS	Wide Area Measurement System
WoT	Web of Things
WBAN	Wearable Wireless Body Area Network
WSNs	Wireless Sensor Networks

Table of Contents

List of Figures

List of Tables

Chapter One: Introduction

1 INTRODUCTION

In the last decade the term “Smart Grid” has been used to indicate the fulfilment of typical requirements of energy systems, such as conservation of resources, saving operational expenditure (OPEX) and effective control. The term Smart Grid generally refers to an advanced electricity grid in which the distribution, transmission, generation, and control of power systems are better coordinated, monitored and controlled by the integration of the Smart Grid infrastructure with an advanced information and communication technologies (ICT) infrastructure for improving the reliability, efficiency, economics, security and safety of the electricity grid. It enables a two-way digital communication between utility company and consumer, to communicate to/from smart meters and similar intelligent monitoring systems [2]. However, research on Smart Grids is currently at a fairly early stage; therefore, there are several issues being researched. An essential issue is that Smart Grids must be operationally secure in order to withstand security threats from malicious elements. Secure end-to-end communication is crucial. A fundamental requirement for a secure Smart Grid is to use a key management scheme for secure communication. This thesis addresses key management in secure schemes for the Smart Grid.

This chapter is organised as follows. First, the topic of the thesis is presented and the aims and objectives of the study are enumerated. Second, the novel contributions of the new approach to security in the Smart Grid in the thesis are presented. Third, an overview of the thesis chapters is presented and followed by a summary of the chapter.

1.1 Smart Grid overview and characteristics

A Smart Grid comprises a set of technologies that uses sensing, embedded processing and digital communications to intelligently control and monitor an electricity grid with improved reliability, security, and efficiency. It is a meta-system that, unlike current wireless or other computer networks, uses a complex network to communicate with many heterogeneous devices and systems with different sub-systems [3]. The complexity of the network is a consequence of the services provided by the Smart Grid and the roles played by each of its functional components. It is divided into seven functional components, namely, Customer,

Service Provider, Power Generation, Transmission, Distribution, Operations and Markets. Each of these components serves a specific role and needs to communicate with other components to be able to provide an efficient service. The typical characteristics of a Smart Grid are listed below:

- Improved reliability, efficiency, security and environment by increasing use of digital information and control systems.
- Grid operation and resources in dynamic optimisation with cyber security.
- Integrate distributed resources and generation.
- Integrate distributed demand response.
- Distribution of intelligent technologies for communication, meter, AMI and substation automation [4] .
- Integration of intelligent applications and real-time pricing.

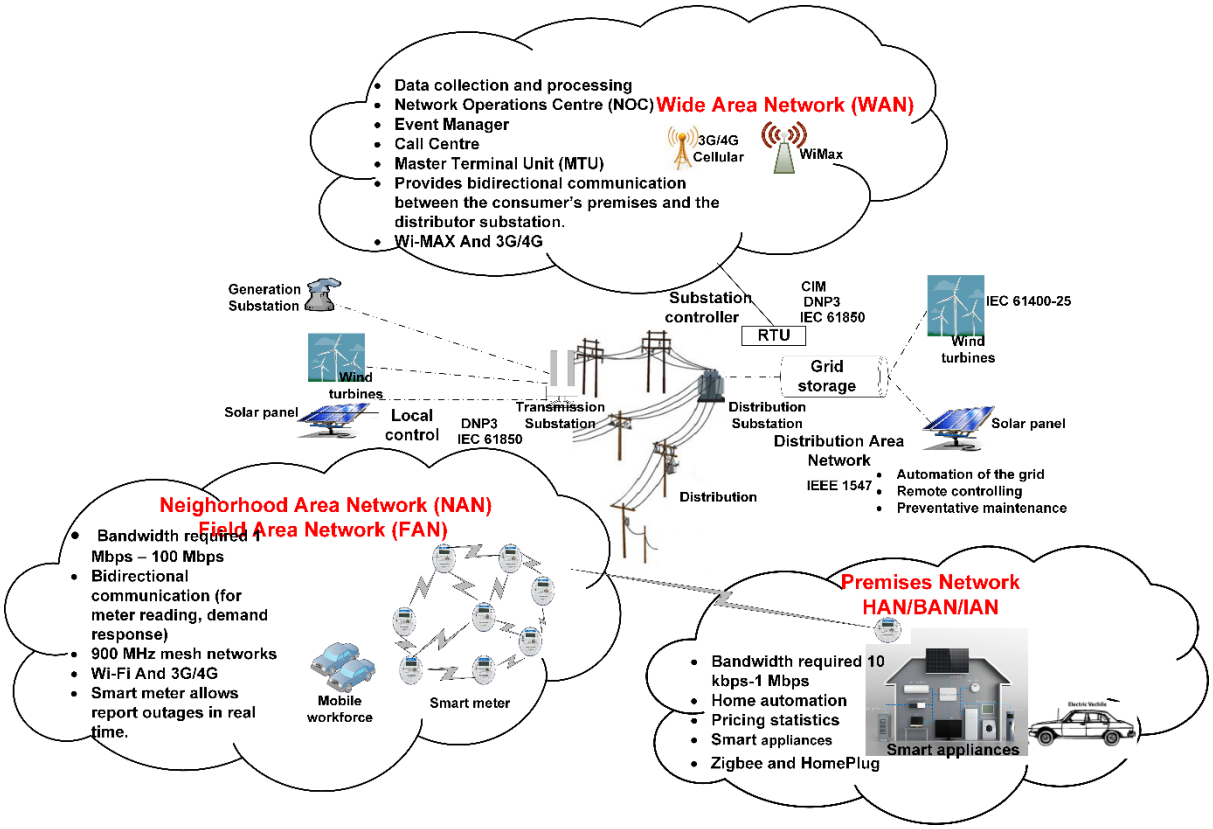

Figure 1-1: Communication domains in a smart grid

The Smart Grid is a modern power electricity system. It operates with sensors, communications, monitoring, automation and computer to achieve safety and security, flexibility, efficiency and reliability in the electricity system. It is an electricity system, which deals with a large number of customers and has an intelligent communications

infrastructure. It enables timely, safe, secure and adaptable information flow needed to provide power to the

evolving digital economy. There are many benefits of the Smart Grid, such as operation based on real-time data, two-way power flow and renewable power generation.

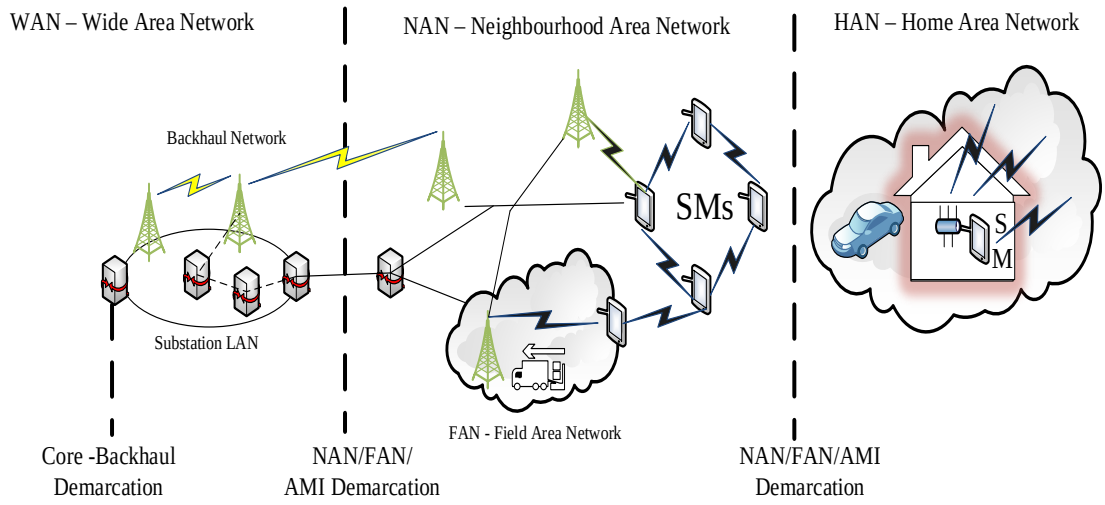

Figure 1-2: Smart Grid - a heterogeneous network

A Smart Grid can be considered as a heterogeneous network, as shown in Figure 1-2, based on the integration of multiple networks such as the Home Area Networks (HANs) for effective energy monitoring, control and management at the consumer end; the Neighbourhood Area Network (NAN) for providing advance metering infrastructure to meter and monitor the HANs; and the Wide Area Network (WAN) to integrate automation on to the Smart Grid backbone [5]. The HAN interconnects to the WAN via a Smart Meter (SM), which is part of the NAN. The majority of the devices in the HAN and NAN are wireless communication nodes. The interconnectivity of SMs into the NAN is collectively referred to as advanced metering infrastructure (AMI) and is the focus of this thesis. The NAN is an interconnection of SMs creating a network (with different topologies), consisting of smart meters and gateways that relay data. The functional layered model is indicated in Figure 1-3. Our focus is on the communication layer in this model.

1.2 Security Challenges and Attacks in Smart Grid

Recently cyber-attacks on critical infrastructure have highlighted security as a major requirement for Smart Grids [6]. Despite its numerous advantages, there are many security

challenges and issues in the Smart Grid, such as access control and identity management, connectivity, privacy, data analysis issues and minimizing cost [7].

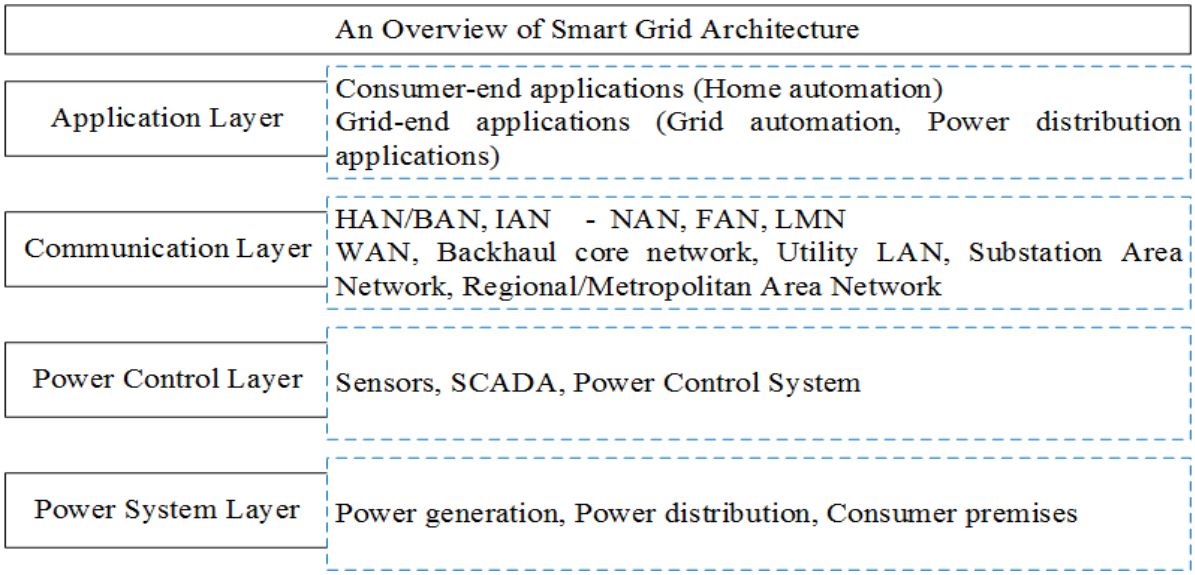

Figure 1-3: Layered functional view of the smart grid

The Smart Grid is classified as a critical infrastructure that provides an essential service to users. The challenge in securing the Smart Grid is that the security solutions should be easily deployable, integrate-able and useable without affecting the performance requirements. Many security solutions have been proposed to fulfil the security requirements of a Smart Grid. However, these solutions are specifically designed for specific security issues, based on a varied set of assumptions, and limited to portions of the functional Smart Grid infrastructure.

Deploying a Smart Grid without adequate security might result in serious consequences such as grid instability, utility fraud, and loss of user information and energy-consumption data [8]. According to a report published by Krebson Security [9], the FBI investigated the hacking of Smart Grid meters in Puerto Rico, Brazil. The bureau distributed an intelligence alert about its findings to select industry personnel and law enforcement officials. The FBI said that it believed former employees of the meter manufacturer and employees of the utility company were altering the meters in exchange for cash, and training others to do so because of "the ease of exploitation and economic advantage to the hacker and the electric customer"

Therefore, it is important to ensure that the data carried by the Smart Grid system is kept confidential and that no one but the right receiver can access the data [9].

In this section we explain the major challenges faced in securing Smart Grids and then we relate the challenges to factors that caused recent attacks on Smart Grids.

1.2.1 Smart Grid security challenges

We list six major challenges faced in securing a Smart Grid. Note that these challenges eventually map on to the three major security requirements, namely, Confidentiality, Integrity and Availability.

a. **Access control and identity management:** There are several challenges with the existing protocol including efficiency, delay, lower overhead and privacy [10]. It is a challenge to ensure that data transmitted via Smart Grids is kept confidential and that no one but the intended receiver is able to see the message. In addition, the Smart Grid contains many components that are interconnected [11]. Because of security concerns related to this, authentication is needed to verify the identity of the receiver in order to avoid any disruption or exploitation [12]. Access to the control centre, transmission, and distribution grids is allowed only for authenticated users, groups, and services [13].

b. **Privacy and security policies:** There is a challenge for suitable security policies to establish relationships among consumers, utilities, and third parties, although applying security and privacy policies should not result in unsatisfactory operational latencies. Information security policies define the guiding rules that security controls are applied to secure data, communication routing, processes and systems. In various cases, the information and network protection policies used by utilities need to update [14].

c. **Threat defence:** There are several vulnerabilities inherent in Smart Grids; therefore, it is a challenge to protect the grids from defined threats by building an effective, layered defence system to function broadly across the entire grid infrastructure. Threat defence provides network segmentation and access control to defend against denial-of-service (DoS) attack. In addition, it provides a suite of security technologies such as firewall, IPS and VPN [13].

d. **Physical security:** Smart Grid systems can have thousands, and often even millions, of remote points and field area networks. This makes it challenging to maintain the physical security of the Smart Grid. The geographical dispersion of these systems also means that it may be difficult to access all of the terminals for maintenance [15].

e. **Connectivity:** Communications connectivity in Smart Grids implies a transition towards an Internet-like distributed environment in which huge numbers of devices are interconnected. This is one of the emerging challenges in this area and as such the application of protective techniques is important [13].

1.2.2 Attacks on Smart Grids

Assailants with different motives and skills can take advantage of weaknesses in the security of a Smart Grid system, and can cause different levels of damage to the system. Attackers at the top level include online hackers, terrorists, workers, opponents, clients, and so on. For example, a client may change data or information, and obtain power without paying for it.

According to Rautmare et al. [16] "the exploitation of the network control system may result in disruption and breaks in operation. That may lead to disruption of service and loss of manufacturing, neither of which is allowable".

a. **Cyber-attack on Ukraine's power grid:** In 2016, when more than 100,000 people in and around the Ukrainian city of Ivano-Frankivsk were left without power for six hours, the Ukrainian energy ministry accused Russia of launching a cyber-attack on the country's national energy grid [17].

b. **Stuxnet:** In 2010, Stuxnet was discovered. It is an advanced and sophisticated malware program that targets industrial control systems. Industrial control systems targeted by Stuxnet are reprogrammed to hide any changes made by a Stuxnet attack. In the early days of Stuxnet attack infection, Iran was the most affected country [18]. However, since Stuxnet can self-replicate, other countries were affected, including Indonesia and India. Security specialists have found that Stuxnet is able to control the speed of motors, and is thus able to send nuclear centrifuges out of control [13]. It is a modern weapon in the cyber war. It was

used to transfer a payload for the target control system. It is the first industrial control system rootkit. It can self-update; in addition, it can inject code into the ladder logic of PLCs, and at that point alter the operations of the PLC, as well as hide itself by alarming false information back to the HMI. Moreover, it adapts to its circumstances [3].

c. **Night Dragon:** In 2011, McAfee reported the discovery of a series of coordinated attacks against energy, petrochemical and oil control systems. The attacks, which mainly began in China, were supposed to have commenced in 2009, functioning ceaselessly and covertly with regard to data extraction [16]. It did not expand its influence and harm as far as the Stuxnet attack; however, it did involve the theft of sensitive and important data. Furthermore, it alarms and evidence of how outside attackers can possibility infiltrate critical systems. At that period, the intended use of the stolen data was unknown, and it could have been used for many motives [3].

d. **Slammer Worm:** Security Focus reported in 2003 that the Slammer Worm had passed through a computer network and targeted a nuclear power plant in Ohio. For almost five hours, the safety monitoring system at the plant was disabled. The infection did not cause any harm, but it alarmed the control system, due to it being under possible attack [13].

e. **Node capture attack:** On Smart Grid application by malicious users such as decrease the reading of meters “electricity bills” or to break the services on people life and so on. Since the Smart Grid reaches each building as well as the complex of communications [19], therefore, it makes it difficult to guarantee physical protection for all the components in the system [6].

f. **Other possible attacks:** One of the well-known attack is the man-in-the-middle (MITM), which is a type of attack whereby the attackers break into an existing connection to interrupt the exchanged data and insert false information into the Smart Grid [20, 21]. This involves eavesdropping on a connection, intruding into a connection, interrupting messages, and carefully modifying data. In addition, Denial-of-Service (DoS) takes place when a system denies service to authorised clients. This may be caused due to resource exhaustion by

unauthorised clients. It is difficult to avoid the DoS in a Smart Grid. Also, it is difficult to stop an on-going attack since the victim and its client may not catch the attack. In this kind of attack, the attacker prevents legal users from having access to information and services by targeting the victim's device and the network connection; this attack stops the user from making outgoing connections on the Smart Grid. Jamming is a DoS attack which targets wireless communication frequency in the Smart Grid [22]. When they are in close range, large amounts of noise may be generated in these appliances. The communication can be jammed so as to make the signal noise very low, and this could lead to the Smart Grid not functioning [23].

1.3 Security requirements for a Smart Grid

In this section, a general and brief review about security requirements in the Smart Grid will be presented including availability, data confidentiality, data integrity and authentication.

In the Smart Grid, the security requirements are one of the main considerations that should be addressed, as malicious users and attackers can modify customers' data or cause any type of attack on an unsecured Smart Grid. Therefore, we should take into account the following factors when considering the security requirements of a Smart Grid:

a. Availability: Availability is one of the primary requirements for a Smart Grid. It is the availability of data in the entire network. The best way to achieve this aim is to have network management and supervision by implementing a reliable and suitable transport layer solution. Therefore, resources should be available in the nodes throughout the whole network. All components should have the capability of self-healing in case any of them fails [24-26]. For example, in the case where power to a node is lost, the other nodes need to reorganise themselves to maintain availability [27].

b. Confidentiality: to make sure that data is not changed or lost. Only permitted and authorised entities should be given access to the data. One of the best ways to achieve confidentiality in a Smart Grid is by using a key management solution [1, 8, 28-30] for encrypting data and establishing a shared secret key among nodes.

c. Integrity: the authenticity of the data received must be confirmed; during the transfer, it must be protected from attackers who are trying to manipulate it. Identity should be confirmed through strong verification. It should implement an implied refusal policy such that access to the network is granted only through precise access permissions [31, 32].

d. Security Weaknesses: Checks must be carried out to ensure that components that interface with the border are protected. In some situations, customer activities can start possible security weaknesses [33]. As such, awareness applications should be put in place to inform the system's customers about the best protection methods when using network resources and applications [27].

e. Devices must know the resources and destinations with which they connect. This is achieved through common verification methods, applying Transport Layer Security (TLS) or Internet Protocol Security (IPSec) [34]. A reliable authentication method is needed while interacting between Smart Grid events. The authentication protocol must function in real-time adhering to restrictions such as lowest computational cost, low interaction expense, and sturdiness to withstand strikes especially Denial-of Service strikes.

f. Authorisation: Authorization is another key requirement for a Smart Grid. It is important that the components of the HAN, NAN and WAN get authorised and is thus allowed to connect with other components. Moreover, it is a good way to make sure that Smart Grids are protected and no malicious node exists in the communication session, as such a node can obtain important information such as the cryptographic key or the secure ID [35].

1.4 Problem definition

1.4.1 Key Management in Smart Grid

Key management is crucial process to achieve data confidentiality (secure communication and information protection) for smart grid. Therefore, many key management schemes are proposed for smart grid. A smart grid comprises several distinct functional segments, which require exchanging data. Secure accesses as well as secure data transportation are two key

requirements for smart grid services. Most key management [8, 28-30, 36-45] schemes available are proposed for specific part of the Smart Grid. Those cannot be integrated due to different security requirements. Therefore, any schemes meant for the Smart Grid as a whole require being able to scale to the size of the network and handle a large concurrency of authentication and/or data transfer and/or command control requests. Bulk command control requests are necessary when addressing demand response situations or an emergency situation on the smart grid network. In addition to such situations, the scheme in place requires to scale in size when new segments of smart meters are added to the network. Such segment sizes can be considerably large (connecting a high-rise residential building or connecting an industrial estate). The security schemes require being able to scale to accommodate such additions and should not impact the storage and processing resources of the devices. These resources are typically used for storing shared keys and generating new hashes or keys. Therefore, scalability is an issue when considering key management for a secure scheme in a smart grid.

A consequence of scalability is the topology of the network. Quite often, the key management schemes are affected by the topology of the network of devices. For example, a tree based hierarchical topology provides a simple means of generating keys for downstream nodes in the sub-trees, whereas, for a mesh network, the key distribution can become a significant overhead, depending upon the degree of connectivity of the nodes. When the network is scaled, it is not unusual to resort to a clustered-tree approach (a mix of tree and mesh, aka partial-mesh) where a cluster head is responsible for the downstream nodes and requires relatively higher storage, if not processing resources. Topology is therefore a significant issue in terms of impact on the resource availability on the devices in smart grid networks. A good key management scheme must therefore be able to have the least impact on the resource requirement on the devices, regardless of the topology of the network.

The data flow within the smart grid extends from the home devices up to the NOC of the provider. A single security scheme that can cover the entire path of the data flow is an ideal requirement. However, while the technology limitations exist, the more important limitations are due to the two different administrative domains that the devices belong to. The devices in the home and the associated group controllers are the private domain of the householder whereas the smart meter and associated devices up until the NOC are the private

domain of the provider. The smart meter interfaces, these two domains and there is a sufficient cooperative action necessary to be able communicate across these two domains. Each domain is viewed as a security risk to another, necessitating a clear boundary between the operations within the home, within the smart grid and between the home and the smart grid. There are no instances of such security schemes that operate across these two domains, in literature. Therefore, designing an integrated security scheme that is interoperable across the domains is a challenging issue until there are regulatory guidelines in place for such communications.

Smart Grid is meta-system where many of systems and applications are integrated using highly complexity connectivity to handle huge amount of sensitive data and information figure 1-1. We should consider node capture attacks as a high threat for communication and data confidentiality. Moreover, ignoring security requirements related to sub-systems in Smart Grid can result in significant damage of data confidentiality or network performance to a Smart Grid. Where it is not practical to design a single key management scheme/framework for all systems, parties and segments in the Smart Grid, it is necessary to consider the security requirements of various sub-systems in the Smart Grid and design the security for the specific sub-system. A secure routing protocol on a smart grid builds logical connectivity among the nodes to form a network.

1.4.2 Node capture attack

A node capture attack involves physically capturing a node, extracting the stored information, use the node to send invalid data on the network or incapacitate it. This may lead to compromise of the entire Smart Grid communication. Moreover, the primary impact of a node capture is providing the attacker a means to launch other types of attack such as DoS, Sybil, Blackhole and other such attacks which affect of providing the proper services. Data confidentiality and customer privacy can be compromised, and that can be led by expansion of the huge amount of data that will be collected. The security of the HAN is not compatible with the security of the NAN.

Therefore, in the event of one of the nodes being compromised, it should not cause the entire security process to break down. The rest of the services should remain secure and available. These requirements should be fulfilled over the available computing and storage resources of the Smart Grid components. Thus, data confidentiality and data integrity are critical

requirements in Smart Grid. Compromise of data confidentiality has a significant effect on users' privacy, which is important consideration that should be addressed.

There are various cryptographic key management solutions that have been proposed to deliver secure communication and decrease the impact of threat of node capture attacks on the Smart Grid. However, these solutions still suffer from its effects.

1.4.3 Scalability

The large-scale network in NAN poses far more challenges for the NAN's nodes compared to nodes in HAN. The network topology in NAN is highly dynamic as nodes regularly join or leave the network session. The communication channel is also subject to many errors and interferences which illuminating unstable characteristics in terms of bandwidth and delay. In terms of solutions to these security challenges HAN and NAN, researchers have proposed different key management schemes [46-52] for secure communications. In the Smart Grid, these schemes try to provide better resilience against node capture attacks, However there is still a chance of the entire Smart Grid being compromised.

Another main issue in key management is to design an adaptable and independent scheme, which can be applicable in different Smart Grid scenarios. Therefore, the solution has to take into account the practical and real network and the requirements for the Smart Grid. Giving this challenge, our intention is to develop a secure end-to-end communication solution for HAN and for large scale NAN. The specific objectives for the solution and the aims on the study are detailed in the next section.

1.5 Research Aims and Objectives

The aim of this thesis is to present an integrated key management scheme that satisfies the communication layer (Figure 1-3) in Smart Grid (HAN, NAN) security requirements. Therefore, the integrated key management approach must be considered based on the communication network and associated security requirements. Thus, scheme should take into account the specific requirements of the Smart Grid system (HAN, NAN), such as availability, resilient to node capture attack, resilient to replay attack, resilient to Sybil attack, scalability, key freshness, and other related properties, such as low-energy consumption on devices. The scheme will secure the communication in the Smart Grid and

prevent any breaches due to malicious attacks. In the event of an attack or a compromise, the impact must be minimal and the operation of the rest of the Smart Grid infrastructure must not be affected in any manner.

To achieve the above-mentioned aim, we have identified the following objectives:

1. Design a key management scheme that offers secure communication for the HAN in the Smart Grid
2. Implement the proposed key management scheme using TelosB motes in HAN
3. Design a key management scheme that offers secure communication for the NAN in the Smart Grid
4. Implement the proposed key management scheme using TelosB motes in NAN
5. Design a secure authentication protocol that supports different communication topologies in the NAN
6. A replay attack and Sybil attack scenarios have been implemented and evaluated in a HAN and NAN scenario.
7. Implement the HAN and NAN network scenarios in a simulation environment using Riverbed simulation to measure performance.
8. Evaluate the developed schemes for HAN and NAN by comparing them with existing solutions.

1.6 Contributions

In completing the above objectives, we have made the following contributions in this thesis:

1. **Key management scheme for a HAN:**

Our proposed key management solution is designed for fulfilling HAN security requirements. We identify the various devices in a home, which are networked. After that we group the devices based on operational/functional factors such as their power consumption and the control functions required. Then, we identify the resource availability

on each device and assess the impact of an attack on the device type. We then list the security requirements of each device group. Based on that we design a secure key management interaction scheme for the groups in HAN. The protocol has been evaluated using TelosB motes and Riverbed simulation. The evaluation results show an improvement in terms of data confidentiality and resilience against node capture attacks. The security analysis is detailed in in chapter five.

2. **Key management scheme for a NAN:**

The main components in NAN segment are smart meters, which form a large-scale network. Therefore, to manage a large scale NAN, organising the NAN into groups of SMs is considered in our scheme. Group key management for NAN has been proposed. In order to achieve a secure end-to-end communication we assign a unique key to each node in the group. This unique key is shared only with the utility company server, and sends encrypted data through other nodes to the utility company Server without decryption at any non-utility company server. We have shown in chapter 6 that using this technique we achieve end-to-end confidentiality.

3. **A light-weight authentication scheme for devices in the NAN:**

In a large-scale environment such as the smart grid, network scalability and availability are two crucial design parameters for a secure scheme. Thus, organising the NAN into groups of SMs is necessary to with the obvious need for grouping SMs in a smart grid, group management is a necessary function within the smart grid. Identification of a group member, members joining/leaving the group is typical group management functions that require authentication. The group members in NAN need to be validated as part of the group. Such validated members can communicate between themselves, primarily for purposes of forwarding data to/from the group head. Therefore, we have proposed a new, secure, group authentication scheme for NAN for Smart Grid. The scenario of a multi-hop network is considered where the nodes require multiple hops to communicate with the NOC, which is the entity that issues the keys. Two topology scenarios, star-star and mesh are considered and separate authentication processes are defined for their operation. The main feature of our scheme is the ability to address security of all communication, which takes place in the network. Moreover, the scheme is specifically designed for NAN and centralized authentication. A detailed of the scheme found in chapter 5 of this thesis.

4. Development of HAN and NAN Test bed using TelosB motes

The secure schemes on a Smart Grid build a logical connectivity among the nodes and components. To evaluate our proposed scheme by launching Replay, Sybil and node capture attacks. Therefore, presents an analysis of the impact of the replay attack and Sybil attack when the scheme uses multi-hop forwarding with the intermediate nodes re-encrypting it for a specific upstream node.

a. Replay attack

We choose to perform the implementation of replay attack on TelosB mote, for launching replay attacks. Which was programmed to capture data packets sent from a smart meter and re-sending them at a later point in time, expecting to authenticate and gain entry into the network. The implementation comprises of four programs done by a nesc program in a TinyOS, one each for the three SMs and the NOC. These programs communicate with each other using the packet content and packet format used by the secure scheme in Fig 3.

The following steps are performed for the implementation of replay attack:

- L-SM authenticates with NOC
- Malicious node captures the authentication packets
- Malicious node sends captured packets to NOC and attempts to authenticate
- GW initially receives the packets, processes them and sends them to the NOC
- NOC receives packets and processes them, identifies them as duplicate packets and discards them.

b. Sybil attack

The Sybil attack was done using a TelosB mote, which was programmed to change its ID randomly, between IDs 110 and 115 and attempt to authenticate with the NOC. The NOC key and the gateway key were stored in the memory of the mote, emulating a capture of an authenticated mote. The first two pairs of messages show successful authentications from node IDs 111 and 112. Node 110 is already authenticated. The captured node attempts to authenticate as node 110 in the third pair of messages.

5. Topology independence for NAN interconnectivity

Node capture attacks in the proposed KM-NAN can significantly threaten network security as well as degrade performance. Based on the simulation results in figure 6-34, it is identified that partial mesh topology is more resilient topology as compared to star topology for KM-NAN against node capture attacks. As compared to KM-NAN star, KM-NAN mesh topology is more flexible as it can allow smart nodes to choose between multiple routes to transmit/receive data to the target location, if one of the node(s) compromised. Due to the flexibility offered by mesh topology, it is not only resilient but also an ideal solution with easy to deploy in KM-NAN.

1.7 Thesis Structure

Chapter one introduction: This chapter is organised as follows. First, the topic of the thesis is presented with its aims. Second, the novel contribution of the new approach posited in the thesis is presented. Third, an overview of the thesis chapters is presented. Finally, the chapter is summarised.

Chapter two Smart Grid Background: In this chapter, Smart Grid technology has been discussed followed by Smart Grid architectural layers. The communication layer (HAN, NAN and WAN) has been of great interest as this layer play a crucial role in the deployment of a Smart Grid based on the integration of HAN, NAN and WAN. This chapter introduces different Smart Grid technologies including AMI, WAMS, and substation distribution systems and so on. We then discussed in detail the Smart Grid architecture including an application layer, communication layer and power control system layer. Finally, we describe the IoT and its role of in the Smart Grid.

Chapter Three Security in the Smart Grid in this chapter discussed the main security issues in Smart Grid. We have explained general challenges related to communication and management where must be considered before Smart Grid benefits can be achieved. Moreover, this chapter provide a general and brief review about security requirement in Smart Grid will be presented including availability, data confidentiality, data integrity and authentication.

Chapter Four Literature Review. This chapter presents a critical overview on literature review and research works relating to key management, authentication. It also includes

discussions on the existing solutions of key management for HAN, NAN, WSN, SCADA and other.

Chapter Five Key Management Scheme for Communication Layer in the Smart Grid (KMS-CLSG). This chapter introduces our proposed solution. We have classified the solutions based on communication layer in Smart Grid networks, including Key management in HAN and NAN. The chapter provide detail of security analyses**.**

Chapter Six Implementation and Evaluation. In this chapter we have explained the implementation and evaluation phase in our proposed solution. We have described the methodologies of the implementation including the attacks that have been addressing the in order to evaluate the proposed scheme such as replay attack, Sybil attack.

Chapter Seven Conclusion and Future Work. This chapter provides a summary of our contributions. We highlight some issues that may be addressed in future including security of WAN, integration of Smart Grid with cloud and design of a simulation tool for Smart Grid communications security. The thesis concludes by highlighting the work have been achieved and summary of results.

1.8 Summary

Over the last decade, the computer network, Internet of Things (IoT) and Wireless Sensor Networks (WSNs) have brought revolutionary changes to the means and forms of communication for a large number of applications including Smart Grids. The traditional energy networks have been modernised to Smart Grid to boost the energy industry in the context of efficient and effective power management, performance, real-time control and information flow using two-way communication between utility providers and end-users. However, integration of smart two-way communication in Smart Grids comes at the cost of cyber security vulnerabilities and challenges. It is a solution to such vulnerabilities that we address in proposing a secure end-to-end communication scheme for the HAN and NAN segments of the Smart Grid.

Chapter Two: Smart Grid Background

2. Background

The advancement in information and communication technology (ICT) has not only given the world a smart and high-quality life but also an efficient power system, energy solutions and intelligent homes to live in. Energy is one of the fundamental requirements to fuel the smart technology and so a 'smart' way of living, and electricity is generally used as the primary source of energy.

According to a report by [53], worldwide energy consumption is predicted to increase annually by 1.6% from 2011 to 2030, adding 36% to the global energy consumption by the year 2030. In addition to the continuous growing demand for energy and the environmental concerns, efficient and effective power performance and management and pricing are becoming more and more critical requirements. The traditional 20th century power grids are not designed to handle rising power demand, increasing proportion of renewable, fluctuating energy generation, electricity blackout, integration with advanced communication and controls, and smart metering infrastructure. The continually growing dependence on electricity and demand for efficient and reliable energy distribution have been constantly addressed to provide a modernised electric system to ensure efficient and effective power performance and management, real-time bidirectional control and information flow between utility providers and end-users and active monitoring. Therefore, the Smart Grid is the future of the power grid; it is designed to meet the future energy requirements that entail capacity, reliability, efficiency, security, sustainability and safety.

To overcome the limitations and challenges experienced by traditional 20th century power grids and to fulfil the requirements of the 21st century, 20th century power grids have started to be replace by a modernised electricity system integrated with advanced communication and controls to enable responsive and resilient energy delivery. This modernised electricity system is known as a Grid System and is also defined as "electricity with a brain", "the energy internet", and "the electronet" [54].

In this chapter, we present an overview of the various aspects of the Smart Grid including Smart Grid technologies, architecture and IoT. The chapter concludes with a summary of the important points.

2.1 Smart Grid Technologies

The market for Smart Grid technologies is growing rapidly as the demand for more responsive and resilient energy delivery rises across the globe. The fundamental technology to integrate intelligence into the grid has been in place for decades. However, recent times have seen fast-tracking technological developments and shifting priorities among utility companies. The integration of ICT and Smart Grid has shown various technologies such as advanced metring system (AMI), wide area measurement system (WAMS), substation automation system and common information models (CIF), which are discussed in the following sub-sections.

2.1.1 Advanced Metering Infrastructure (AMI)

Advanced metering infrastructure (AMI) is core technology to deliver the operational and business benefits towards the implementation of the Smart Grid system. AMI plays a major role in providing the necessary communication and control functions required to deploy energy management services such as pricing schemes, meter readings, demand response and power quality. The deployment of AMI ensures a granular control for consumers to monitor the utilisation of energy in addition to growing distributed energy resources (DER). Ensuring a secure AMI is crucial to satisfy both the consumers and service owners that Smart Grids are reliable and trustworthy [55] .

It is a system that manages, gathers data, measures, analyses electricity usage and involves smart meters and service providers via two-way communication. AMI enables service providers to inform their users of electricity pricing at any time, and allow monitoring of demand in real time. Therefore, AMI is different from advanced meter reading (AMR) technology as it allows bi-directional meter communications [30]. According to the authors in [56], an AMI system involves different technologies and applications including smart meters, user gateways, home area network, wide-area communications infrastructure, and meter data management systems (MDMSs), which are integrated to perform as one system. Similarly, the authors in [57] state that AMI is a system used to collect, store, analyse, and

measure electricity usage data, which provides a fitting gateway between the consumer and electricity supply. Figure 2-1 below provides an illustration of the AMI network and how the components of this network communicate.

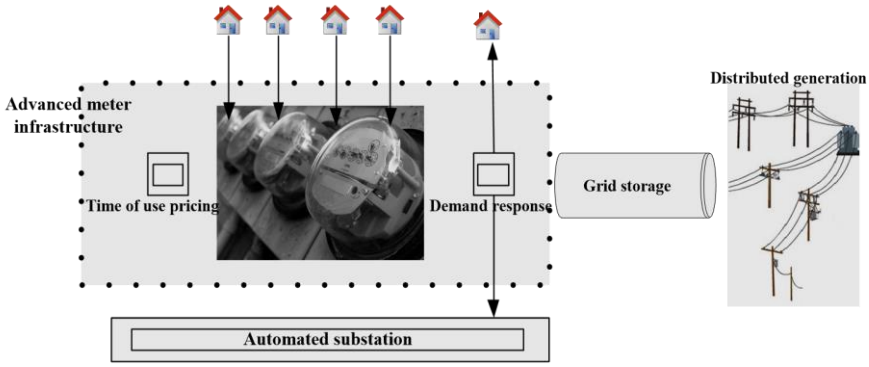

Figure 2-1: The AMI network

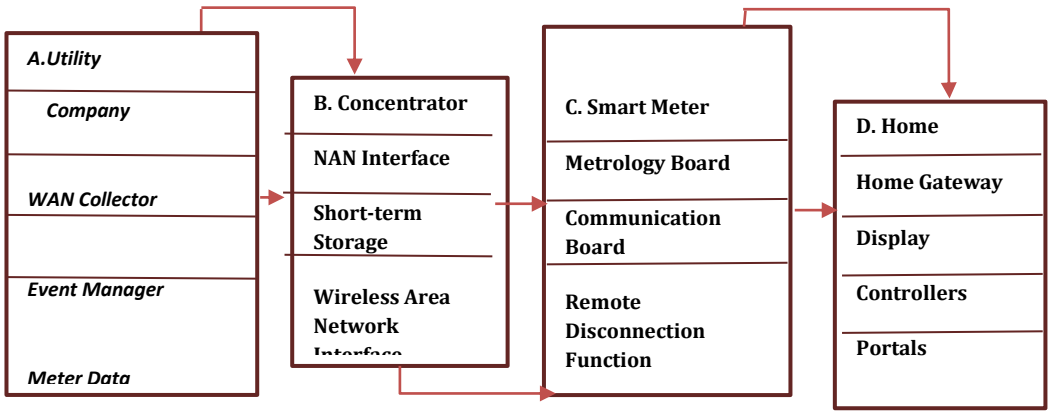

Figure 2-2: Four major components of the AMI [10]

SMs are installed in domestic and commercial establishments, and have to be interconnected to communicate with upstream management entities [55]. They require a topology to be formed, and the topology depends upon how they are distributed within a specific wireless range. Ideally, a single hop to the upstream node, typically performing 'gateweying', 'security/authentication' and 'data aggregation' functions, is desired. This may be possible largely in dense areas such as structured high-rise buildings or shopping centres. In a sparsely inhabited area or condominiums, the limited wireless range of the SMs might require a multiple hop path to the upstream node in the NAN (Figure 2-2). This implies that the intermediate nodes in the hop path must provide an authenticated forwarding of data from the downstream nodes. The security mechanisms deployed must ensure that each node is authenticated centrally as well as by the group. The focus of this thesis is on a

secure authentication scheme for such multi-hop networks formed by SMs in the NAN. The SMs in a group in the NAN need to authenticate within the group, and the group should be aware of SMs joining and leaving the group so as to ensure that the security assets distributed reach only the intended members of the group [55]. This aspect of security in NANs will be further discussed in subsequent sections of this chapter.

2.2 Smart Grid Architecture

In this sub-section, Smart Grid architecture is introduced. A discussion is put forward on the functionalities of each layer and related communication technologies are highlighted. Smart Grids heavily rely on high-speed, intelligent, reliable and secure bi-directional communication and control between utilities and consumers to coordinate the generation, distribution and consumption of energy effectively and intelligently. Due to a variety of communication components, the Smart Grid has been considered as a heterogeneous network infrastructure and generalised into four layers: application layer, communication layer, power control layer and power system layer, as shown in Figure 2-3.

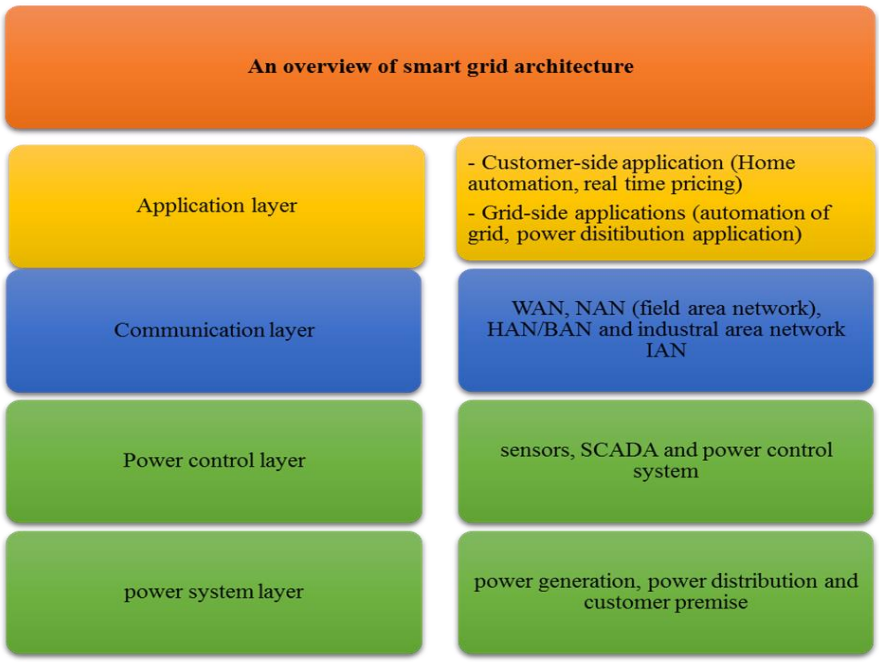

Figure 2-3: Smart Grid architecture - Overview [60]

The power system layer involves electricity generation, distribution and customer premise. The power control layer is comprised of sensors, control systems (such as SCADA) and the power control system. The communication layer consists of WAN, NAN (field area

network), HAN/BAN. Finally, the application layer includes power transmission, customer application, and real-time pricing.

The application layer can generally be categorised into customer-side applications and grid-side applications. It provides Smart Grid applications for customers (such as information on energy usage or real-time pricing, critical peak pricing, automated controls for appliances and smart devices) and for the utility provider (such as substation monitoring, fault detection, integrated volt-VAR control [60].

The communication layer provides a network for the transport of data and information in a two-way, efficient, reliable and secure manner between the power systems and the data centre. As part of the communication layer, the HAN is initially a multi-supplier environment composed of smart appliances that need to be set-up together continuously using suitable standards such as ZigBee, and HomePlug NANs are employed for covering large geographical areas and distributed field devices. Typically, NANs use Wi-MAX (Worldwide Interoperability for Microwave Access) or 3G/4G for wide-range communication. Table 2.1 presents a comparison of different communication protocols and standards.

The WAN performs as the core network. It consists of the backbone network and the backhaul network. In the WAN, the backbone network connects the utility backbone and substation to provide high-capacity communication with minimal latency, and commonly uses optical fibres. To provide broadband connectivity to the NAN, the backhaul network is the link between the WAN and the NAN. In addition, it interconnects distributed systems such as sensors, SCADA, remote terminal units (RTU) and mobile workforces. The main task of the WAN is to transport the smart grid's data to distant sites in an efficient and reliable way. Utility control centres have been operating WANs and managing the operations and processes in the grid for many applications, such as grid monitoring and SCADA [61].

The major components in Smart Grid architecture are Electric Household Appliances, Renewable Energy Resources, Smart Meter, Power utility Centre and Service provider [62], as illustrated in Figure 2-4.

Electrical Household Appliances (smart and legacy) are expected to be able to communicate with smart meters via a House Area Network (HAN), assisting efficient energy intake control to all home devices. The Smart Grid uses renewable energy resources such as solar and wind power to provide power to home devices. Smart meters contain a microcontroller that has memory, digital ports, timers, real-time, and serial communication facilities [63]. Smart meters sign-up the power intake generally and transmit it to the utility server, connect or detach a customer's source of energy and send out alarms in case of a problem. The power utility communicates with the smart meters to control energy intake [62].

2.2.1 Application Layer

The application layer of a Smart Grid generally consists of consumer-end and grid-end applications. At the consumer-end it provides energy usage information, real-time cost, critical peak cost, and automated control for smart devices. At the grid-end, it provides substation monitoring and fault detection, etc. [60].

2.2.2 Communication Layer

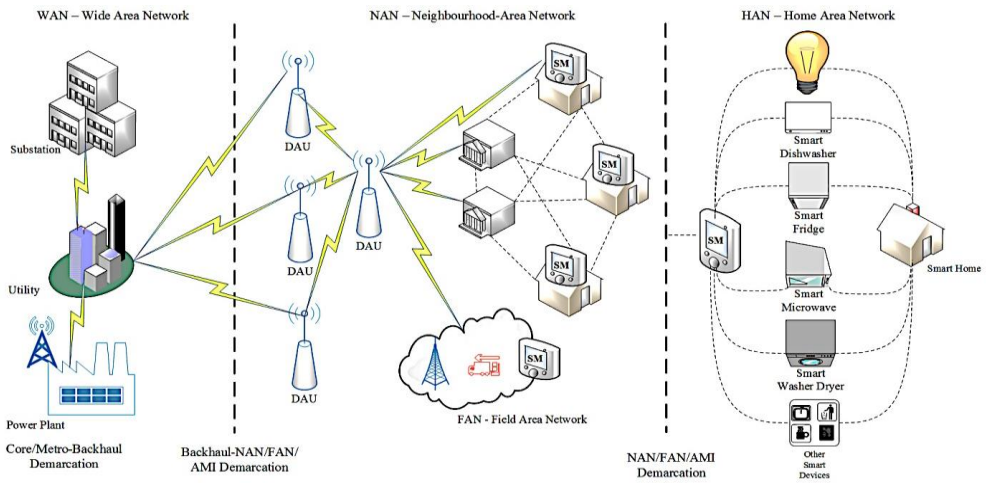

Figure 2-4: An overview of smart grid communication domains

The Smart Grid is considered to be an intelligent network of meta-systems and subsystems providing energy cost-effectively and reliably. Figure 2-5 illustrates the communication network of a smart grid. It has a hierarchical structure, comprising three areas, Home Area Network (HAN), Neighbourhood Area Network (NAN) or Field Area Network (FAN) and Wide Area Network (WAN). Smart Grids derive benefit from the fact that homes can be automated using ubiquitous computing and such automation can help in

energy monitoring. It is the embedded Internet of Things that provides several services linked to physical devices or resource monitors and enables the management of the energy consumption of devices and appliances. The communication layer consists of three major IP-based and field-level communication networks: wide area networks (WAN), local area networks (LAN) and consumer area networks (CAN). The communication networks are further divided/categorised into more sub-communication networks, as listed below [60].

2.2.2.1 Home Area Network (HAN)

A home area network (HAN) is a sub-communication network at the CAN end, which helps to extend the Smart Grid capabilities into a home by exploiting various network technologies/protocols such as IEEE 802.15.4/ZigBee, Wi-Fi, RFID, Ethernet, Z-Wave, HomePlug, Wireless M-Bus, Wavenis [64], as shown in Figure 2-5. The HAN is sometimes referred as a Business Area Network (BAN) or Industrial Area Network (IAN), as these networks share many common characteristics and design disciplines. A HAN, integrated with sensors and actuators, enables the consumer end to remotely interconnect as well as control various automated smart devices ranging from smart meters to in-house displays, renewable energy sources and storage, to smart appliances such as washing machine, refrigerators, TVs, oven, lights, heating, ventilating, and air conditioning (HVAC), and plugs for electrical cars [64]. One of the important components of a HAN is the home energy management system (HEMS), which enables consumers to monitor how much power their household has consumed. The HAN enables dedicated demand side management (DSM) such as energy efficiency management and demand response through active involvement of power users and consumers [65]. A HEMS is the backbone of communication between SM and home appliance. To facilitate the interconnectivity in the HAN with external networks such as neighbourhood area network (NAN), which interconnects smart meters, an energy service interface (ESI) as a HAN gateway has been developed as part of the Utility AMI Open HAN Energy Services Interface.

2.2.2.2 Neighbourhood Area Network (NAN)

A Neighbourhood Area Network (NAN – sometimes referred to as a Field Area Network (FAN) or Last Mile Network (LMN)) is a sub-communication network at the LAN end. A NAN, as shown in Figure 2-6, consists of multiple HANs between the individual service connections to distribute electricity and information [66]. A data-aggregator unit (DAU)

within the NAN collects the data from HANs with smart meters using network technologies such as WiMax, Zigbee, PLC and ANSI C12 Protocols [67] [65]. The NAN behaves as an access network to forward data from consumers to the backhaul enterprise office. In addition to data collection, the DAU also consists of a NAN gateway, which enables NAN connectivity with the HAN and WAN. The NAN is one of the components of Smart Grids because it is responsible for transporting huge volumes of data and distributing control signals between utility (service) providers and smart devices connected at the consumer's end.

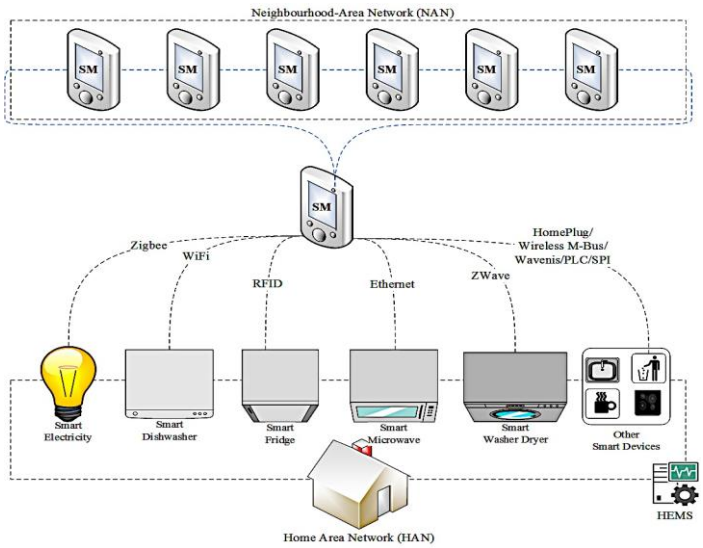

Figure 2-5: HAN communication technologies

2.2.2.3 Wide Area Network (WAN)

A wide area network (WAN) acts as a bridge between HAN, NAN and utility network and enables connectivity between multiple distribution systems by covering a very large area. Based on various technologies such as Ethernet, cellular network, and broadband networks, WAN provides a backhaul network to connect utility networks to consumers' premises for communication and NAN data transmission [65]. A WAN aggregates data from multiple NANs and relays it to the utility provider's private networks. The utility service provider's WAN is also responsible for delivering a two-way communication network, required for substation communications, power quality monitoring, and distribution automation, while

associating aggregation and backhaul for the AMI along with any demand response and demand side management applications [68].

2.3 Internet of Things (IoT)

Through the years, the era of information technology and pervasiveness of digital technologies has showed an exponential growth, with an increase in the numerous technological improvements available, offering a wealth of new services. Recently, the Internet of Things (IoT) has attracted a great deal of attention, since it involves several applications, including smart grids, control systems, remote healthcare, smart mobility, managing traffic flow and so on. In addition, it is expected to grow in popularity in the future. The term IoT was used by Kevin Ashton in 1999 to mean that all things – including physical, digital or any entity that has a chip placed inside it or can be identified via an IP-address – are connected through wired and wireless networks [73]. Basically, it is ubiquitous connectivity with everyday objects communicating and operating constantly. This is leading to a smart world with ubiquitous computing and provides services that enable remote access and intelligent functionality [74]. However, over the past decade, the term has been integrated into a wide range of applications such as healthcare, control and monitoring, utilities and transport [75]. According to Rose et al. [76], the term Internet of Things can refer to "scenarios where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers, allowing these devices to generate, exchange and consume data with minimal human intervention".

Table 2-1 Different communication technologies in a smart grid

Technology	Application	Data rates	Approx. Coverage
ZigBee	Used for HAN, home appliances and AMI	250kbps	10 to 100m
HomePlug	It is a power line used for electricity wiring to communicate in HAN [64]	14Mbps 200Mbps	300m
WiMAX	Demand response, AMI/wireless automatic meter reading (WAMR)	75 Mbps	50Km
Cellular G3-PLC	SCADA and controlling for RTUs AMI, demand response, monitoring for remote site [65].	240kbps 33.4 kbps	50Km 6km

Satellite	AMI, WAN	450 Kbps	Depends on number of satellites and their beams

Pervasive and ubiquitous sensing enabled by Wireless Sensor Network (WSN) technologies has transformed the way we drive our personal and professional lives. In this technology-oriented globe, WSN technologies are driving the economy and look like they can offer numerous opportunities in various applications by enabling the ability to measure, gather and realise environmental indicators, from mild ecosystems and natural resources, to urban environments and control systems. With the global attention on energy and water management and conservation, the Internet of Things is of great interest to extend the associated benefits of Smart Grids beyond automation, distribution and monitoring [77].

2.3.1 Role of IoT in the Smart Grid

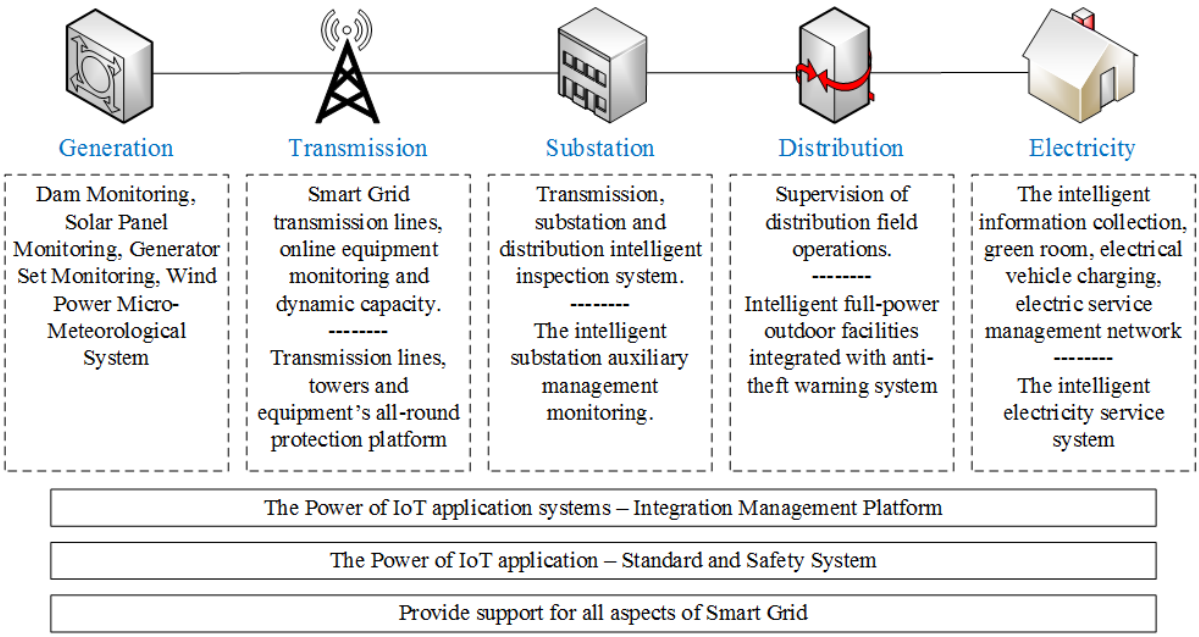

Figure 2-6: Role of IoT in smart grids [79]

The IoT scope provides three essential layers: perception (sensing layer), reliable transmission (network layer) and intelligent processing (application layer). The IoT enables real-time analysis of big data flows that could improve efficiency, reliability and economy of systems, for example, connecting all appliances in the smart house to save electricity or provide better monitoring. Therefore, the IoT is convenient, sustainable and makes things

intelligent everyday of future life [78]. From the Smart Grid perspective, the IoT provides a distributed computing intelligence across the whole infrastructure with the help of embedded nodes to achieve an efficient and effective management of Smart Grid infrastructure. From HAN to NAN and WAN to utility providers, the IoT, along with its key technologies such as radio frequency identification (RFID), sensor networks (WSNs), smart technology and nanotechnology, takes a dominant place due to the fact that it helps to provide real-time, accurate and comprehensive communication, data transmission and monitoring over power transmission and distribution [79]. The role of the IoT in the context of Smart Grids can be visualised from Figure 2-7 [79]:

The growth of the IoT and Smart Grids is mutually supportive. On the one hand, the IoT used in a Smart Grid plays a crucial role to promote the development of Smart Grids and achieve real-time information gathering, monitoring and controlling of important operating parameters [80]. On the other hand, the intelligent communication networks have become a driving force towards the development of the IoT network paradigm [81].

2.3.1.1 Cloud of Things (CoT)

The CoT represents an important extension of the IoT. The CoT refers to the virtualisation of IoT infrastructure to provide monitoring and control. IoT deployments typically generate large amounts of data that require computing as well as storage. A cloud infrastructure that can provide these resources can effectively offload the computing and storage requirements within the IoT network to the cloud. An added benefit is the ability to virtualise the underlying IoT infrastructure to provide monitoring and control from a single point. An application using IoT could therefore become a smart application. A CoT connects heterogeneous appliances to the virtual cloud domain. Both tangible and intangible objects (home appliances, sensor-based and network-enabled) and surrounding people can be integrated on a network or into a set of networks [82]. The CoT suggests a model consisting of a set of services (or commodities) that are delivered just like the traditional commodities. In other words, the CoT can provide a virtual infrastructure which can integrate analytic tools, monitoring devices and visualisation platforms [83]. Moreover, the CoT is a recent technological breakthrough that can enable end-to-end service provisioning for users and businesses to directly access applications on demand from anywhere, anytime [82].The

emerging CoT services will enable a new generation and intelligent use of a collection of applications that will be fed with real-time data and analysis, as shown in Figure 2-6.

In a smart grid, the occupant expects to be able to monitor and control various systems in a home using a Home Management System, a typical CoT application. The operation is based on real-time data and two-way communication with renewable power generation. One of the main purposes of a smart home is to adapt to the green, energy saving, environmentally friendly concepts that have emerged in recent years. There are many applications involved with smart homes, including demand response, dynamic pricing, system monitoring, cold-load pick-up, and the mitigation of greenhouse gas emissions [84]. A CoT for a HAN is expected to play an important role in smart grids. The obvious benefits of deploying a CoT based on Smart Grids are improved storage, computing offload from the sensors and devices and faster access via the Internet [84]. The following are the summarised benefits of utilising a CoT in a smart grid:

a) Better-quality storage ability, memory, and maintenance of the resources

b) Reduced energy consumption of devices

c) Real-time control and fast, extensive analytics

d) Capability to support several platforms and OS.

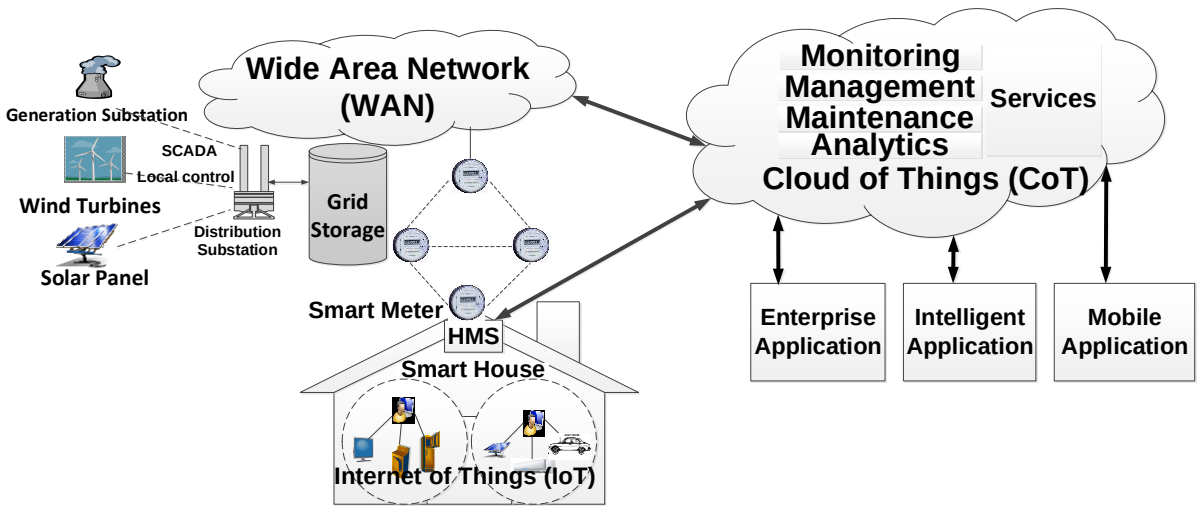

Figure 2-7: CoT for a smart grid

2.4 Security in the Smart Grid

The efficiency and reliability of a Smart Grid severely depends on it having reliable and secure communication and control systems. These systems are becoming more and more sophisticated to achieve better and more reliable control. The high degree of reliability corresponds sophisticated security schemes to cope with cyber-attacks and breaches. The lack of strong security in power grid systems can cause severe damage to a nation's economy and growth development, from small scale to large scale. In 2003, due to a Slammer Worm attack via a dial-up network connection on a computerised safety monitoring system, the Davis-Besse nuclear power plant in Ohio was turned down and it took a couple of hours to restore the service to normal [97]. In March 2008, the Hatch nuclear power plant in Georgia had an outage of over 48 hours due to the date on the control system being reset and badly damaging the safety system after a security update was applied and the machine was rebooted [98].

Stuxnet is considered to be one of the first malicious coding attacks targeted at industrial control systems responsible for monitoring and controlling large-scale industrial facilities like power plants. In 2009 and 2010, Stuxnet, a 500-kilobyte computer worm, targeted Iran's industrial sites and infected at least 14 sites and destroyed a thousand or more centrifuges at a uranium-enrichment plant [99]. A great threat is also posed by cascading power system failures, which allow intruders to bring down grid components, causing the collapse of the power transmission and blackouts such as the 2003 blackout in northeast US, a 2011 blackout in California, Arizona and Mexico, and a 2011 blackout in 2012 [2]. In addition, the cyber-attack on Ukraine's power network also highlighted the importance and challenges of security in the Smart Grid context [17].

2.5 Security Challenges in the Smart Grid

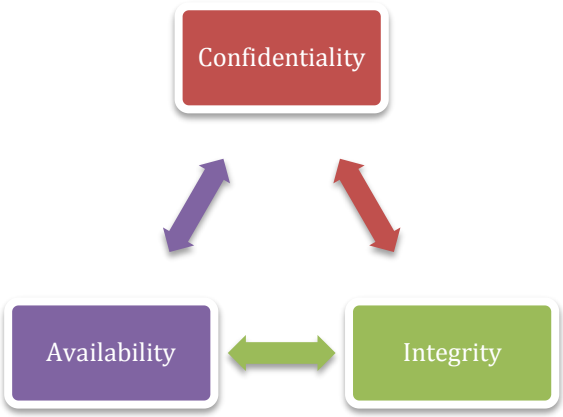

Figure 2-8: Security requirements

In smart grids, cyber security and privacy have been regarded as one of the biggest challenges due to the fact that power transmission and the communication network can be vulnerable in physical as well as cyberspace. According to the US National Institute of Standards and Technology (NIST), a Smart Grid must be able to cope with three severe security challenges: confidentiality (C), integrity (I) and availability (A), as shown in Figure 2-8 [100]. This section provides an overview of security challenges in smart grids, including confidentiality, integrity, availability, privacy as well as key management challenges and cyber-attacks.

Figure 2-9 shows a taxonomy of security challenge concerns in the smart grid, where security challenges have been categorised based on host level, architectural level and credential level. The architectural challenges are further categorised under policy mapping, denial of service (DoS) to impact system's availability and information security. The information security challenges such as confidentiality, integrity and authorisation challenges can be achieved through a cryptography mechanism with efficient key management approaches.

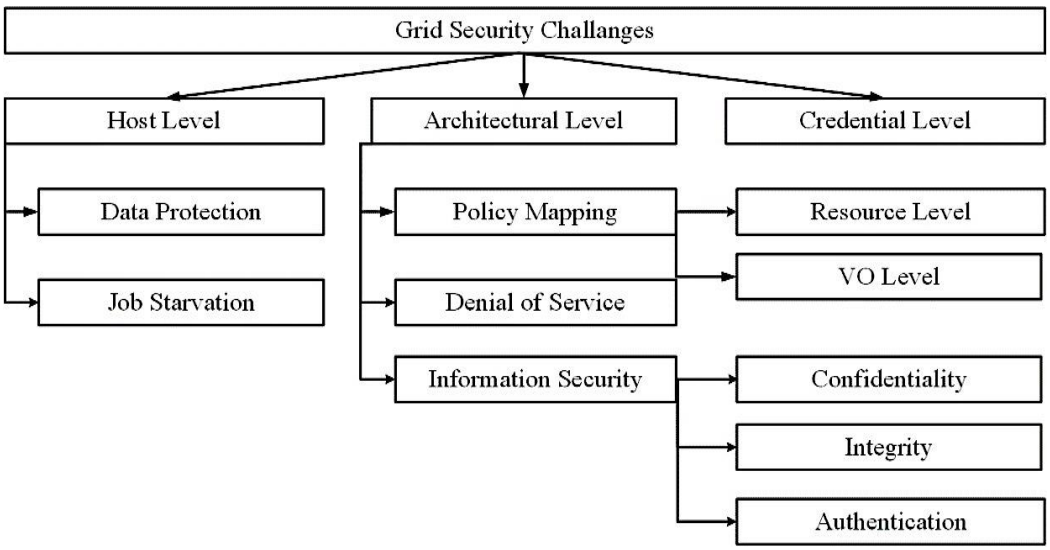

Figure 2-9: Taxonomy of security challenges in the smart grid [101]

2.5.1 Data Confidentiality

In the context of Smart Grid authentication, the security parameters involve identifying the person authorised to get into the Smart Grid system and so thwart malicious activities. In order to secure the Smart Grid from unauthorised access to maintain the confidentiality. Abuse of confidentiality results from exposure of private information and, with the increasing accessibility of customer information over the communication network, ensuring confidentiality has become a significant challenge. Some examples of attacks targeting confidentiality are: illegitimate access to device memory, spoofing of payload, altering of a smart meter software, message replay and data injection attacks [102]. Therefore, it is very vital for the grid system to identity the legitimate and illegitimate users using secure authentication approaches and strategies to main confidentiality. To counter such attacks, encryption/decryption through secret key management approaches has been considered, in addition to device configuration reset, and replacing/removing compromised nodes.

2.5.2 Integrity

The integrity parameter of the security refers to the protection of the sensitive data against any interception and/or damage by illegitimate users. In the Smart Grid context, system integrity refers to the protection of measured sensitive data such as metering data, voltage readings, device status and control commands. The risk to integrity (i.e. system integrity, process integrity and data integrity) in a Smart Grid can come from various threats, such as

replay and data injection attacks and allowing intruders to get access to the entire network [92].

2.5.3 Availability

In the Smart Grid context, the availability parameter must be considered as the first priority since the availability of a power system plays a vital role in our everyday lives. Therefore, it is crucial to ensure that all the components of a Smart Grid are available and accessible to provide services to consumers. Malicious threats like denial-of-service (DoS) and/or distributed DoS (DDoS) can severely damage the system's availability, such as causing degraded performance and blackout, impacting society as well as business. To counter such attacks, the replacement of a tempered attack, transmitting messages over a different channel frequency and updating secret keys have been considered. Consequently, there is a massive need to assess the impacts of and countermeasures for such attacks on a Smart Grid.

2.5.4 Privacy

With the advancement of savvy networks, the amount of sensitive data included and exploited within Smart Grids has significantly expanded in recent years. The deployment of Smart Grids and intelligent electronic devices (IED) can provide a massive amount of personal and sensitive information about consumers such as electricity usage, living pattern and habits, and their availability [103]. The privacy of consumers' personal and sensitive data is vital to successful adoption and the deployment of smart grids, as poor privacy can expose both the consumer and the utility service provider to their competitors and malicious activities [45]. Therefore, a secure Smart Grid must integrate a framework to ensure that the measured data is going to be gathered, utilised and revealed under conditions offering strong protection.

2.5.5 Key Management

As a countermeasure to security threats and to enhance confidentiality, integrity and privacy within Smart Grid systems, encryption and authentication approaches based on cryptography keys are of great interest. The cryptography mechanisms have been categorised as symmetric and asymmetric/public key cryptography. The former mechanism (symmetric cryptography) is based on a single key shared between communication devices

whereas the latter mechanism (asymmetric cryptography) is based on a combination of public and private keys. Asymmetric cryptography mechanisms such as RSA [104] and Diffie-Hellman key [105] have been considered infeasible for IoT/sensor nodes because of the high computational complexity [45]. On the other hand, a symmetric cryptography mechanism, based on a single key, is faster and preserves less power; however, it presents the key management with challenges in maintaining confidentiality and integrity.

A secure key, responsible for encrypting and decrypting data, is crucial to ensure secure communication. Unauthorised or illegitimate access to a secure key will result in a vulnerability threat to sensitive information, personal information, billing information, living style, habits and system control. It is, therefore, a secure management and validation of a secret key is a fundamental requirement for key management approaches and to enhance Smart Grid security and establishing a relationship of trust.

2.5.5.1 Key Management Issues in the Smart Grid

Due to a variety of communication components, the Smart Grid has been considered as a heterogeneous network infrastructure and generalised into four layers: application layer, communication layer, power control layer and power system layer, as shown in Figure 2-3. The selection and implementation of cryptography mechanism and thus the key management is vital in the Smart Grid context, due to heterogeneous infrastructure and resource-constrained nature of the integrated nodes. Due to the heterogeneous nature of the network, a single key management approach is not an ideal approach for all networks – such as smart meter, AMI, NAN, and SCADA – in the Smart Grid [69]. Therefore, the key management approach must be considered based on the communication network and associated security requirements. According to [45], a secure and efficient key management approach is the combination of various processes such as key generation, key distribution, network joining and leaving process, key renewal, revoking and destruction process, additional node joining and replacement. Due to the heterogeneous nature of the network, network topology, transmission pattern and resource-constrained nature of the sensor nodes, key management has been a challenging issue.

Due to the different network topologies of NAN networks (such as star, tree and mesh/partial mesh), the scope of key management varies significantly. The connectivity between neighbouring nodes in all three topologies varies significantly, therefore, a secure key

management scheme must be able to cope with the appropriate topology while ensuring all the vital processes of a secure and efficient key management approach, such as key generation, key distribution, network joining and leaving process, key renewal, revoking and destruction process, additional node joining and replacement [106].

In addition to network topology, network transmission (i.e. unicast, multicast and broadcast) can severely weaken the key management approach. A NAN can communicate via unicast, multicast and broadcast transmission; therefore, a key management scheme must be able to cope with all types of communication while maintaining security. In [45], a key management scheme based on a key graph was proposed for the AMI considering unicast, multicast and broadcast transmission. The key management scheme provides the key generation, key freshness, authentication and integrity, and forward and backward security. However, it lacks the key distribution, key destruction, key renewal/revoking and node replacement phases to ensure security.

According to [45], a secure and efficient key management approach is a combination of various processes such as key generation, key distribution, network joining and leaving process, key renewal, revoking and destruction process, additional node joining and replacement. Considering the fact that a Smart Grid consists of millions of interconnected devices spread across a large number of locations, the key management scheme must be scalable to dynamically adapt the network to integrate all key management processes.

2.5.5.2 Meta-system Interconnections

The Smart Grid is a type of meta-system where a single computing resource composed of a heterogeneous group of autonomous computers (HAN, NAN and WAN) is linked together by a network. The meta-system interconnections raise various challenges, a critical one of which is security, as it opens doors for an intruder to execute an attack from any component of the meta-system. Key management for securing communication between components in a Smart Grid is a fundamental requirement. However, due to the meta-system and heterogeneity of the smart grid, a single key management scheme is not ideal to fit all components [107]. Therefore, the security requirement in a meta-system like a Smart Grid must be considered based on the components involved in communication.

In addition to security, interconnections in meta-systems generate exceptional volumes of data, speed and complexity with ad-hoc data exchange in which centralised coordination and control is very difficult to achieve [108]. The management of metadata in Smart Grid meta-systems is a highly challenging task. A suitable information and communication architecture is required to allow seamless communication and data exchange to avoid data uncertainty, vastness or integration issues.

2.6 Attacks on the Smart Grid

Smart Grids are vulnerable to various threats and attacks like node capture (NC) attacks, denial of service (DoS) attacks, distributed DoS (DDoS) attacks, replay attacks, data injection/alteration attacks, identity spoofing attack, and compromised key attack. Some of the critical attacks are discussed below.

2.6.1 Node Capture Attack

In the Smart Grid context, a node capture (NC) attack is one of the most severe threats due to the unattended nature of the integrated sensor nodes. As the name implies, a NC attack allows an intruder to capture a node and get access to the system by compromising the secure key, node identification, and the data transmitted between node and network [109] [110]. In the context of HAN and NAN, a node can easily be compromised due to a node capture attack. Figure 2-10(a) shows the NAN topology with normal nodes without any compromised node, whereas Figure 2-10(b) shows the NAN topology with two compromised nodes due to a node capture attack as a threat to NAN topology.

In Kifayat et al. [111] , three critical factors responsible for opening a door and leading intruders to capture and compromise the node and so the entire network, have been highlighted. These three critical factors are cryptography, node deployment and node density.

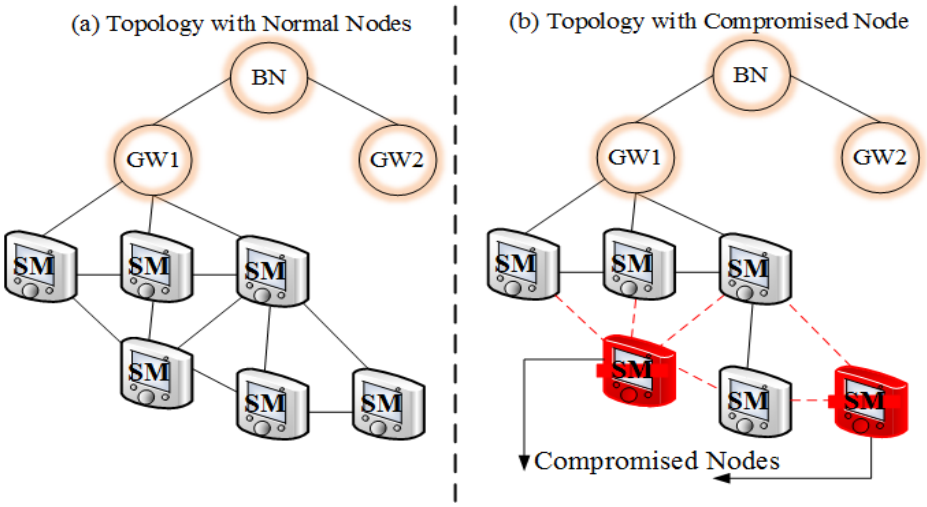

Figure 2-10: NAN topologies - impact of compromised nodes

- ***Cryptography:*** Cryptography and key management are considered to enhance the security of data transmitted across the AMI and authenticate the involved nodes. A weak and poor key management approach can become a threat for the entire network as a compromised node can allow an intruder to get access to sensitive information.

- ***Node Deployment:*** A node deployment plays a critical as it defines the NC attack's scope. In the Smart Grid context, a neighbourhood area network (NAN) can be deployed in the form of star, tree and mesh topology. The impact of an NC attack on a Smart Grid can vary based on the network topology, such as the fewer the communication links between neighbouring nodes (such as tree topology), the greater the possibility for an intruder to threaten the entire network, as evident in Figure 2-11(a). In contrast to tree topology, mesh topology provides a higher number of communication links, reducing the possibility for an intruder to threaten the entire network. Thus, mesh topology provides more routes between neighbouring nodes, and is therefore more resilient to NC attacks.

- ***Node Density:*** A Smart Grid such as a NAN with high node density can be severely threatened by an NC attack as the higher the node density, the larger the network for the intruder to target.

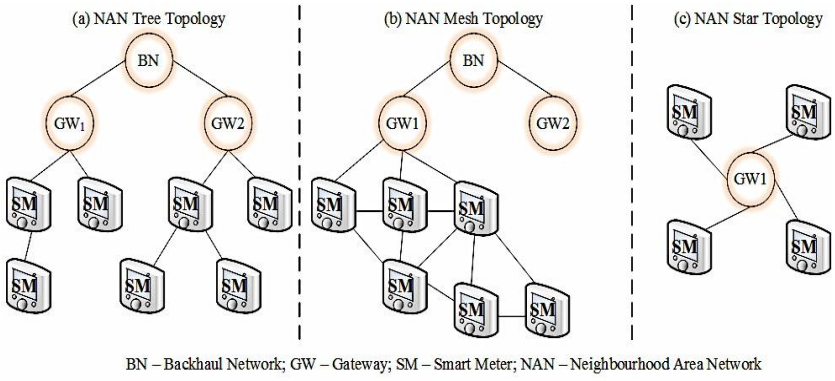

Figure 2-11: NAN topologies (Tree, Mesh and Star)

2.6.2 Denial of Service (DoS)

The denials of service (DoS) and/or distributed denial of service (DDoS) are a common type of attack on communication networks. The DoS/DDoS attacks target the system availability by thwarting message delivery through delaying, blocking or corrupting the communication between Smart Grid components. The availability of a Smart Grid is its fundamental requirement and therefore the Smart Grid system must be secure enough against the DoS attacks at all communication layers, such as physical layer, MAC layer, network and transport layer [107]. Table 2.2 shows the DoS attacks based on the communication layer in the context of power system.

Table 2-2: DoS attacks in Power Systems [107]

Communication Layer	Attacks in Power System
Physical layer	Jamming in substations
MAC layer	ARP spoofing
Network/Transport layer	Traffic flooding, Buffer flooding

- ***Physical Layer:*** The data flow between the network components in a Smart Grid significantly relies on the communication channel. If the communication channel between nodes and the control centre becomes the target of a DoS attack (i.e. jamming the communication through injecting a large number of packets) by an intruder, then it can significantly affect the power substation system's performance due to delayed delivery of time-critical messages [112]. Due to the delay-constrained nature of the Smart Grid infrastructure, even a low-level DoS attack (jamming the network to add delay) can cause severe damage by adding to the delay for time-critical control communication.

- ***MAC Layer:*** In addition to jamming at the physical layer, spoofing (i.e. masquerading as another device to inject fake information) is a relatively severe threat at the MAC layer as it targets both the system's availability and integrity. From the Smart Grid perspective, a compromised node can broadcast fake address resolution protocol (ARP) packets to bring down the connectivity of smart nodes to substation nodes [113].

- ***Network and Transport Layer:*** Network and transport layers are vulnerable to DoS threats due to the TCP/IP protocol model and the multi-hop communication. DoS attacks such as distributed traffic flooding and worm propagation over the Internet via network and transport layers can cause severe damage to the entire network [107]. In a study by Jin et al.[114]. The impact of a buffer-flooding DoS attack on a DNP3-based SCADA network was evaluated. DNP3 protocol has been widely used in power SCADA systems to communicate the observed sensor state information to the control centre. It is highlighted that SCADA systems are quite vulnerable to DoS attacks like buffer flooding.

In the context of HAN and NAN, a node can easily be compromised due to a node capture attack. The compromised node can be used to trigger a DoS attack, where a compromised node illegitimately sends a large number of malicious packets or performs malicious activity at a rate, which can severely upset the communication between nodes. In the context of HAN/NAN, where multi-hop communication is common, the DoS attack can exhaust nodes' storage, computing and processing capability. The scope of the attack can vary based on the network topologies, as shown in Figure 2.11. It is therefore clear that Smart Grids must be secured to avoid DoS/DDoS attacks.

2.6.3 Sybil Attack

A Sybil is a malicious and masquerading type of attack in which a malicious or compromised node represents multiple forged identifications similar to other normal/honest nodes. The normal nodes, due to their lack of ability to distinguish forged nodes, are misled into communicating with malicious nodes [115]. This enables malicious and compromised nodes to attack routing, data aggregation, fault-tolerant schemes, resource allocation and misbehaviour detection protocols and sensitive data flowing in the network to damage the

system's efficiency, confidentiality and integrity [116]. Zhang et al, discussed three Sybil attack domains, named as community, social and mobile domain, in the context of IoT to define the edge and the capability of the intruder, as shown in Figure 2-12 [117].

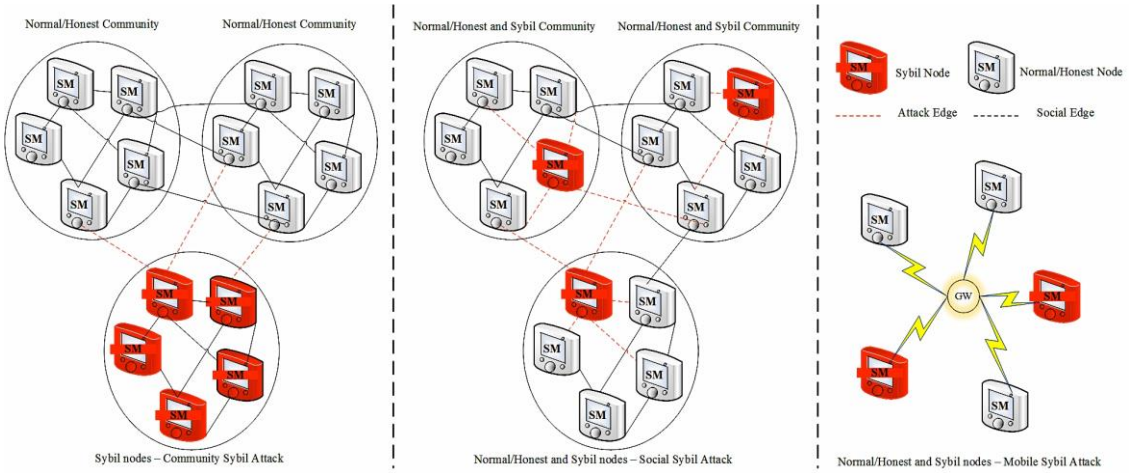

Figure 2-12: Types of Sybil attacks [117]

In the community Sybil attack as shown in Figure 2-12, intruders build the connections with the Sybil community with other malicious nodes. In community-level Sybil attacks, the connectivity with normal/honest nodes is not strong, due to limited connectivity. As compared to a community Sybil attack, a social Sybil attack shows that a malicious node can connect with other Sybil nodes as well as with normal/honest nodes. Due to more social connectivity, Sybil social attack is more vulnerable to Smart Grid as AMI is more exposed to the intruder. As compared to both community and social Sybil attacks in the mobile domain is dependent on the dynamic topology due to the node mobility. Due to its dynamic nature, it is less vulnerable to attack compared to community and social Sybil attack as the latter attacks allow intruders to attack a static network.

In the context of the HAN and NAN, a node can easily be compromised due to a node capture attack. The compromised node can be used to trigger a Sybil attack, where a compromised node illegitimately claims multiple identities as Sybil nodes to the HAN and the Gateway. Figure 2-13(a) shows the NAN topology with normal nodes without any compromised node or Sybil attack. Due to a node capture attack, a node (SM) has been compromised, as shown in Figure 2-13(b), as a threat to the whole NAN topology. The intruder exploits the compromised node to initiate a Sybil attack, as shown in Figure 2-13(c), where a compromised attack represents the multiple forged identifications as SM w, x, y,

and z to other nodes in the NAN to retrieve confidential data, mislead other nodes, severely affect the network traffic and report false readings.

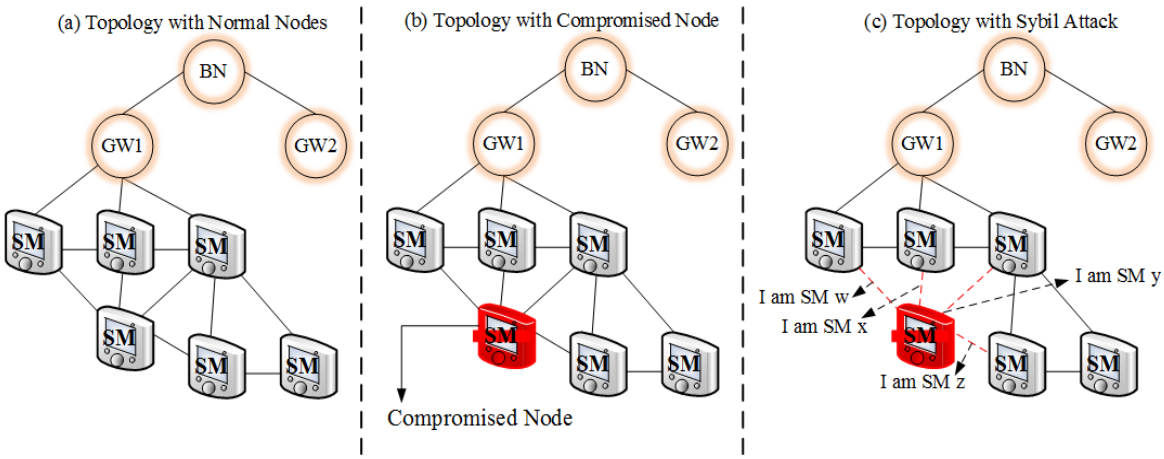

Figure 2-13: Sybil attack due to compromised node in the NAN

The interconnectivity of SMs in the NAN is collectively referred to as advanced metering infrastructure (AMI) and is vulnerable to Sybil attacks. Detecting and eliminating a Sybil attack quickly and accurately has been a key challenge due to the resource-constrained nature of sensor nodes integrated into the Smart Grid as they present a trade-off between security and adopting learning to defend against a Sybil attack. The integration of strong cryptography and authentication approaches can be used to prevent a Sybil attack by restricting compromised node from pretending to be legitimate nodes.

2.6.4 Replay Attacks and Data Injections

Intruders can deploy a replay attack by secretly capturing, intercepting and resending (replaying) the data packets back into the system. A message secretly recorded by an intruder can hold secret information, allowing the intruder to intercept/modify by injecting data and then resending the data packet with the same privileges to gain access to the system. In the Smart Grid context, an intruder can secretly record the data transmitted from a consumer to smart meters and evaluate it to get the consumer's power usage routine. Based on the analysis, the intruder can exploit access to the smart meter by injecting the control signals into the system, such as AMI [118]. Figure 2-14 shows an example of a replay and data injection attack, where an intruder exploits the compromised attack to listen, record, intercept and replay the data to mislead other nodes and report fraudulent readings. The access can be used to damage the system, reduce the system's performance or steal

electricity. One of the prime examples of a replay attack is the Stuxnet worm, which targeted Iran's nuclear programme [99]. The Stuxnet worm allowed intruders to remotely access the sensing and actuating devices to intercept and inject malicious code into the software program to initiate coordinated attacks against the SCADA infrastructure. In addition to damaging the system, replay attack and data injection can be used to steal energy[119]. Strong encryption and a secure key management scheme can protect Smart Grids against replay attacks and data injection.

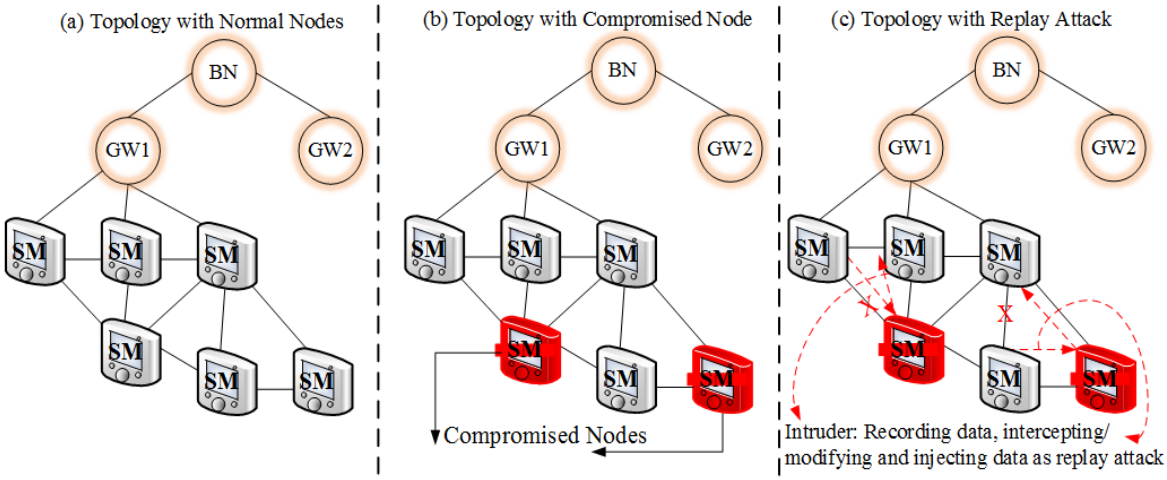

Figure 2-14: Replay and data injection attacks due to a compromised node in the NAN

2.6.5 Repudiation Attack

Considering the fact that a Smart Grid consists of millions of interconnected devices spread across a large number of locations, one of the fundamental requirements of the energy suppliers and end-consumer value-added energy service is the assurance that data flowing over the communication network is coming from the entities responsible for it. A lack of non-repudiation is one of the major barriers to building a trustworthy Smart Grid as it can cause energy theft, wrong meter readings and so affect the billing information [120]. Therefore, it is vital to have Smart Grid nodes should not be able to repudiate. Repudiation attacks can be controlled by integrating strong cryptography with efficient key management and mutual inspection strategies to ensure that data or control information has been issued by the actual source responsible for that action [102, 120]

2.6.6 Eavesdropping Attack

Wireless communication is one of the fundamental forms of communication in smart grids. Wireless communication is carried out in open space and is therefore vulnerable to eavesdropping attacks by an intruder. Eavesdropping attacks can allow intruders to catch sensitive information from smart meters to analyse the consumers' living patterns and damage confidentiality and integrity. Integrating strong cryptography with efficient key management can control such attacks.

2.7 Summary

Table 2-3: Attacks on a HAN and their impact

Groups	Attacks	Attack impact
1	DoS	Unable to turn ON/OFF a device in the group, device inaccessible. , stop systems work as normal.
2	DoS, spoofing	Device is inaccessible, Impersonate a group device, send spurious data, stop systems work as normal.
3	DoS, spoofing , Traffic analysis, Replay attack, Sybil attack	Device is inaccessible, impersonation, spurious data injection, stop systems work as normal.
4	DoS, Traffic analysis, Replay attack	Loss of control, spurious data injection, Stop systems work as normal

The HAN and NAN are subject to a variety of attacks and require specific mitigation features to be built into any scheme that provides security for the NAN and HAN. We put down the potential attacks, their impact and the necessary mitigation features for each attack. From that, we derive the security features that the schemes we intend to design must possess to secure the HAN and the NAN. Table 2-3 provides the list of potential attacks in a HAN and their impact. Table 2-4 that provides the potential mitigation features required in the security scheme to be designed for the HAN follows it. A similar approach is taken to arrive at the necessary security features for the security scheme to be designed for the NAN, in Table 2-5. All these requirements are used to compare the features available in the security schemes available for smart grid security, in the following chapter where we review the existing literature available.

Table 2-4: Security requirements for a HAN

Groups	Two way Communication Requirements	Security	Security Requirements
1	Low	Low	Authentication
2	Low	Low	Authentication+ signature
3	Medium	Medium	Authentication+ encryption+ time synchronize
4	High	High	Authentication+ encryption+ time synchronize + signature

Table 2-5 shows the most important attacks that could target the NAN. The security requirements from the NAN are drawn from the potential impact of the attacks. The table also summarises the potential mitigation techniques in the last column. The scheme for the NAN must take into account the attack mitigation factors drawn from this table.

Table 2-5: Security requirements for a NAN

Attacks	**Attack impact**	**Security Requirements**	**Potential mitigation**
NAN sniffing	Capture data and spurious data injection	High	Authentication (A)+ encryption (E) + time stamp (TS)
NAN comm. blocking	Block packets sent over the NAN	Medium	A+E
NAN msg. tampering	Tamper meter data in order to alter charges	High	A+E+TS
Neighbor meter DoS	Stop normal data traffic	High	A+E+TS
Concentrated node DoS	Stop normal data traffic	High	A+E+TS
Node capture attack	Steal all the information stored within the node.	High	A+E+TS
Replay attack and Sybil attack	Loss of control, spurious data injection, Stop systems work as normal.	High	A+E+TS

The research for Smart Grid technologies is growing rapidly as the demand for more responsive and resilient energy delivery rises across the globe. The fundamental technology to integrate intelligence into the grid has been in place for decades. However, recent times have seen fast-tracking technological developments and shifting priorities among utility companies, with renewable generation and increased consumer storage to achieve efficient and effective power performance and management and cope with rising power demand, the increasing proportion of renewables, fluctuating energy generation, and electricity blackouts. However, this raises various challenges ranging from reliability to efficiency, economics and energy storage technology, to big data management and integration, and privacy and security.

In the Smart Grid context, cyber security and privacy have been regarded as one of the biggest challenges due the fact that the enormous amount of data storage and transmission might reveal personal information such as end-users' activities, billing information, habits, their preferences, and energy usage. The enormous exchanges of information and messages have raised severe security threats. Therefore, the critical and sensitive information and control messages need to be protected against unauthorised access and vulnerability threats. In this chapter, various security challenges including secret key management and attacks have been discussed.

Chapter Three: Literature Review

3. Introduction

The Smart Grid contains heterogeneous communication networks, including small-scale (e.g., a substation system) and large-scale (e.g., the AMI system) networks, wireless and wire-line networks. Thus, it handles critical and sensitive information and control messages need to be protected against unauthorised access and vulnerability threats. The previous chapter, several security issues, challenges and security requirements including key management and authentication have been discussed.

This chapter presents, highlights and considers various key management schemes. In general, it is observed that there are two approaches taken for the initial authentication with the network – using a pre-deployed key or dynamically generating a key. Most schemes prefer to use a symmetric key and justify its use with the low computing power required, the low computing delay and the low storage required due to the reduced key length (typically 128 to 160 bits). However, there are schemes that choose to use asymmetric key cryptography, designating an upstream server as a trusted CA. Such schemes use asymmetric key cryptography for the initial authentication and key exchange. A symmetric key is used for encrypting data exchanged.

Schemes that are originally designed for WSNs can be effectively implemented for Smart Grid use. Table 3-1 gives a brief comparison of the features of a WSN and a SG network. However, there are certain factors that determine the suitability of a specific key management solution. These factors depend upon the functional topology of the Smart Grid segment where the devices are deployed (i.e., a HAN or a NAN). The functional topology, in turn depends upon the data flow patterns (i.e., sensor-to-sensor or sensor-to-NOC), the direction of the flow, radio range and connectivity (single hop vs multi-hop) and the data reliability required. This impacts the type of communication that is used to distribute the keys – unicast and multicast/broadcast. Likewise, the choice of using a unique key per sensor or a group key is impacted. Added to these are the limitations of the sensor devices in terms of energy use, computing capability and memory storage. The various key management schemes presented address different aspects mentioned above. It is therefore evident that

each of the schemes is efficient for a specific set of factors and no single scheme claims to provide a generic solution, deployable across the Smart Grid, efficiently.

Table 3-1: Major differences between WSN and SG networks

Features	**WSN**	**SG**
Connectivity	Mostly, ad hoc	Structured
Security requirement	High	High
Functionality	Monitor and control	Two way exchange data, monitor and control, new electricity generation facilities.
Heterogeneous network	No	Yes
Performance	Limited-resource devices	Limited-resource and high-resource devices

The Smart Grid contains heterogeneous communication networks, including small-scale (e.g., a substation system) and large-scale (e.g., the AMI system) networks, wireless and wire-line networks. Moreover, it handles with critical and sensitive information and control messages need to be protected against unauthorised access and vulnerability threats. The security issues and challenges including key management and attacks have been discussed in the previous chapter.

It is not practical to design a single key management infrastructure to generate and distribute keys for all networks in the Smart Grid. Moreover, key management on a Smart Grid is to be performed and protected in its communication networks among various parties such as a smart meter, AMI, sensors, IED and SCADA. Therefore, it is not practical to design a single key management infrastructure to generate and distribute keys for all systems and parties in the smart grid. Furthermore, it is important to consider the security requirements of various systems in the Smart Grid for chosen key management schemes [121]. Many approaches have been proposed so far to implement a key management system for smart grids. In order to understand the key management issues and inconveniences for smart grids, we first need to review and compare these recently proposed approaches and architectures aimed at distributing and managing authenticated keys for Smart Grid systems.

In [106], a protocol is proposed that provides secure unicast, multicast, and broadcast communications in a Smart Grid network. This protocol applies a binary tree approach that supports these three kinds of secure communications. It reduces the computation overhead and protects communication in unicast, multicast, and broadcast scenarios. However, the efficiency of the computation overhead is unknown when one or more nodes leave or join the session. The communications overhead is also unknown. Dapeng et al. proposed a key management scheme for smart grids. They analysed the key management requirements for a Smart Grid such as the proposed scheme, and found that they have to be efficient and scalable due to the transmission and reception of the low-power sensors to ensure mutual authentication between a sensor and an aggregator [122]. They proposed a key management scheme for use in Smart Grids that meets these requirements. The proposed scheme is based on a public key and secure Needham-Schroeder authentication protocol. They tested the scheme by launching a man-in-the-middle attack, and the replay attack, which can be successfully rejected. Furthermore, they addressed the issue of additional vulnerabilities in session keys and communication. The main advantages of this scheme are high security, scalability, fault-tolerance, and accessibility. However, they mixed both PKI and trusted anchors, which increases complications for the Smart Grid since these schemes require at least two different types of server for the PKI and the trust anchors.

Hasen et al proposed a novel key management protocol for data communication between the utility server and customers' smart meters. The model is mainly between home smart meter and a security associate in the utility, which covers unicast and multicast communications [123]. The protocol improves the network overhead caused by security key management controlling packets, and at the same time it can prevent attacks like the aforementioned man-in-the-middle (MITM) attack. However, the authentication method between the SM and the appliances inside the HAN has not been addressed.

3.1 Key management in the Home area network (HAN) in a Smart grid

Literature specific to key management in Home area networks is discussed in this section. A HAN is a network connecting home devices such as smart TV and other smart appliances into a utility provider's smart meter system. In this way, energy demand could be better managed and load balancing will be more efficient. However, along with the economic

benefits it offers, the HAN is also exposed to potential attacks, and so key management is important to combat the potential threat.

The authors in [22] presented a mutual authentication scheme and key management protocol for a HAN. The scheme allocates a Trusted Agent (TA) for every HAN with the assumption that the communication topology is mesh. Mutual authentication is performed between the nodes and a TA using a public/private key pair technique that is based on identity-based cryptography. Their scheme has two layers consisting of public/private key pair and a symmetric key. However, using public and private keys between the nodes and a TA for the HAN node that have limited resources contributes to increase in delay overheads and the energy budget. In [23], the authors presented a session key exchange scheme in a HAN to protect against replay attacks between HAN nodes and a smart meter by the use of a freshness counter. The solution offers protection against replay attacks by using handshaking and self-generating timestamps.

In [21], the authors presented an authentication and key exchange protocol for secure password verification and session key generation over an insecure communication channel. The protocol uses Authenticated Key Exchange (AKE) and stores verifiers instead of the passwords. AKE uses a one-way hash function in computing the verifier and then stores the verifier in the server. Also compromising the server and finding the verifier is not enough since the password is still required. In SRP, the user enters a password and then a verifier is computed from the password along with a randomly generated password salt. The user name, salt and verifier are all stored in the server database. Finally, the client can now be authenticated to the server.

[27] proposed an efficient scheme that mutually authenticates a smart meter of a home area network (HAN) and an authentication server in the Smart Grid (Smart Grid) by utilising an initial password, by decreasing the number of steps in the secure remote password protocol from five to three and the number of exchanged packets from four to three. Furthermore, the author proposes an efficient key management protocol based on an enhanced identity-based cryptography for secure Smart Grid communications using the public key infrastructure. These proposed mechanisms are capable of preventing various attacks while reducing the management overhead. The improved efficiency for key management is realised by

periodically refreshing all public/private key pairs as well as any multicast keys in all the nodes using only one newly generated function broadcasted by the key generator entity.

3.2 Key management for NAN

In their paper, Seo et al [26] proposed an efficient encryption key management mechanism for end-to-end security in the AMI. By applying certificate-less public key cryptography (CL-PKC) for smart meter key management, the approach eliminates certificate management overhead at the utility. Moreover, this mechanism is practical, because it does not require any extra hardware for authentication of the smart meters. In this approach, the utility supports a PKI and has its own public key certificate, but the smart meters are not required to have certificates. Instead of using certificates for the smart meters, the concept of using CL-PKC to generate and manage the smart meter keys is utilised. Unlike the utility, which is a static entity, smart meters are dynamic entities, which often leave or join the AMI. If smart meters are required to have certificates, the utility has the burden of managing these certificates.

In CL-PKC, each user's complete private key is a combination of a partial private key generated by a Key Generation Centre (KGC) and an additional secret generated by the user. The advantage of this approach is that the KGC is not prone to the problem of key escrow, because the KGC is no longer responsible for the user's complete private key. Therefore, even if an attacker compromises the KGC, they cannot obtain the users' private keys. Moreover, the special structure of CL-PKC allows a user to encrypt a message without having to verify the public key of the message receiver via a public key certificate. By utilising CL-PKC key settings for smart meters, the authors eliminate the utility's overhead of certificate management.

[28] proposed protecting consumers' sensitive energy usage information by the use of a virtual ring architecture that can provide a privacy protection solution using symmetric or asymmetric encryptions of customers' requests belonging to the same group. They compared the efficiency of the proposed approach with two recently proposed Smart Grid privacy approaches, namely, one based on blind signature and other based on a homomorphic encryption solution. They showed that this approach maintains the customers' privacy while reducing the performance overhead of the cryptographic computations by more than a factor of 2 when compared with the scheme in [26]. It is further demonstrated

that the Smart Grid privacy solution is simple, scalable, cost-effective, and incurs minimal computational processing overheads. The proposed solution can support both symmetric and asymmetric encryption based authentication schemes. Furthermore, they demonstrated that the privacy solution is computationally more efficient and is more resilient to a wide range of attacks such as replay, known session key and man-in-the middle attacks.

3.3 Key management in the IoT

From the 1990s, large, multifunctional intelligent sensors were developed for various applications [4, 5]. This advancement continued with the fast development of sensors with radio, which became a trend in the field of sensor networks. Wireless sensor networks are designed to be low cost, have easy deployment and very low operation maintenance. Today, the application of wireless sensor networks is found in almost every endeavour, from hazardous environments such as earthquake and volcano monitoring [6] where it is dangerous for humans to take measurements, to medical sensors used in monitoring human health. Other applications include in the military, agriculture and the environment. Security has been a challenge to implement on sensor-based devices due to the constrained resource availability. Specifically, cryptographic implementations are limited by processing power, ability to generate random numbers and the ability to generate large primes. Key management experiences from WSN implementations are used to design the key management schemes for the smart grid applications.

LEAP [128] is a Key Management protocol. It aims to increase the protection of non-security protocols. It supports four kinds of keys to each node. One node is shared with the base station, which contains individual keys. Then pair-wise keys are shared with nearby nodes. Cluster keys are shared with a set of nearby nodes. Finally, one key, which is a group key, is shared with all nodes in the network. LEAP supports a protocol to authenticate local broadcast. Furthermore, it supports in-network processing for its key sharing. Therefore, it sufficiently protects the sensor networks from many security attacks. Finally, the LEAP scheme is effective for key creation and key updating while maintaining the necessity of small storage for each node.

3.4 Group-Based Key management

Group-Based Key management is implemented for multicast communication to offer a common and efficient management solution to the deployment of a symmetric group key to all nodes. A group key management protocol is central to the preservation of privacy in the multicast communication in a Smart Grid and it computes the symmetric group key and forwards the partial keys to all genuine multicast nodes. When a member joins or leaves the group, the group-based key management protocol should update the shared key so that only current group members understand it. This process is also known as rekeying, and is grouped into either individual rekey or periodical batch rekey. The former rekeys the group key for every group membership update such as joining /leaving. The latter processes the joining and leaving requests in a batch at the end of each rekey interval.

Harn proposed a Group Authentication Scheme (GAS), where the role of a group manager is responsible for registering all members of the group and issuing a distinct token to each member [10]. Subsequently, the members of the group authenticate and interact with each other without the need for the group manager's involvement. They propose a non-interactive basic t-secure m-user n-group authentication scheme ((t; m; n) GAS), where t is the threshold of the proposed scheme; m is the number of users participating, and n is the total number of group members. This scheme, based on Shamir's secret sharing [11], works for synchronous communications only. Therefore, they also propose an asynchronous (t; m; n) GAS, which can determine whether all users that participate in a group actually belong to that group [10]. The proposal in [10] is primarily for a many-to-many communication within a group (intra-group). It enables autonomous authentication within the group as well as detection of invalid members. The requirement for a Smart Grid scenario that we consider does not necessarily require a many-to-many characteristic. In addition, the limiting factor for the authentication scheme is the threshold t. There is no estimate of the scalability of t or the generic suitability of the scheme to resource-constrained devices. In the specific scenario we consider, the proposal in [10] is over-dimensioned.

Mahalle et al., present a Group Authentication scheme for IoT based on Threshold Cryptography-based Group Authentication (TCGA) [12]. They extend [10] to use Pallier Threshold Cryptography [13], using its properties, namely, homomorphic addition, indistinguishability, and self-binding. Primarily, they address the problem of different groups (applications) requiring communicating with each other. The authentication scheme has a pre-authentication phase where a group head does the key distribution and followed

by a group authentication phases where a secret session key is distributed. The group members rely on the group head to initiate all group communication. They demonstrate that their scheme performs better than [10]. However, the implementation is on WiFi based laptops and reflects a scaled performance of their scheme on IoT platforms. Our scenario does not require communication within the group. Group members do not need to communicate between themselves. The authentication is centrally done and the intermediate nodes verify that a downstream node is already authenticated. We also intend to use only symmetric encryption on the motes to minimize any processing delays at the intermediate nodes.

Yang et al., propose a generic framework for group authentication [14]. Their scenario considers password-based authentication in one go, for a user group. The focus is on reducing the time taken for authentication, like in [13], rather than authentication of a member, anonymously. The scheme is fairly close to our application scenario since the hierarchy of authentication (NOC – Gateway - Device) is quite similar (Server - group authenticator – end user). However, there is no evidence that it is applicable for low resource devices that we consider or the fact that the scheme will work (similar to the proposal in [9]) for multi-hop scenarios where an intermediate device requires to perform authenticated forwarding, as in our case.

Wang et al., present a group authentication and a group key distribution scheme for ad hoc networks [15]. They argue that conventional group authentication protocols cannot serve the requirements of ad hoc networks since there is no designated group leader and the fact that the number of nodes in the network are not known in advance and can change dynamically. Therefore, schemes such as those in [10, 13] cannot be deployed. The scheme proposed uses an identity based bilinear pairing. There are five distinct phases, which include a join and leave phases for the individual nodes. This is quite similar to the key management architecture schemes for SCADA networks discussed in [16]. Again, there is no specific mention of a multi-hop scenario requiring authenticated forwarding. Multi-hop scenarios are necessary for functional grouping as well as to build the radio path up to the NOC. Unlike in the case of WLANs used in [19], the radio range and the transmit power of the motes that we consider, are limited.

Nicanfar et al., address the authentication between a smart meter and the utility server termed as a Security Associate (SA). The SA is a dedicated server delegated to perform authentication by the central server at the NOC and is used for authentication by a group of SMs. They propose two separate schemes for authentication and key management, termed Smart GridAS and Smart GridKM, respectively. They propose a four-phase authentication approach, which has not been implemented and measured for performance [17]. They consider a mesh topology for SMs constituting the NAN, and use WiMax for interconnecting the smart meters. Their work is fairly close to the scenario we consider, from a topological perspective. Their functional requirement is similar to our requirement in that the authentication has to be done with a central entity. However, they delegate the central authentication autonomy to the SA. There are clear differences in the scenario we consider. Firstly, in our scenario such an intermediate node is merely a SM with the role of a gateway and with no autonomy. The risk of such delegation, we believe, is that the SA nodes are susceptible targets for attacks and can cause considerable impact in terms of the central server delegating the autonomy to a backup SA and the reachability of the SA from the end nodes. Secondly, They do not consider what we term as "authenticated forwarding". The traffic from the downstream nodes is not validated at the intermediate nodes. Thirdly, they use an asymmetric encryption method for privacy and a broadcast mechanism for key distribution. We believe, which key distribution via broadcast does reduce the communication overhead, multicast is a more secure option. Our scenario uses a single central entity for authentication and individually distributes the keys to each of the nodes.

Subir et al. [130] proposed a unified key management mechanism (UKMF) that can generate ciphering keys for multiple protocols of multiple communication layers from a single peer entity authentication procedure. The unified key management mechanism is suitable for Smart Grid use, especially for smart metering, where smart meters are assumed to be low-cost wireless devices for which repeated peer entity authentication attempts for each protocol can be included to increase system overhead. The proposed mechanism is flexible in that peer entity authentication can be treated as either network access authentication or application-level authentication. However, the mechanism has established that information discovery for bootstrap application ciphering is an important and as yet missing piece in realising the unified key management framework vision. This part needs further analysis.

Yee et al. [29] proposed a key management for a wide area measurement system in a smart grid. The scheme targeted a concrete set of security objectives derived from NIST's security impact-level ratings. For multicasting, they identified multicast authentication as the primary challenge. In the scheme, they used TV-HORS for the multicasting authentication.

A lightweight and distributed group authentication scheme for ad-hoc network devices is presented in [09]; however, performance analysis of the proposed scheme is not discussed in this work. In particular, they propose [12] a secure and reliable innetwork collaborative communication scheme to provide a secure and reliable AMI in a Smart Grid with smart meters interconnected through a multi-hop wireless network. Here, the AMI system approach can provide trusted services, data privacy and reliability by mutual authentications whenever a new smart meter starts and connects to the Smart Grid AMI network. Data integrity and confidentiality are accomplished through message authentication and encryption services respectively using the corresponding keys established in the mutual authentications. A transmission method is proposed to ease the data collection and management message delivery between smart meters and a local collector for AMI communications. The performance of the proposed security scheme is verified through simulations, and results show that the proposed method has a better end-to-end delay and packet losses compared with a basic security method, and the proposed method can provide secure and reliable communications for AMIs in Smart Grid systems.

LiSH+ is a group key management scheme characterised by developing a secure self-healing mechanism with t-revocation and collusion resistance capability. For the key management, a dual direction hash chain is employed to guarantee both the backward secrecy and forward secrecy of the group key. The self-healing mechanism was implemented to ensure availability of group members in case of device failure and prevent the collusive users from exploiting the group key in the proposed scheme. When a node is compromised, the compromised users could be revoked from the group dynamically by the broadcasting message [29].

In [12], the Tree-based Group Diffie-Hellman (TGDH), every group member contributes to the group key generation. It has the advantage of fault-tolerance. However, for group membership changes, it lacks scalability in terms of computational cost. TGDH has some other drawbacks. Every group member performs the expensive Diffie-Hellman key

exchange with times exponentiation operations for every group membership update where n is the group size. Secondly, every sponsor should sign and forward a large number of rekeying multicast messages to update a group key. This results in expensive communication overhead and computational costs. Table 5 shows other Benefits and Limitation of Group Key Management Schemes.

In [12], the Tree-based Group Diffie-Hellman (TGDH), every group member contributes to the group key generation. It has the advantage of fault-tolerance. However, for group membership changes, it lacks scalability in terms of computational cost. TGDH has some other drawbacks. Every group member performs the expensive Diffie-Hellman key exchange with times exponentiation operations for every group membership update where n is the group size. Secondly, every sponsor should sign and forward a large number of rekeying multicast messages to update a group key. This results in expensive communication overhead and computational costs.

A GSA [30] is a scheme that aggregates in three categories of SAs, namely: Categories 1 and 2, which take place between the KD and a member, and Category 3, which takes place among members. The first category (SA-1) is for bidirectional unicast communication between the KD and a group member. It is initiated by a member, to "pull" GSA information, including the SA, keys and SA-3, from the KD, to either join the group, or re-join after getting disconnected. Hence, it is also referred to as the pull SA or registration SA. Only the KD and the corresponding member know this SA.

The second category (SA-2) is required for the unidirectional multicast transmission of key management or control messages from the KD to every group member. Since the control messages include the update or replacement of SA-3, it can be said that SA-2 is used to update SA-3. SA-2 is used by the KD to "push" rekeying messages and the SA updates to the members. Hence, it is also known as the push SA or rekeying SA. The KD and all members know this SA. The third category (SA-3) is required for the unidirectional multicast transmission from member sender to member receivers. Since it is used to secure the data traffic, it is also referred to as the data security SA. The KD and all members of the group know this SA.

3.5 Authentication and Key Management for AMI

The authors in [45] proposed key management for an AMI system which is built based on the key graph. They define the secure exchange between a Management Side (MS) (e.g., utility) and appliance or devices (SX) at the customer's premises (i.e., smart meters). There are three different key management processes proposed in KMF to deal with the hybrid transmission modes: the contents of key management for unicast, broadcast, and multicast modes. Relatively simple cryptographic algorithms are chosen for key generation and refreshing policies due to the storage and computation constraints of SMs. The KMF has been defined as KMF = (U, K, R) where U is nodes in the AMI system; K denotes keys of nodes, gk is group of keys and R is the binary relation between U and K; therefore, user u knows key k if and only if (u, k) is in R.

The proposed KMS is closely integrated and supports the unicast, broadcast, and multicast. The distribution of the keys and related data will not affect the normal network traffic in an AMI system. Moreover, the proposed scheme can deal with normal security attacks. Furthermore, forward and backward security is dealt with in the proposed scheme. The authors of [45] apply the hierarchy of keys or a rooted tree; therefore, every user is given a subset of keys which contains its individual key, a key for the entire group for group communications, and a key for its subgroup. However, the proposed scheme requires updating the key redistribution for each joining or leaving of the session. Furthermore, the network topology has not been taken into account, which will cause some unwanted nodes in a group to receive rekey messages.

The authors in [129] propose a lightweight key distribution and management scheme tailored to AMI. Specifically, a group ID-based mechanism is proposed to establish the keys for a large amount of entities with a small overhead. They propose a group identifier-based mechanism to establish the symmetric keys, in which a gateway shares a different secret key with every single smart meter and the keys are generated based on the D-H algorithm, however, without authenticating the smart meters during the key generation phase. Moreover, they add a verification step to the pairwise key construction. Since the proposed scheme requires every single meter to have a symmetric key, it is not scalable for smart grids. Moreover, use of symmetric keys is vulnerable to MITM attack.

Subir et al., in [130], proposed a unified key management mechanism (UKMF) that can generate ciphering keys for multiple protocols of multiple communication layers from a

single peer entity authentication procedure. The unified key management mechanism is suitable for Smart Grid use cases, especially for smart metering, where smart meters are assumed to be low-cost wireless devices for which repeated peer entity authentication attempts for each protocol can be contributed to increased system overhead. The proposed mechanism is flexible in that peer entity authentication can be treated as either network access authentication or application-level authentication. The authors present the details on an EAP-based unified key management mechanism and show that it is important to consider re-key efficiency of the ciphering keys bootstrapped from EMSK. The authors also discuss the test environment where the proposed unified key management mechanism is integrated with an ANSI C12.22-based smart metering application, and where PANA is used for both network access authentication and application-level authentication. The authors present preliminary implementation results achieved using a commercial microprocessor, typical of those deployed in smart meters, and using a general-purpose computer.

The key management mechanism defines a unified key management function (UKMF) across multiple protocols within the same communication layer or across different communication layers. The conceptual model of the author's framework is applicable to any protocol requiring a cryptographic operation at any communication layer. Ideally, there should be only one UKMF across all protocols with ciphering mechanisms. In the partially unified model, mapping between a protocol and a UKMF or DKMF could be arbitrary. In both the fully and partially unified models, a protocol that uses a UKMF may also have a DKMF, where the latter may be managed by the UKMF. For example, some application protocols may be DKMF based on its own application-specific key management protocol, while the UKMF may generate a symmetric key to be used by the application-specific key management protocol to bind the UKMF with the DKMF. In both models, the initial peer entity authentication between a pair of UKMFs can be based on either network access authentication or application-level authentication. However, the mechanism has established that information discovery for bootstrap application ciphering is an important and as yet missing piece required to realise the unified key management framework vision.

The authors introduce a new scalable and efficient key management scheme called Efficient and Scalable Multi-group Key Management for secure data communications in an Advanced Metering Infrastructure (eSKAMI). It is based on a Multi-group Key graph structure that supports the management of multiple Demand Response (DR) projects simultaneously for

each customer. The authors demonstrate the new structure scales to large Smart Grids with dynamic Demand Response project membership while meeting Smart Meter constraints in terms of memory and bandwidth capacities. Figure 2 shows an example of the key graph with the MDMS providing four DR projects. Some users subscribe to only one of the DR projects while other users may subscribe to multiple DR projects simultaneously.

Nicanfar et al. propose using a CA as a Security Associate (SA) server in the utility network [123]. Their system has two secret values, with the SA keeping the first secret (the main part) and smart meters keeping the second secret value, which is only a counter generated by the SA and it is part of the system's secret values managed by the SA. However, the authors do not consider the security issues when appliances are installed in the SM perimeter and focus instead on the security between the SM and the utility.

In [31], the authors present a lightweight key management scheme with a novel key refreshment policy that decreases the network overhead, which makes symmetric keys to secure communications between SMs and MS using elliptic curve cryptography (ECC) parameters and simple cryptographic algorithms like hash functions. Unicast messages are transmitted from MS to SM and reverse. To provide the confidentiality and integrity of the message sessions, the key is refreshed at every session. Figure 3-4 shows the scheme with the following process:

- Sender generates the session key and uses it (SM or MS)
- End system forms following packet, and sends it through communication channels
- Message verification and decryption at receiving side

For broadcast, messages are transmitted from MS to SMs. Similar to unicast messages, to ensure confidentiality and integrity; session keys should be refreshed before every broadcast session.

- Sender generates the session key and uses it (MS to SMs)
- MS forms the below packet, and broadcast

Broustis et al., term the first scenario as reverse single sign-on and succinctly describe a framework for group authentication which is applicable for mobile telecom networks and extendible to the M2M context, which is relevant to our discussion [9]. They introduce a

gateway entity to coordinate/represent the group and this entity performs the required upstream authentication. The group authentication is based on a group challenge sent by the gateway to all devices. The devices individually respond to the gateway with their credentials. In the absence of the gateway, the upstream authentication server does the authentication and the overall saving in communication overhead remains one-sided (from the authentication server to the device group) [9]. The proposal in [9] is similar to our proposal in terms of having a gateway as an intermediary. In the scenario we consider, each node in the network authenticates with a central entity, the network operations centre (NOC). This includes all intermediate nodes (group leaders) that provide a path to the end nodes to reach the NOC. Operationally, each group leader has no autonomy to authenticate a group member, but it has sufficient information to validate that a group member attempting to relay packets through it has indeed been authenticated, centrally. There could be a hierarchy of groups, if necessary functionally to reach the NOC, resulting in a multi-hop path from the end device to the NOC [9] does not discuss such an authentication requirement with multi-hop paths.

In summary, the key features that we intend to utilize for authentication and key management are a relatively simple authentication scheme for a group of devices, an activity monitor that characterizes the traffic from the devices as well as a means of authenticated forwarding. We have clarified what we mean by group authentication in our context and defined each of the features we require for our scheme and compare the availability of these features with the schemes discussed so far and establish the security requirements of our scheme. The

Table 3-2: Gap in existing solutions for the HAN

Features	**Security Schemes for HAN**				
	Hasen et al	**Kim et al**	**Tizazu, et al**	**Zhao et al.,**	**Our Proposal**
Topology - S/M/T	M	Binary tree	M	S	Tree
Multi-hop paths	No	No	Yes	No	Yes, if required

Validated Forwarding at intermediate nodes	Yes	No	Yes	No	Yes
Symmetric Cryptography	No	Yes	Yes	No	Yes
Resilient to NC attack	No	No	No	No	Yes
Resilient to replay attack	No	Yes	Yes	Yes	Yes
Resilient to Sybil attack	Yes	Yes	Yes	Yes	Yes
Authentication at the Group Controller	No	No	No	No	Yes
Specifically designed for HAN	No	No	Yes	No	Yes
Nodes are not time synchronized	No	Yes	Yes	No	Yes
Scalability	N/A	No	N/A	No	Yes

requirements are drawn for the Smart Grid model detailed in section 3. These requirements are in addition to the basic security requirements, namely, confidentiality, integrity, non-repudiation and forward/backward secrecy.

3.6 Comparing schemes available for HAN and NAN

Table 3-3: Gaps in existing literature for NAN

Features	Schemes						
	Broustis et al.	Harn	Wang et al	Yang et al.,	Nicanfar et al.,	Subir et al.,	Our proposal
Topology - S/M	M	N/A	N/A	S	M	N/A	Yes
Multi-hop paths	Yes	Yes	Yes	No	Yes	N/A	Yes
Validated Forwarding at intermediate nodes	Yes	Yes	Yes	No	N/A	No	Yes
Symmetric Crypto	Yes	No	No	No	No	EAS	Yes
Resilient to NC attack	No	No	No	Yes	No	Yes	Yes
Resilient to replay attack	No	Yes	Yes	Yes	Yes	Yes	Yes
Resilient to Sybil attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Centralized Authentication at NOC	No	No	No	No	Yes	Yes	Yes
Specifically designed for NAN	No	No	No	No	Yes	Yes	Yes
Nodes are not time synchronized	No	Yes	Yes	No	Yes	No	Yes
Scalability	N/A	N/A	N/A	N/A	N/A	N/A	Yes

Over the previous chapter, we have looked at the elements of the HAN and NAN, their communication needs, the potential security threats and the mitigation features required. In this chapter, we have seen the various security schemes available in literature and how they address the security requirements in the scenarios they consider. In the HAN and NAN scenarios that we consider, we compare the existing solutions and locate the gaps in the existing solutions when applied to our scenarios. We begin with a comparison of the requirements for the HAN scenario. Table 3-2 compares the available HAN solutions that are closes to the scenario that we intend to propose a solution. Table 3-3 compares the available NAN solutions that are close to the scenario that we consider proposing a solution.

The tables 3-2 and 3-3 list a common set of features that are considered for both the HAN and NAN. All comparisons in literature are made against these features and the gaps are identified. We pick features that have three or more “No”s listed against them and identify them as gaps to be addressed. We now briefly highlight three specific features that are important to be considered from the design perspective.

1. Node capture attack is a harmful attack where a malicious user is able to steal information that is stored in nodes such as cryptographic keys and ID. Based on our literature review, we have discovered that existing solution approaches [47, 49,151,150] on node capture attack over smart grid network are still lacking in

providing effective solutions that mitigate such attacks and are vulnerable to them. Therefore, the proposed solution must be resilient to node capture attack.

2. In addition, in a large-scale environment such as the smart grid, network scalability is crucial design parameter for a secure scheme. An increase in the smart gird nodes size should not affect the overall performance. Schemes proposed in [44, 133] apply public/private keys and session keys. However, using public and private key between smart grid's nodes and home appliances with limited resources will not be efficient and it's possible that network might become worse as it scales. This is called negative scalability. Such as could cause significant delays. In addition, the task of distributing key pairs, revoking them and validating them are overheads that contribute to delays. Scalability is an essential design parameter to be considered in the design of our schemes.
3. A topology independent for interconnectivity is necessary requirement in design security scheme for a large network environment such as the smart grid. Different sections of the NAN or a HAN could have different topologies for reasons of providing overlapping coverage. Mesh topology is more flexible as it can allow smart nodes to choose between multiple routes to transmit/receive data to the target location or group gateway. Partial mesh or cluster-tree topologies are often practical. Schemes [20,106] only consider star or tree topology.

With these gaps specifically identified, we proceed to the next step of designing the security schemes for the HAN and NAN.

3.7 Summary

This chapter has presented the literature review of key management in Smart Grids – HAN and NAN, IOT and WSN and AMI. The authors proposed different key management protocols to secure wireless mesh network and Smart Grid communications. Smart Grid networks generally consist of multiple components and applications, which add to the difficulty in implementing key management. Key management is important for wireless mesh such as a Smart Grid network due to the potential threats to it. Key management includes initialisation of keys, key generation, key distribution, key updates and key storage with the goal of key management for node operations and prevention of attacks that could comprise a node. Wireless mesh networks generally comprise a number of low-cost,

resource-constrained nodes. These nodes tend to have low memory, computation, communication and energy capabilities. Key management consists of four principal areas: key deployment or pre-distribution, key establishment, node or member addition and node or member removal. Its functional requirements include: confidentiality, which means that the content of the information flowing in a wireless sensor network must be protected from disclosure to unauthorised parties; authentication, which means that the parties who are able to access the shared information should be identified and authenticated; data integrity, which means that data should not be changed between transmissions due to the environment or malicious activities; robustness is another requirement, which deals with node compromise and attack; overhead cost, which includes the need to keep the computation, communication and memory

Chapter Four: Key Management Scheme for Communication Layer in the Smart Grid (KMS-CL-SG)

4. Introduction

In the previous chapter we provided a wide literature review of the areas of key management and authentication of smart grid (Smart Grid) communication including HAN, NAN, SCADA and AMI. We have highlighted missing requirements that need to be addressed in the security scheme. This chapter describes the scheme of our key management solution for a Smart Grid's communication layer. Since a Smart Grid is a meta-system, it is not practical to design a single key management scheme for all systems, actors and segments in the smart grid, as the security requirements of various subsystems in the smart grid vary. Therefore, we have proposed a key management scheme for HAN and NAN.

4.1 The Key Management Scheme for the Smart Grid Home Area Network (KM-HAN)

In this section, we describe the security scheme that addresses the secure data transfers between the devices in the smart home up to the power company's Network Operations Center (NOC) through the smart meter installed at the smart home. We start by illustrating the topology of the devices in the smart home, the smart meter and the power company's NOC. This is followed by listing out the assumptions with regard to the devices, their mode of communication and a few configuration options implemented across this topology.

This section describes the HAN in smart grid system architecture, describes two classification groups and communication scenario, and threat model.

4.1.1 Network Architecture

In general, a HAN connects the smart devices across the home with a smart meter. The HAN components can communicate using technologies such as Zigbee, wired or wireless Ethernet, or Bluetooth. There are two ways to interface the home depending on the countries where it is implemented. One way is through smart meter as the interface to network

operation centre and other actors. The other way is to interface with WAN and NAN by using a separate control and aggregation node [131].

The HAN components are divided into two groups based on [132]. Group one comprises appliances that require two-way communications such as smart electric vehicle, air conditioning (AC) and solar panel. Group two comprises home appliances that require one-way communication such as smart TV, lighting system and charger. An example of group one is a solar panel that requires two way communications to provide unneeded power to utility company also, AC is expected to receive a signal from utility provider to reduce energy intensity during off-peak hours. However, group two members need only one-way communication to send the electricity consumption data. The devices in Group one have higher resources capabilities compared to those in Group two.

4.1.2 Notations and Assumptions

Before we begin to describe our scheme, we explain the notations and assumptions used in this chapter.

Table 4-1: Notations used to represent the scheme

D	Smart device
i	The number of smart devices inside home, i= [1 ... N]
H	Unique group of smart devices inside home, which have high resources capacities devices and the data exchange, is bidirectional.
L	Unique group of smart devices inside home, which have low resources capacities devices and the data exchange, is one way.
$D_{H,i}$	Unique identity for a smart device in the group H.
$D_{L,i}$	Unique identity for a smart device in the group L.
G_{D_H}	A home group controller node in the group H.
G_{D_L}	A home group controller node in the group L.
$K_{G_{D_H}.D_{H,i}}$	A unique symmetric key shared between the group controller G_{D_H} and the smart devices $D_{H,i}$ in the group H generated by using the master key MKG_{D_H} and devices $D_{H,i}$
MKG_{D_H}	A symmetric master key for group controller G_{D_j}
$SM_{n,g}$	A unique ID of a smart meter

$K_{sm,D_{H,i}}$	A unique symmetric key shared between smart meter $SM_{n,g}$ and the smart devices $D_{H,i}$.
$K_{sm,D_{L,i}}$	A unique symmetric key shared between smart meter $SM_{n,g}$ and the smart devices$D_{L,i}$.
$K_{sm,G_{D_H}}$	A unique symmetric key shared between smart meter $SM_{n,g}$ and the home group controller node in the group H
$K_{sm,G_{D_L}}$	A unique symmetric key shared between smart meter $SM_{n,g}$ and the home group controller node in the group L
$K_{G_{D_L}.D_{L,i}}$	A unique symmetric key shared between the group controller G_{D_L} and the smart devices $D_{L,i}$ in the L group
$TS_{D_{H,i}}$	A time stamp of node $D_{H,i}$
$TS_{D_{L,i}}$	A time stamp of node $D_{L,i}$

The following assumptions are made in the proposed scheme

1. We do not consider device to device $D_{H,i}$ to $D_{H,i}$ or $D_{L,i}$ to $D_{L,i}$ communication
2. The smart device$D_{H,i}$, $D_{L,i}$ and group controller use unicast communication.
3. The home group controllers, G_{D_H} and $G_{D_L}$are trusted devices.
4. All smart meters $SM_{n,g}$ are registered on the group controllers G_{D_H} and G_{D_L}.
5. The smart devices $D_{H,i}$, $D_{L,i}$ are registered with the group controller
6. The HAN interconnected as a tree with the devices as leaf nodes.
7. An adversary could eavesdrop on all traffic or replay messages.
8. Smart meter $SM_{n,g}$ is tamper-resistant.
9. Time stamps are used for data freshness checking. The time is not synchronized across the devices on the HAN, but the time stamps are verified to ensure they are incremental and periodic. This requires that the devices that verify the data for authentication and/or freshness store the time stamp of the previously received data.

4.1.3 Proposal Overview

Group Key Management scheme for HAN has a set of features that address secure data transfers across the smart home. To achieve confidentiality between end-to-end communications, symmetric-key cryptography is employed where a unique key is assigned to each smart device. Data are collected from smart devices in an encrypted form and sent to smart meter. The scheme manages the key distribution and generation across nodes of the

network and exchanges these keys securely when necessary. Consequently, the secure data transfers are consistent and resilient to changes in the network.

4.1.4 A Group Key Management Scheme for HAN

The operation of the scheme requires that the devices participating in the scheme be configured before deployment. This is termed as the pre-deployment phase. The activities in the pre-deployment phase are first illustrated. Then, it is followed by an explanation of the communication and authentication between the nodes within a group and their group controller and the group controllers and the smart meter.

4.1.5 Pre-deployment Phase

The pre-deployment phase concerns the security configuration of the nodes of the HAN, prior to their functioning on the network. First, we present the steps for the pre-deployment of the two HAN groups comprising of the high resource devices $D_{i,H}$ and the low resource devices $D_{i,L}$ as well as their respective group controllers G_{D_H} , G_{D_L} and the smart meter $SM_{n,g}$.

- Assign unique ID to each smart device $D_{i,H}$ and $D_{i,L}$
- Assign a unique master key MKG_{D_H} to group controllerG_{D_H}. This master key is used to generate a shared key between G_{D_H} and its devices
- Yield and store a unique key $K_{G_{D_H},D_{H,i}}$ by using the master key $MKG_{D_H}$and node ID $D_{H,i}$ on $D_{H,i}$
- Assign a unique key $K_{G_{D_L}.D_{L,i}}$ to group controller $G_{D_L}$and share it with $D_{L,i}$.
- Assign unique key $K_{sm,D_{H,i}}$ to every smart devices $D_{H,i}$ shared between $SM_{n,g}$ and $D_{H,i}$.
- Assign unique key $K_{sm,D_{L,i}}$ to every smart devices $D_{L,i}$ shared between $SM_{n,g}$ and$D_{L,i}$.

4.1.6 The High Source Devices *H* Group

Each device $D_{H,i}$ that is connected to the smart meter $SM_{n,g}$ will require storing unique key $K_{sm,D_{H,i}}$ shared with smart meter$SM_{n,g}$. The home group controller G_{D_H} stores the its master key MKG_{D_H} and symmetric key $K_{sm,G_{D_H}}$

Pre-deployment for groups *H* and *L* -

Devices: Group controller and devices which are group members

Outcome: Assign unique IDs to each device, organize them into two groups, assign a group controller to each group, a smart meter to the groups and initialize the devices with the shared keys.

Step 1: Formation of the groups H **and** L

Identify the group controllers G_{D_H} **and** G_{D_L}

Formation of the group H with smart devices $D_{H,i}$

Assign a unique ID for each smart device $D_{H,i}$

Formation of the smart meter $SM_{n,g}$

Assign a unique ID for each smart devises $SM_{n,g}$

Step 2: Assign master group key and unique key for each device in the Group H

If node= G_{D_H}

$K_{sm,G_{D_H}}$ ← // assign group controller unique key

$K_{sm,D_{H,i}}$ ← // assign $D_{H,i}$ unique key

End if

Figure 4-1: Pre-deployment steps for the HAN

4.1.7 The Low Sources Devices - *L* Group

Each device $D_{L,i}$ that communicates with the smart meter $SM_{n,g}$ will store two unique keys $K_{sm,D_{L,i}}$ shared with smart meter $SM_{n,g}$ and $K_{G_{D_L},D_{L,i}}$ shared with its group controller. G_{D_L} stores two keys, a symmetric key $K_{sm,G_{D_L}}$ which is used to encrypt data for secure communication between home group and smart meters and $K_{G_{D_L},D_{L,i}}$ which is used for authenticating the device at the group controller G_{D_L}.

4.1.8 Communication phase

In this section, we explain the communication (data transfers not relating to key management) phase for home area network.

4.1.9 The High Source Devices *H* Group

The smart devices $D_{H,i}$ exchange data bi-directionally with the smart meter. $D_{H,i}$ encrypts its data and time stamp sent to the smart meter encrypted using the shared symmetric key $K_{sm,D_{H,i}}$ as $E_{K_{sm,D_{H,i}}}(Data, TS_{D_{H,i}})$. $D_{H,i}$, then uses $K_{G_{D_H}.D_{H,i}}$ to generate a message authentication code (MAC), $MAC_{.D_{H,i}}$ that will be verified by G_{D_H} to authenticate $D_{H,i}$. The encrypted data destined for the smart meter and the MAC are sent to G_{D_H} as $E_{K_{sm,D_{H,i}}}(Data, TS_{D_{H,i}}), MAC_{.D_{H,i}})$. After validating the MAC value, G_{D_H} -encrypts the encrypted data destined to the smart meter, using the symmetric key $K_{sm,G_{D_H}}$ as $E_{K_{sm,G_{D_H}}}(E_{K_{sm,D_{H,i}}}(Data, TS_{D_{H,i}}))$. Upon receiving this data, $SM_{n,g}$ decrypts the message it receives from the home group controller node G_{D_H}, using the symmetric key $K_{sm,G_{D_H}}$ and further decrypts the message to retrieve the data and time stamp sent by $D_{H,i}$. The data from the $D_{H,i}$ will be available in an unencrypted form in the memory of the smart meter $SM_{n,g}$. This is of concern from a security perspective.

4.1.10 The *L* Group

These devices communicate one way; they send data to the smart meter. $D_{L,i}$ uses steps similar to the other group to send data to the smart meter. $D_{L,i}$ encrypts its data as $E_{K_{sm,D_{L,i}}}(Data, TS_{D_{L,i}})$. The encypted data destined for the smart meter is encrypted again, with the time stamp, using the key $K_{G_{D_L}.D_{L,i}}$ as $E_{K_{G_{D_L}.D_{L,i}}}(E_{K_{sm,D_{L,i}}}(Data, TS_{D_{L,i}}), TS_{D_{L,i}})$. Upon receiving this, G_{D_L}validates the source by decrypting the data and verifying the time stamp. It then encrypts the data destined for the smart meter using the shared key between $G_{D_L}$and $SM_{n,g}$, $K_{sm,G_{D_H}}$as $E_{K_{sm,G_{D_L}}}(E_{K_{sm,D_{L,i}}}(Data, TS_{D_{L,i}}))$. The smart meter retrieves the original data by decrypting the data using $K_{G_{D_L}.D_{L,i}}$ and $K_{sm,G_{D_H}}$. At $G_{D_L}$and $SM_{n,g}$, the source of the data is considered successfully authenticated if the data is successfully decrypted using the shared key of the source. The time stamps are used to verify the data freshness.

4.1.11 Security Analysis

The proposed scheme is evaluated against the following security characteristics - resilience against forward and backward secrecy, node capture, resilience against replication attacks, and secure data aggregation.

- Forward and backward secrecy

  In a devices group with active smart devices $D_{H,i}$ $D_{L,i}$ where a node may join or leave during the lifetime of the group, two security considerations arise.

  Backward secrecy: A new smart device $D_{H,i}$ $D_{L,i}$ must not have permission to access any data that is communicated before it joins the session.

  Forward secrecy: In a case where a smart device $D_{H,i}$ $D_{L,i}$ leaves the group, it must not have permission to access any future data.

- Resilience against replication attacks

  An attacker could replay old messages that have been obtained from previous communication. However, in our scheme time stamps are sent along with the data and each of the receiving entities verify them against the previously received time stamps, which are stored on the devices. The time stamp is used as a session token, which is expected by the receiver with a reasonable tolerance in value when checked against the periodicity of data expected. Each of $D_{H,i}$ and $D_{L,i}$ encrypts a time stamp with the data, which is sent from the appliances to the smart meter$SM_{n,g}$.

- Resilience against Sybil attacks

  On Sybil attack, a malicious node introduces multiple fake identities to group controller node G_{D_H} and G_{D_L} in the HAN for illegitimate purpose. Our scheme provides an authentication to confirm that one node cannot pretend to be other, for example when a node $D_{H,i}$ sends data to group controllerG_{D_H}, it must compute a MAC on the data sent. The MAC is computed using the shared key between $D_{H,i}$ and G_{D_H} no adversary node can pretend to be the node X. Furthermore, each node in

HAN has unique ID and its keys bound to its ID. If the compromised node uses a different ID from the stored ID in$SM_{n,g}$, it doesn't hold the valid keys related with fake ID.

- Resistance to man-in-the-middle (MITM) attack

  Messages exchanged between smart meters $SM_{n,g}$ and $D_{H,i}$ are crucial in a HAN. The data generated by the devices are encrypted using the key shared with the smart meter. It is forwarded to the smart meter via the group controllers without being decrypted at the group controllers. An attacker will therefore not have access to the data on the network in a direct form, except at the two end points. In addition to the encryption, the group controller authenticates the node either by verifying the MAC (Group H) or by being able to decrypt the contents and verify the time stamp (Group L), both of which are encrypted. So, an attacker will require guess two keys to be able to access the data sent by an end device. Thus the confidentiality of the data is achieved.

- Scalability

  An increase in the HAN size should not affect the overall performance. We use group key management mechanisms to address the scalability of the HAN. The HAN is divided into different groups of homogenous devices (such as H and L) and corresponding group controllers such as (G_{D_H} andG_{D_L}) with distributed management tasks, to make the HAN scalable and efficient. The scheme uses only symmetric keys unlike [44, 133] in which they apply public/private keys management and session keys.

4.2 The Key Management Scheme for the Smart Grid Neighbourhood Area Network (NAN) (KM-NAN)

4.2.1 The Smart Grid Network Model

In this section, we present the Smart Grid network model considered for the discussion and detail the requirements for its secure operation. We also explain the potential security threats we consider for a case study to test the proposed solution. The Smart Grid network model

considered for our discussion, shown in Figure. 4-2, which comprises three network segments:

- Home Area Network (HAN): one Smart Meter (SM) and N Smart Devices (SDs). This group of devices is interconnected in a Star topology with SM as the star point.

- Neighborhood Area Network (NAN): mesh network (not necessary full mesh) of M SMs. SMs are divided into G groups. Group g (g = 1...G) has Mg SMs. Hence the following equation is considered:

$$M = \sum_{g=1}^{G} Mg \quad (1)$$

  One SM of each group is selected as Group Controller (GC). The GC is hereafter termed as the Gateway node, GW.

- Wide Area Network (WAN): Network (e.g., Internet) that connects GCs to the Network Operations Centre (NOC).

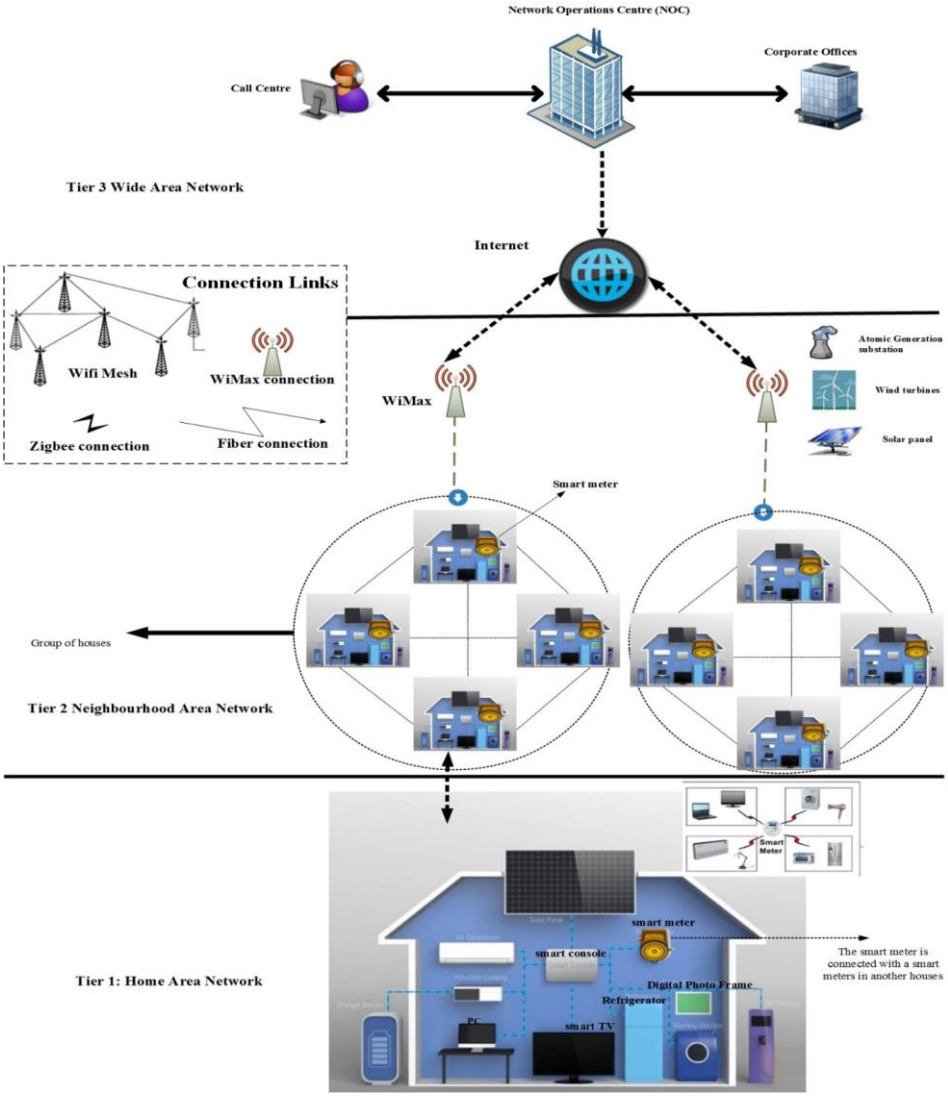

Figure 4-2 Smart Grid Network Model

The data generating elements are part of the HAN. This data traverses the entire network to reach the NOC. The smart meters, which are a part of the NAN, generate data as well as receive data from the NOC. Therefore traffic to the NAN elements is two-way. Data may or may not be forwarded into the HAN by the smart meters, depending upon the deployment requirement.

4.2.2 Threat Model and Assumptions

There are two basic types of threats that need to be countered - attacks that originate due to malicious users eavesdropping to monitor the wireless communications between the nodes

in the network and attacks that originate due to the capture of a node physically or causing it to fail.

Eavesdropping: Unauthorized users may try to eavesdrop on exchanged data and control messages within HAN and NAN. The eavesdroppers can use the information exchanged and the exchange patterns to launch man-in-the-middle (MITM) attacks or replay attacks to impersonate a node. Therefore, all nodes should be authenticated and all messages should be encrypted. The keys used for privacy should not be easily guessable.

Node Capture: Physical node captures or forced failure of nodes such as in a DoS attack amount to a node capture attack. In such an event, if the keys on the node are captured, the attacker should not be able to gain access to the network. The solution should minimize the impact of such attack on the remaining nodes and ensure the rest of the network functions normally. Authentication Scheme for NAN

In a neighborhood area network, authentication is required to secure routing in the network. Smart meters have to be registered with the group controller to obtain permission to communicate in the network. For our authentication process, we make the following assumptions:

a. Smart meters are grouped together based on a policy and are aware of the group members. The events and functionalities of the policy are not in the scope of this paper. This work does not address the policy on which smart meters groups are constituted.

b. Every smart meter in a group has a unique identity, which is a serial number and each group has a unique group identity, which are used in the authentication process. All network devices involved in the group authentication process know these details.

c. The link layer between the smart meters and gateway are protected at the link layer. Which makes communication encrypted at the link layer.

d. Every smart meter in a group maintains a wireless connection with its gateway and the network topology between the home smart meter and the gateway node is a tree. The topology between the gateway and the utility

could be a mesh. They form a cluster-tree topology between the SM and the gateway.

e. The smart meters have pre-distributed shared symmetric keys, which are used for initiating the authentication process and keys during authentication.

f. Symmetric cryptography yields a better cryptographic strength for a given key length compared to asymmetric cryptography. The resulting data length is close to the size of the input.

g. Smart meters cooperate with one another to forward packets on multi-hop paths to the NOC. A routing protocol to handle the mesh topology is active and provides the shortest route from a given end device to the GW, within the group.

h. GW nodes have sufficient power (more than the end devices) to be able to perform the forwarding from the group to the NOC and vice versa

i. In the event of the failure of a gateway node, all nodes in the group will be unable to access the NOC, until the GW is reinstated/active. There is no fallback node that will take on the role of a gateway. The failure rates of the GW are low.

j. The groups and the group gateways are pre-identified and formed. These formations are not ad hoc and therefore there is no need for a node to play the role of a gateway

k. The nodes on the network are not time synchronized.

l. The value of the clock ticks of a node cannot be retrieved to set the same clock value on another node. Such an operation is possible only with a reset of the node, which essentially implies that the clock tick value is lost since the clock is reset. It can be argued that such is the exact function of a time protocol such as ntp, but sufficient care is taken to ensure that this value is not accessed by any network function.

m. The NOC provides a central authentication service. It comprises a sufficiently large server with a fail-over configuration and able to maintain the state of all the devices on the network. Given the nature of the service requirement of the smart meters in the smart grid, all authentication attempts, except the one at startup upon installation must be approved before the NOC sends an authentication response to the node requesting authentication.

n. The NOC maintains a history of the meta-data (originator-ID, timestamp, group-ID) over a sufficiently long period to derive statistics such as message arrival epochs, message arrival times, inter-message times, message size and activity profiles so that it knows when it can expect the next packet from a specific ID. Such a history is essential to detect malicious attack traffic since our scheme does not require the devices on the network to be time synchronized.

4.2.3 Notations

Having stated the assumptions made, we proceed with detailing the security scheme for the NAN scenario. The following subsection begins with a listing of the notations used to detail the security scheme. This is followed by the details of the authentication process.

The scheme addresses two cases - smart meter in Multi-Hop (Mesh) and smart meters in star topology.

Table 4-2: Notations used for KMS-NAN

4.2.4 Key management and authentication of Group Gateway GW

G	Unique group number
$SM_{n,g}$	Smart meter ID
GW_g	A gateway for a group of smart meters to the NOC
MK_{NOC}	Master Key for NOC
MK_{GW}	Master key for the group Gateway
$K_{sm,noc}$	Symmetric key generated by $K_{sm,Noc}$ = F (MK_{NOC}||SM_{ng}), and shared with NOC, and SM_{ng}.
$K_{GW,SM}$	Symmetric key generated by GW_g, and shared with GW_g, and SM_{ng}.
$Proxy\ SM_{n,g}$	Existing smart meter for authenticating a new smart meter
$K_{SM,SM}$	Symmetric key shared between $Proxy\ SM_{ng}$, and SM_{ng}
K_{GW_g}	Symmetric key shared with NOC, and GW
AV_i	Authentication value inside the group where $AV_i = F\ (R\|\|MK_{GW})$
R	Random number generated by GW_g to produce AV_i

We now describe the method that is used by NOC to authenticate GW_g. Figure 4-3 shows a NAN topology indicating the hierarchical authentication structure/path that is used for GW_g authentication. For completeness, in the figure we also show SMs. The authentication of SMs is discussed in later sections. The group controller of a group g is denoted by GW_g. The smart meter n of group g is denoted by SM_{ng}.

NOC creates a random master key K_{NOC}. This key will be used to generate keys for each child GW_g (GW_1 and GW_2. etc.)

$$K_{GW_g} = \mathcal{F}\ (K_{NOC}||GW_g) \qquad (2)$$

where $\mathcal{F}()$ is a secure one-way hash function and || is the concatenation operator. The key K_{GW_g} is stored at the corresponding GW_g. The NOC does not need to store it, since it can be generated from K_{NOC}. In a similar way, each child node GW_g produces shared keys for its

own child nodes. For example, if GW_1 has several child nodes as group gateways, GW_1 uses its master key K_{GW_1} to generate a key for each of its child nodes, $GW_{g'}$:

$$K_{GW_{g'}} = \mathcal{F}\ (K_{GW_1} || GW_{g'}) \qquad (3)$$

The keys generated are stored at the corresponding child nodes. Similarly, each of these nodes will generate keys for its child nodes and so on, until all the leaf nodes with no children have been reached.

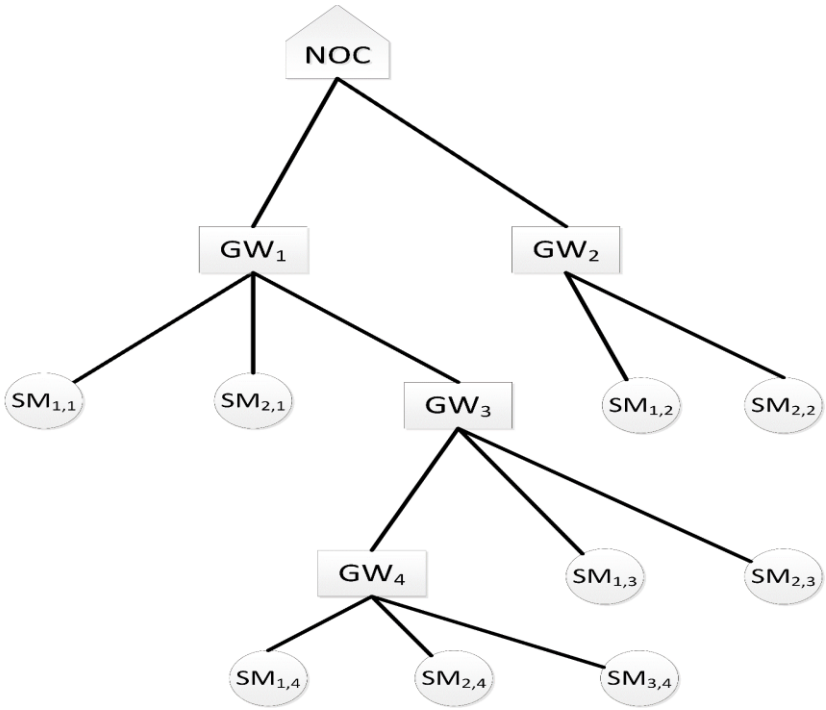

Figure 4-3 Authentication for Group Gateway

4.2.5 Case 1- Star-Star Topology

In this scenario, we consider a star for NAN topology in the group, with GW_g at the centre. The GW nodes directly communicate with the NOC. This scenario is simple since each SM has a direct link (one-hop) to its GW. This means that no network discovery needs to be made, since GW can detect its network. The process of SM authentication is also simple, because each SM can be directly authenticated by the GW_g.

First, the pre-deployment phase is discussed. This phase assigns the master key MK_{NOC} to the NOC and is depicted in Figure 4-4.

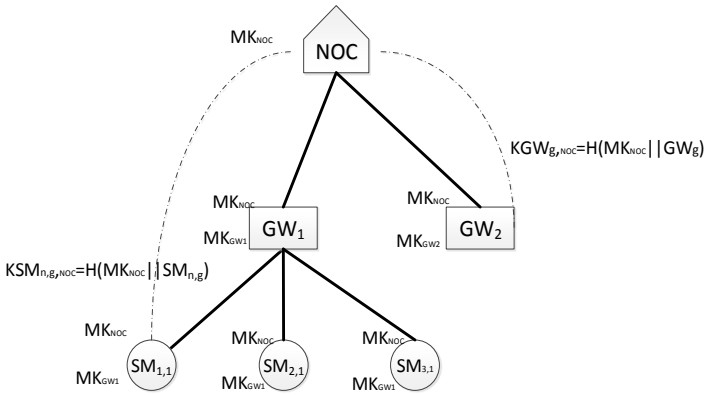

Figure 4-4: Pre-deployment of a NAN in star topology

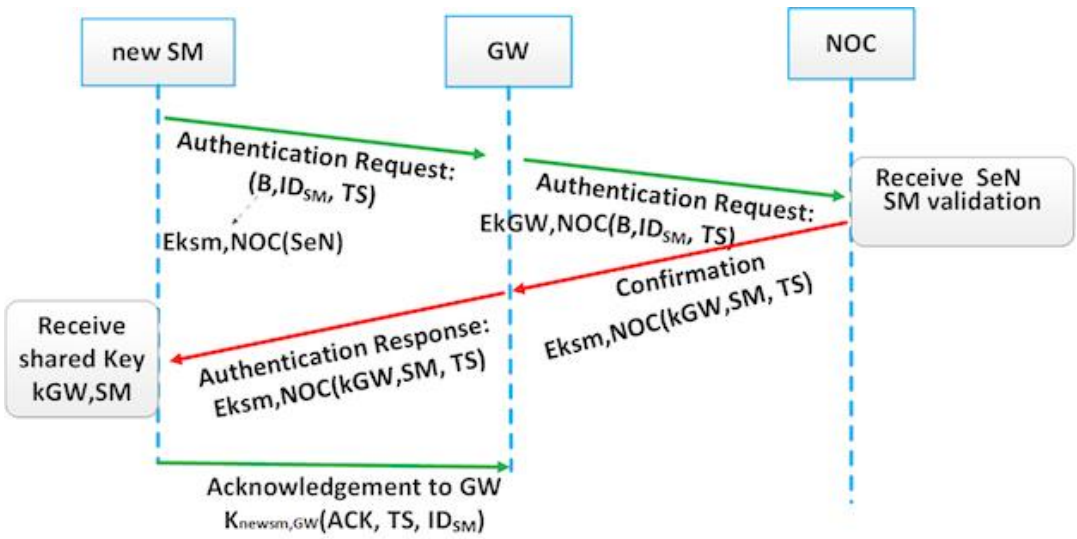

Figure 4-5: Authentication of an end device in a NAN with star topology

Secondly, the smart meter authentication is highlighted. Specifically, a SM_{ng}that wants to join a group needs to be authenticated by GW_g. As shown in Figure 4-4, initially, the new SM_{ng}will send a request message to GW_g. This message includes B, which is the encrypted message (serial number of new SM_{ng}) using symmetric key $K_{sm,\mathrm{noc}}$. Identity number of new smart meter, SM_{ng}, and Timestamp, TS (this is used to mitigate the replay attacks). The gateway GW_g will re-encrypt the message using K_{GW_g} and forwards the message to NOC. The NOC received B and decrypted it using $K_{sm,noc}$ and in order to validating serial number of new SM_{ng}. NOC responds to GW_g with a confirmation after validating serial number of new SM_{ng}. NOC will encrypt $(K_{GW,sm}, TS)$ using $K_{sm,noc}$ and send it to the new SM_{ng}via GW_g. After SM_{ng} receives the message it decrypts it using $K_{sm,noc}$ and obtains shared key

with GW_g $K_{GW,sm}$ SM_{ng} then replies with an acknowledgement message encrypted with the key.

4.2.6 Case Two - Multi-Hop (mesh)

The SMs are interconnected in a partial mesh or a full-mesh topology. Each group in the NAN consists of a GW and its nodes. The GW nodes are in turn interconnected to the NOC in a star configuration i.e., all the GW nodes are one-hop away from the star point, the NOC. Nodes within a group will require multiple hops to reach either the GW or the NOC. Full-mesh topology is happens where every SMs has a circuit connecting it to every other SMs in a group. Figure 4-6 illustrates this topology. In this case, there are six SMs that form a partial mesh topology between them with a multi-hop path to the NOC. A pre-installation phase comprises storing the shared key between the SM and the NOC, $K_{sm,noc}$, the ID of the device $SM_{n,g}$, a group ID G and a serial number SN on the devices.

4.2.7 Network Discovery and Registration

When a SM_{ng} is initally switched on, it requires learning about its neighbors in the network, which are within its range, in order to forward packets through them. To discover its neighbors, it broadcasts a Hello message and at the same time is listening for Hello packets that are broadcast by its neighbors (other SM_{ng}, GW_g, or NOC). The network discovery process is repeated every T time units to accommodate updates in the NAN topology. After receiving a Hello message, each SM_{ng} inserts information about its neighbour in the Neighbours table. These tables can be optionally sent to NOC, so that it has a total view of the NAN.

4.2.8 Authentication of the Smart Meters, SM_{ng}

When SM_{new} requests to join a group, it needs to be authenticated by GW_g. There are some SMs that have no direct link to GW_g. Therefore, the authentication method shown in Figure 4-5 is not suitable, and we propose a two-step authentication scheme. The new SM, SM_{new}, will be authenticated through another, already authenticated SM_{ng}, which is referred to as proxySM_{ng}.

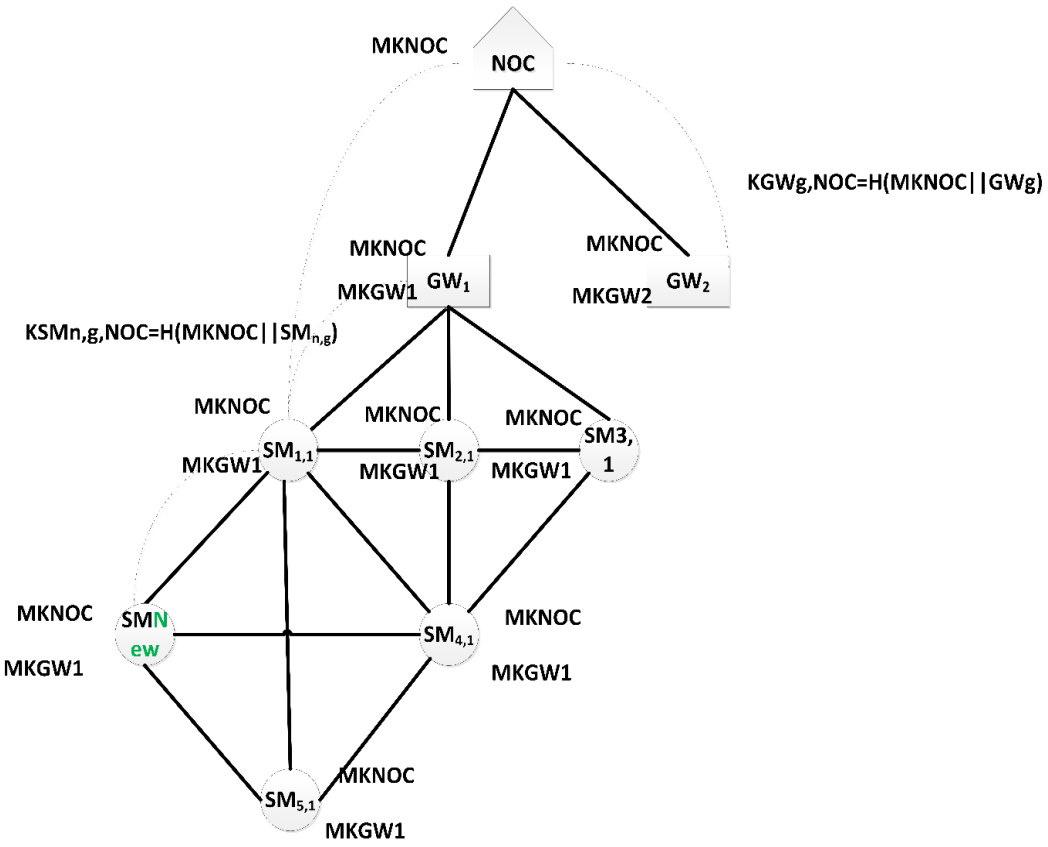

Figure 4-6 Pre-deployment for a Multi-hop NAN topology

Initially, the new SM_{new} sends an Authentication Request to the proxy SM_{ng} Figure 4-7. This message includes the following information:

a) Mi which is (serial number of new SM_{new}, SNNSM) encrypted using $K_{new,NOC}$,

b) Identity number of new SM_{ng}, IDSM_{ng},

c) Timestamp TS.

The proxySM_{ng} encrypts Mi along with its identity and TS using the shared key between proxySM_{ng} and GW_g. After GW_g receives and decrypts the message, GW_g re-encrypts Mi using the key K_{GW_g}. NOC will decrypt Mi using $K_{g,noc}$, check the serial number of new SM_{new}, SNNSM, and validate SM_{new}.

The NOC sends an authentication response, addressed to the new SM. The message, Xi consists of the encrypted master key of GW_g, MK_{GW} using $K_{sm,\text{noc}}$. When the new SM_{new}

receives MK_{GW}, it sends an encrypted acknowledgement to GW_g, using MK_{GW}. GW_g generates a random number R and multicasts the encrypted random number R, as a message, using shared key, $K_{GW,SM}$, thereby refreshing the keys of the group when the new SM, SM_{new} is authenticated. When all SMs receive the encrypted message they decrypt the message using $K_{GW,SM}$ to obtain the random number R. Then, each SM applies a one-way hash function on the random number R to generate the authentication value AVi. This authentication value is used by the gateway to authenticate nodes within the group. For example, for a group of SM with numbers between 10 to 20, the GW will multicast the key to all SM within a time duration of 5s (timeout value) when using a wireless mesh network such as ZigBee or Wi-Fi. Figure 4-7 illustrates the following steps in a ladder diagram.

a) SM sends an authentication request

b) NOC validates data and sends an authentication response

c) Authentication response contains MK_{GW}

d) GW sends R to New SM

e) New SM sends an ACK to GW

f) GW multicasts R to the group

Following the authentication, the SM sends data to the NOC. The steps involved in communication are listed below. Notice the authenticated forwarding in steps (d), (e). The intermediate nodes use a MAC to check the integrity and source of the packet that arrived. Also, note that the source node will ascertain that its data is delivered only when it receives an acknowledgement from the NOC. The details of the communication phase are out of the scope of this discussion.

a) SM decides neighbor to forward to, for a packet destined to the NOC

b) SM generates its encryption key K_{forw}, $\mathcal{F}$' $(R||SM_{n,g})$ where $\mathcal{F}$' is the one-way-hash function

c) SM generates a MAC for the message using K_{forw}

d) Neighbor receives the message with MAC and validates it. Knowing what node id it came from, it generates the forwarding key of the source using

e) If successful, it generates a MAC and forwards it to a neighbor (to the GW, if it is the neighbor). If the MAC fails, the packet is simply dropped.

Our scheme is scalable for the requirements of a Smart Grid. In our scheme, each gateway and its group transact individually with the NOC and have no interdependency on other gateways or groups, except for forwarding data to the NOC. When the devices are scaled, an appropriate number of gateways are included to match the number of groups formed. Each gateway and its group need access to keys for their own group, the gateway and the NOC. Each node will therefore have a pre-installed NOC key, a master GW key sent by the NOC and a random secret R sent by the group gateway. All other keys necessary are derived from this information. Therefore, our scheme is scalable to any number of end devices. However, we realize the need to limit the number of nodes per group to keep the number of paths low, the routing delays low and consequently the end-to-end delays low.

4.2.9 Updating of MK_{GW}

When $SM_{n,g}$ leaves its group and from the network, destroying old MK_{GW} and allocating a new master gateway key to all nodes $SM_{n,g}$ in that group is very crucial. It is because, the leaving node $SM_{n,g}$ may be replaced by a vulnerable node to relay false message and communicate with other nodes therefore, MK_{GW} revoking/re-keying is required. The NOC responsible to inform the other $SM_{n,g} \in GW_g$ nodes in that group and send a new MK_{GW}, which is encrypted using $K_{sm,noc}$.

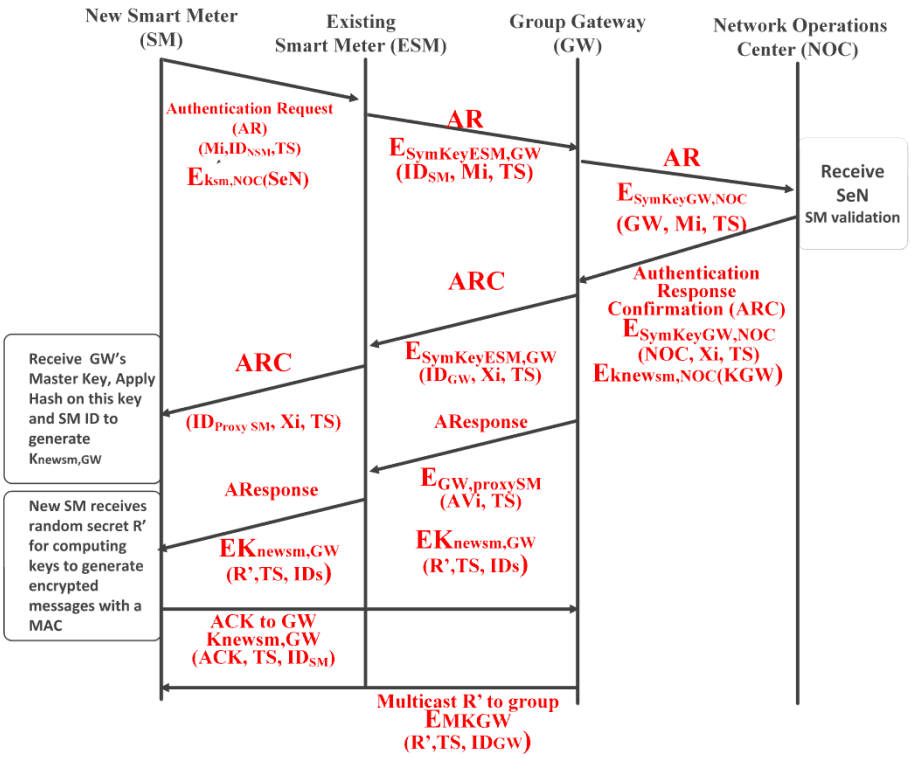

Figure 4-7 Protocol for NAN in a case 2

The following are the process steps of the updating MK_{GW}:

1. A smart meter node $SM_{n,g}$ must send a network leaving request L_{REQ} to the assigned dedicated node GW_g of that group. $K_{GW,SM}$ (L_{REQ}, TS, ID $SM_{n,g}$)
2. The GW_g will inform the other $SM_{n,g}$ nodes in its group (multicast) and NOC (unicast) about the leave using the messages $K_{GW,SM}$ ($L_{SM_{n,g}}$, TS, ID GW) and $K_{GW,NOC}$ ($L_{SM_{n,g}}$, TS, ID GW)
3. Removing the node $L_{SM_{n,g}}$ with L_{REQ}
4. NOC regenerates a new master gateway key MK'_{GW} and sends it to the specific gateway, which in turn multicasts it to all the remaining $SM_{n,g}$ in the group, encrypted using $K_{sm,noc}$.

The updating of MK_{GW} process described above introduces a cost of re-keying. This cost has two factors:

1. Additional processing overhead. Assume that the generation of a MK_{GW} key requires x CPU cycles. The processing overhead, Oproc noc = 1x (because NOC has to generate one key MK_{GW} for GW.

2. Communication overhead that includes two multicast and two unicast messages. The unicast messages are between the gateway and the NOC and the multicast messages are within the group.

4.3 Security Analysis

The authentication scheme is analysed against the two classes of threats mentioned in section 4. Sybil attack is an impersonation attack that is the result of eavesdropping and the node capture attack is the physical nodes capture which is very likely in the context of Smart Grid network.

The authentication scheme described in previous sub-section is two-way secure, meaning that after the authentication process, both parties new SM and GW can verify the authenticity of each other. The authenticity of GC is verified since the Authentication Request from SM is encrypted using GW's key. Also, in the Authentication Response, GW sends the SN of new SM. Only GW and SM know the mapping of SN to the ID number of SM. The authenticity of new SM is verified in a similar way. First of all, the Authentication Response is encrypted using SM's key and, therefore, only SM is able to decrypt it using its shared key. Also, the new SM provides to proxy SM both its ID number and SN, which provide additional security.

Denial of service (DoS) makes a node as well as the service on it inaccessible by others. An attacker sends a large number of packets, malicious or otherwise, addressed to the node and effectively at a rate which can block out all other communication. This causes the node receiving the packets to exhaust its storage and computing power, processing the packets that arrive from the attacker. Such a risk is imminent in a multi-hop network where the communication between two end points is routed via intermediate smart meters. The proposed authentication scheme authenticates every participant on the network before accepting any traffic from it. While this reduces the probability of spurious data on the network, the spurious traffic remains a problem. If such traffic targets a gateway node, then, an attack can potentially incapacitate all nodes that communicate using that gateway. Additional means of detecting such intrusions and methods of isolating the attack traffic are necessary to handle such vulnerabilities.

Our scheme does not handle jamming attacks. Jamming attacks are DoS attacks that targets wireless communication frequency in the smart grid. When nodes are in close range, large amounts of noise may be generated in these appliances. It is difficult to avoid jamming in our scheme because the victim and its client may not catch the attack. In this kind of attack, the attacker prevents legal users from having access to information and services by targeting the victim's device and the network connection. This attack stops the user from making outgoing connections on the smart grid. The communication can be jammed so as to make the signal noise very low, and this could lead to the failure of specific portions of the Smart Grid [134].

4.3.1 Node capture attack

Node capture attack is both a challenging and interesting attack with a goal taking control over a smart meter's communication after gaining physically access [42]. This attack could easily be carried out because Smart meters are placed in customer premises and not within the utility's provider physical premises. Abdullah et al [135] presented studies on the attacks and vulnerabilities of Smart meters in a NAN and listed out node attack as the least attended to yet significantly dangerous to the Smart Grid network. Most of the schemes discussed in [48, 50, 136-138] show a vulnerability to node capture attacks. A successful attack could reveal shared keys thereby permitting an attacker to participate in encryption and decryption process or in a worst case scenario, inject false data into the Smart Grid network to comprise other nodes.

Our proposed group authentication scheme is secured against node capture attack. Even if the keys are captured by an attacker and used to send data, the data packet would get validated for forwarding, but the packet would be tagged as an invalid packet since the time stamp of the packet sent by the attacker would not match the timestamp value expected by the NOC. The NOC records the timestamps of all the packets it receives, node ID wise, so it knows what to expect in the next incoming packet from a particular node. However, if by some means the malicious node is able to retrieve the timestamp information from the captured node and set its local clock to that of the captured node, then the scheme will be effectively broken. This condition breaks the assumption number a, c, h.

4.3.2 Replay Attack

Both schemes present in [50, 51] show a vulnerability to replay attack. Our scheme is secure against replay attacks because it uses shared keys for communication and as well as time stamps. Both the communicating parties, based on a shared random secret, generate the shared key. By knowing the shared random secret one cannot derive the shared secret key. Therefore, it will be computationally difficult for an attacker to generate data, which is validated with an appropriate time stamp. Similarly, replaying previously transmitted data will render the data invalid since the time stamps are encrypted along with the data and when verified at the receiving end will not match with the expected value of the time stamp recorded on the receiving device [139].

In the event that an attacker, by some means is able to decrypt the captured packet and retrieve the contents of the packet, the node identity, the authentication value and its time stamp will be available to the attacker. Using them, valid data packets can be generated and spurious data can be sent to the NOC. However, it requires the attacker node to estimate the clock ticks of the active node and replay the packets for them to be accepted by the NOC. If the attacker is able to retrieve the value of the clock ticks of the node it has captured packets from, and regenerates the packets with valid time stamps, then the scheme can be broken. This again breaks the assumption (h) from the list of assumptions in section 5.2.2. However, such an attack is not termed as a replay attack, since the packets are re-crafted using the time stamp from the clock tick value synchronized with the node and other values from the captured packets.

Replay attacks can be more harmful than Denial of Service attacks, and this is because they can result in remote activities even against encrypted packets. In article [15], the authors state that replay attacks can alter authentication packets, allowing them to gain unauthorized access to the AMI. Once the attacker obtains access privilege to AMIs or smart meters, he/she can easily inject control indicators into the systems. The attacker has to initially study the packets being transferred from the customer's equipment to smart meters and examines these packets to identify the customer's general levels of power usage. Subsequently, such an attacker can spoof transmitted packets, and inject signals into the system. To analyze the effect of replay attacks on AMI, we consider a scenario whereby there is a simple network topology, and Sender-S has created 2, 3, or 4 hop (overlapping) transmission routes to receiver-D through relays R1 and R2. In such a situation, the attacker would be in Sender S's locality and eavesdrops on any packets being sent by S.

From the above, Sender A denotes the group of Smart meters "SM (L-SM)", while the Relays R1 and R2 denote the Gateway GW, and Receiver B denotes the Network Operations Centre. Thus, as previously mentioned, the normal network route should include packets travelling from a group of smart meters through an intermediate SM, referred to H-SM, to the GW and the GW then forwards the packets to the NOC.

However, as seen above, the attacker can carry out any of the following activities:

1. The replay attacker can decide not to alter packets' contents. Consider a situation where the PDR (i.e. the Packet Delivery Ratio) for all transmissions is '1'. If S sends a packet P1 and R1 receives this packet, followed by P2, the attacker eavesdrop on these transmissions. Subsequently, R1 forwards both P1 and P2 to R2. However, during intervals, the attacker can easily resend packet P1 to R1 again; thus, R1 is misled and resends P1 to R2, resulting in a delay in the time taken to send both packets P1 and P2.

2. The attacker edits the packet header: The replay attacker can receive packet P1, edit this packet, and then resend several of these packets to R1, resulting in flooding of the network and higher time delay/discrepancy during transmission.

The sender-to-receiver performance degradation resulting from the actions of the replay attacker can be measured by the equation:

$$\Omega tdynamic\ (S\ D) = TS + NAV\ C\ (TS) + TD \qquad (3)$$

Whereby:

TS is the time to process message at Sender-S.

TD is the time to process message at Receiver-D.

NAV C (TS) is the time duration for communicating or sending packets between the sender (S) and receiver (D).

Using a more simplified analysis, we assume packets are sent from the smart meters to the gateway in "S1" seconds, and from the gateway to the NOC in "S2" seconds. In such a

situation, a normal transmission from the sender to the receiver will take a maximum time interval of "S1 + S2" seconds. Considering a situation whereby a replay attacker eavesdrops on packets for "X1" seconds, and then replays these packets for "X2" seconds, the average time taken during a replay attack would be:

$$S12 + X2 + S22 \qquad (4)$$

Therefore, if an attacker listens during network packet transmissions for 100 seconds and then replays these packets for the next 100 seconds, applying the equation (2) above, time delay or discrepancy will be approximately 50% higher than the required time for sending packets. Furthermore, it can be deduced that when the hop count between nodes is increased (2 to 3 or 4), the time delay or discrepancy also increases. This is particularly based on the attacker's location, since the attack takes place from the location of the sender, the replayed messages travel through the major parts of the network with longer pathways, thereby resulting in increased time delays during transmission. Therefore, one replay attacker can reduce the routing time for packets by as much as 50%-60%, while numerous attackers can result in even more time disruption during network transmissions.

4.3.3 Sybil Attack

In a Sybil attack, a malicious node assumes multiple fake identities and attempts to inject traffic into the network. Our scheme prevents vulnerability to such attacks by falling back on the need to validate the authentication value and time stamp value in a packet. The authentication value is derived from the random number shared by the gateway. This value is encrypted with the key shared with the gateway and verified at the gateway. So, in order to fake multiple identities, the attacker node must have access to all the shared keys of the nodes it intends to fake [139]. If the attacker is able to get these keys and the random value from the gateway, the ID of the node can be faked. However, in order to successfully transmit data the attacker will require having valid time stamps that the NOC can validate. Like in the earlier cases, the scheme will be broken if the attacker successfully synchronizes the clock tick values of the nodes that are being faked. In such a scenario, assumption (h) from the list of assumptions in section 4.2.2 is broken.

The attacker can simply re-initiate an authentication process, to overcome the time stamp problem. Re-authentication is a directed activity controlled by the NOC and therefore any

attempt to re-authenticate will immediately be detected by the NOC, thereby mitigating the attack. If this authentication attempt is successful, then the scheme breaks. This can occur if the assumption (l) from the list of assumptions in section 4.2.2 is broken.

4.4 Summary

Table 4-3: Key management issues resolved in KM-HAN, KM-NAN

KM Issue	Resolution
Confidentiality	Encrypted Key exchange
Integrity	ID encrypted SEN, TS
Availability	Cryptographic key
Authentication of source	Authentication value

We have included the security requirements for the HAN and NAN scenarios based on which the design of KM-HAN and KM-NAN have been done. These schemes have been shown to be resilient to attacks and the assumptions that the scenarios make to claim the resilience have illustrated the cases when the security scheme breaks.

The typical key management problems that are addressed and resolved is in Table 4-3. We also compare the overheads of our schemes with two other schemes that are very similar to the scenarios we have considered. They are listed in Table 4-4. We observe that KM-NAN is economical, overall. The total number of keys required is four and only two keys are stored in the memory of any device, at any given time. Only one key is generated resulting

Table 4-4: Comparison of the overheads of the security schemes

Resources used in the security scheme	Abdallah & Shen	Demertzis et al	KM-HAN/ KM-NAN
Total keys for authentication & communication	N/A	N/A	4
Number of keys stored in memory of end device (SM, NOC) / intermediate devices (H-SM, GW)	2	2	2
Number of keys exchanged	2	2+password	1

Number of keys generated	Two pairs	2	1
Key type	Symmetric	Asymmetric	Symmetric
Number of messages to authenticate	2	Certificate	1

in a reduction of computing overheads as well as delays. Each device authenticates with the other using only one message when compared to the multiple messages used by other schemes. We now discuss the implementation, simulation and security verification of KM-HAN and KM-NAN in the forthcoming chapters.

Chapter Five: Implementation and Evaluation

5. Introduction

The previous chapter described the scheme of our novel key management solution for a Smart Grid's communication layer. In this chapter we present the implementation of our work. Our work addresses the key management in the communication layer; therefore, our scheme has been divided into two different communication levels: HAN and NAN. We have therefore evaluated the performance of each of these levels separately and compared them with existing proposed schemes from the literature. In this chapter we provide a detailed description of the implementation setups and results of our proposed scheme. We describe the performance evaluation process and discuss the different simulation scenarios used to show the performance of each level of our scheme. To begin, we have implemented the first level of the communication layer in a Smart Grid HAN scheme and evaluated the energy conception. Our contributed secure scheme is evaluated on the real TelosB, which is an open-source platform that includes a mote with sensors and the development using the TinyOS platform. TinyOS is a small, open-source, energy-efficient software operating system that supports large-scale, self-configuring sensor networks. Both TelosB and TinyOS were developed by UC Berkeley [140]. The scheme has been evaluated on the real platform in terms of prevention in different types of attack, such as replay, node capture, Sybil, time complexity and amount of information. The evaluation was very detailed, with many results obtained through the execution of the programing used.

5.1 Test bed Development

5.1.1 TinyOS

TinyOS is a small open-source operating system (OS) whose permissive, free software license enables programing power-embedded devices with limited amounts of RAM and flash. TinyOS was developed at UC Berkeley, which provides a framework for the most common type of motes' application programming [141]. It supplies software designed for the component's hardware elements, for example, sensing, communication, storage and routing. The TinyOS's software component-based structure and event-driven execution

model provide particular roles by either another sensor's software or a sensor's hardware [140]. The software component includes the following:

- Modules,

  Modules are components that have variables and executable code

- Configurations

  Configurations are components that wire other components together

- And application.

  In TinyOS the impalement of components of the application is different from regular programming. There are two-way directions in TinyOS that allow a user to issue a command to its provider and vice versa [142].

5.1.2 NesC

NesC (network-embedded systems C) is the programming language, with a set of cooperating tasks and processes that builds applications for the TinyOS platform.

It is a programming language that provides the minimum memory requirements and enables the system to interact with the hardware by utilising asynchronous interrupts. Moreover, it provides an event-driven concurrency model that uses a C-based programming language with components wired together to run applications.

Furthermore, it includes some types of the C libraries' standards and syntax with some extensions, for example, commands and events added to accommodate its event-driven style to programming [143] .

5.1.3 Selection of Hardware

There are a lot of sensor motes available for implementation consideration for any WSN's deployment, such as the Mica2, IMote2 and TelosB. Table 5-1 compares the characteristics of these motes [144].

Table 5-1 compares the characteristics of these motes

Sensors Motes	TelosB	MicaZ	IMote2
Processor Speed	8 Mhz	16 MHz	13-416 Mhz
Memory Size	10 KB	512 KB	32 MB
USB Interface	Yes	No	Yes
IEEE 802.15.4 support	Yes	No	Yes

We have utilised TelosB motes figure 5-1 to implement our contributed secure scheme on a real WSN platform. TelosB motes are programmed to utilise a specialised coding language, NesC, and also integrate an IEEE 802.15.4-compliant radio and have a 250 kbps data rate. It suites sensors for detecting integrated light, temperature and humidity motes.

Figure 5-1 TelosB sensor mote

5.2 Home Area Network (HAN)

Figure 5-2 the implementation of HAN in TelosB motes

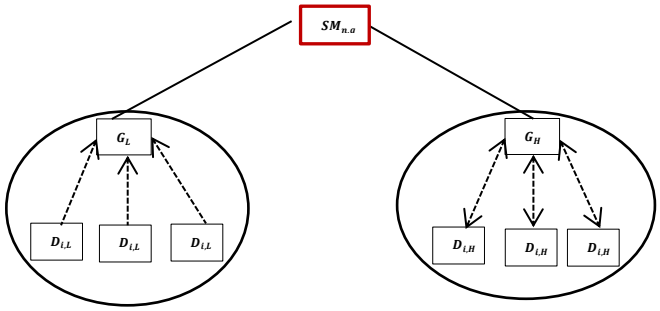

Figure 5-3: Topology of a HAN

An implementation of HAN scheme on TelosB motes figure 5-2, using TinyOS 2.1.2 has been done. AES was chosen for encryption. The key size is chosen as 16 bytes, the block size is 16 bytes and all input is processed with the same block size. The output is one block. SHA1 is used for generating a hash. Although SHA1 is advised as deprecated, it is valid for use until 2017. We consider generation of a signature equivalent to generating a message authentication code (MAC).

The motes in a specific class encrypt the sensed data using AES with a block size of 16 bytes and then sign the encrypted block using SHA1. The application data is 7 bytes. AES encrypted data is 16 bytes and SHA1 gives a 20 byte output. The total application payload is 36 bytes long. Figure 5-5 indicates the time taken to encrypt the data on the sender mote and the time taken to decrypt the data on the receiving mote. Similarly, Figure 5-7 indicates the time taken to generate the SHA1 hash on the sender mote and time taken to generate the hash on the receiver side and compare it with the received 20-byte hash value. On an average, the privacy overheads are about 4.6 milliseconds and the authentication overheads amount to 13.9 milliseconds. With the security scheme in place, we could expect a minimum

overhead of 18.5 milliseconds. This delay would add on to the normal operating delays (network delays) of such networks

5.2.1 Development of the group controller

The group controller program is implemented for the L-group of nodes, which only send the data to the group controller for onward transmission. The implementation consists of two programs, one on the end device and the other on the group controller. The program on the device does the following tasks:

1. Record the sensed data periodically (set to five seconds) into a variable.
2. Encrypt the node id, sensed data and the time stamp into an encrypted block.
3. Generate a signature of the encrypted block using SHA1.
4. Append the signature to the encrypted block to form the payload for transportation.
5. Send the packet destined to the gateway controller using `sendmsg()`.
6. Print the timestamp when the message was sent and the time taken to encrypt and time taken to sign

A portion of the code is included below as an illustration.

The program on the group controller performs the following tasks:

1. Receive a packet from a downstream node
2. Copy the signature block (MAC), compute a signature on the data part and verify the computed signature and the received signature.
3. If the signatures match, process the packet further. Drop the packet if they don't match.
4. The data in the payload is decrypted to check the contents further.
5. Check to see if the received node id is valid. If not, drop the packet

5.2.2 Development Platform & Devices

The development was done using the Eclipse IDE with a TinyOS plugin that provides for TinyOS function templates, syntax checks, wiring checks for modules and interfaces of TinyOS and pre-compilation checks such as internal and external references. The Eclipse IDE and TinyOS 2.1.2 package were installed on Ubuntu Linux 12.04 LTS Desktop version. This was set up on a Dell laptop with a 2.5 GHz processor and 8 MB RAM. The sensor

motes used were TelosB motes, described earlier. The compiled programs generated executable codes for the sensor motes and were downloaded on to the motes for operation.

The programs included print statements for purposes of information and debugging (not included in figures 5-4 and 5-6). The output of these print statements was captured by using a terminal emulator program that could read the output from the mote's serial (USB) port. The outputs from the motes illustrated in this chapter are screen captures of these outputs in the terminal emulator window.

```
task void sendmsg()
        {
          if (_radioBusy == FALSE)
          {
//Copy parameters to send
                dest_node_id=CLASSGW;
                msg1.NodeId = (uint8_t) TOS_NODE_ID;
                msg1.lum = luminance;
                msg1.ts = call LocalTime.get();
//original message block
                pointer8=(uint8_t*) &msg1;
                memcpy(in,&pointer8,16);
//Encrypt message
                 call AES.keyExpansion(exp,seck)
                call AES.encrypt(in,exp,out);
                encmsg = call Packet.getPayload(& encpkt,
sizeof(EncMsg_t));
                 memcpy(&(encmsg->eblock), out, 16);
//Sign the encrypted block
                call SHA1.reset(&ins);
                call SHA1.update(&ins, (uint8_t*) (encmsg->eblock), \\
                 (uint32_t) sizeof(encmsg->eblock));
                call SHA1.digest(&ins, (uint8_t*) (encmsg->sblock));

//------------Send the data packet----------------------

                if (call AMSend.send(dest_node_id, & encpkt,
                       sizeof(EncMsg_t)) == SUCCESS)
                {
                        _radioBusy = TRUE;
                        call Leds.led2On();
                }
                else
                {
                  printf("AMSend!=SUCCESS %d %d  %d\r\n",
                           i,SUCCESS, TOSH_DATA_LENGTH);
                }
            }
    }
```

Figure 5-4: The sendmsg() task on the end device

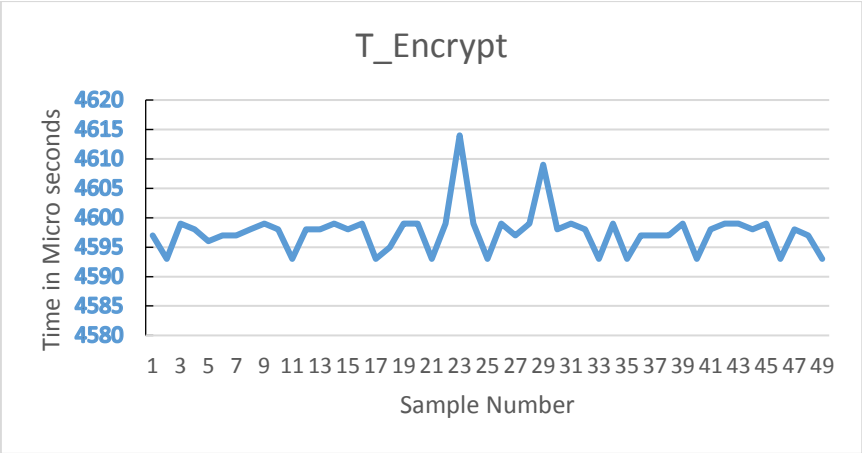

Figure 5-5: Total time taken for encryption and decryption at sender and receiver nodes

```
event message_t *RadioSnoop.receive[am_id_t id](message_t *msg,
                                                void *payload,
                                                uint8_t len) {
    call Leds.led1Toggle(); return receive(msg, payload, len);
  }

event message_t *RadioReceive.receive[am_id_t id](message_t *msg,
                                                void *payload,
                                                uint8_t len) {
   call Leds.led1Toggle();
   return receive(msg, payload, len);
  }

message_t* receive(message_t *msg, void *payload, uint8_t len) {
    message_t *ret = msg;
//If the packet is from REPLAYTHISNODE, queue it for Tx in
//radioSendTask()
if (call RadioAMPacket.source(msg) == REPLAYTHISNODE) {
post radioSendTask();
atomic {
      if (!radioFull)
        {
          ret = radioQueue[radioIn];
          radioQueue[radioIn] = msg;
          radioIn = (radioIn + 1) % RADIO_QUEUE_LEN;
          if (radioIn == RADIO_QUEUE_LEN)
            radioFull = TRUE;
          if ((!radioBusy) && radioFull)
            {
              radioBusy = TRUE;
            }
        }
      else
        drop();
        }
      } return ret;
  }
```

Figure 5-6: The receive() task on the end device

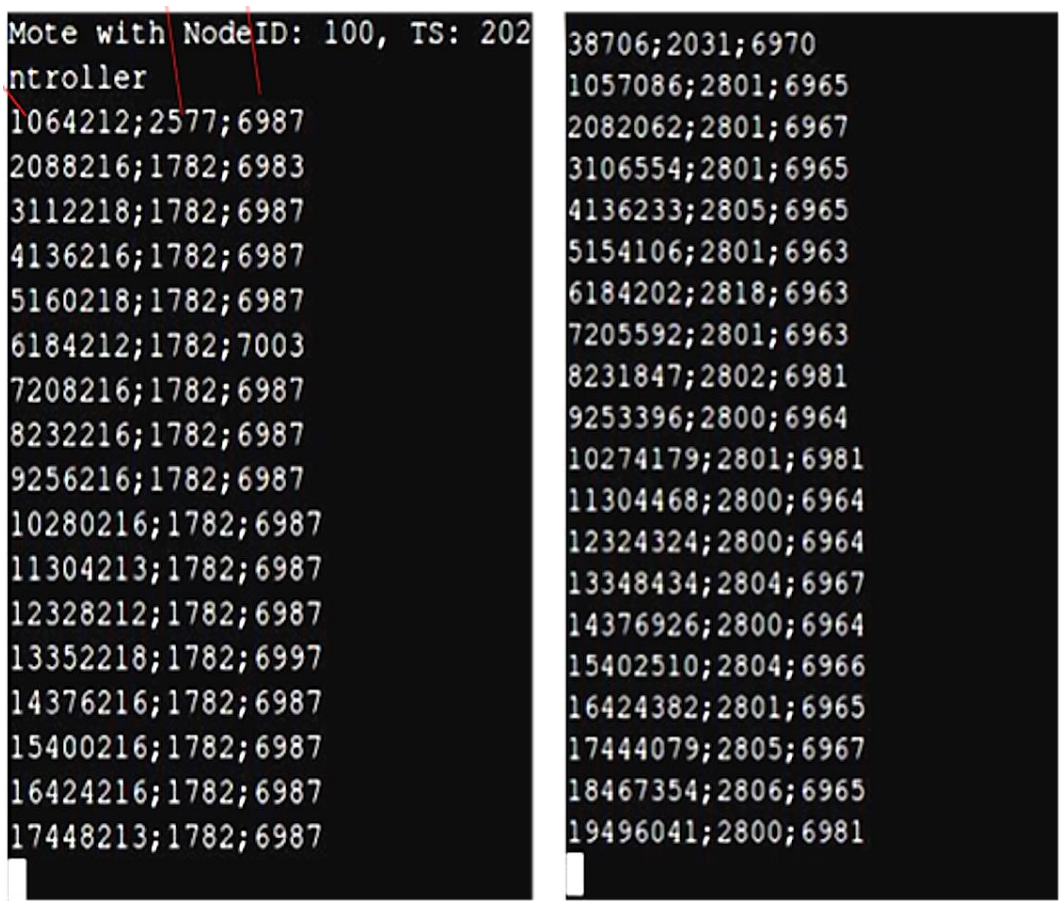

Figure 5-7: Outputs of ssender and receiver motes indicating timestamps in mu-secs (col 1), time to encrypt/decrypt (col 2) and time to sign/verify (col 3)

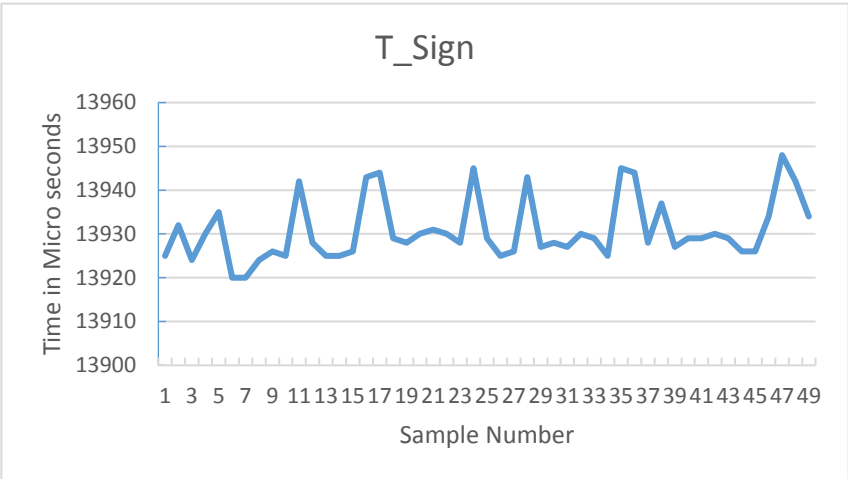

Figure 5-8: Total time take for signing and verifying at the source and destination nodes

Total time taken for encryption and decryption at sender and receiver nodes (1E+1D)

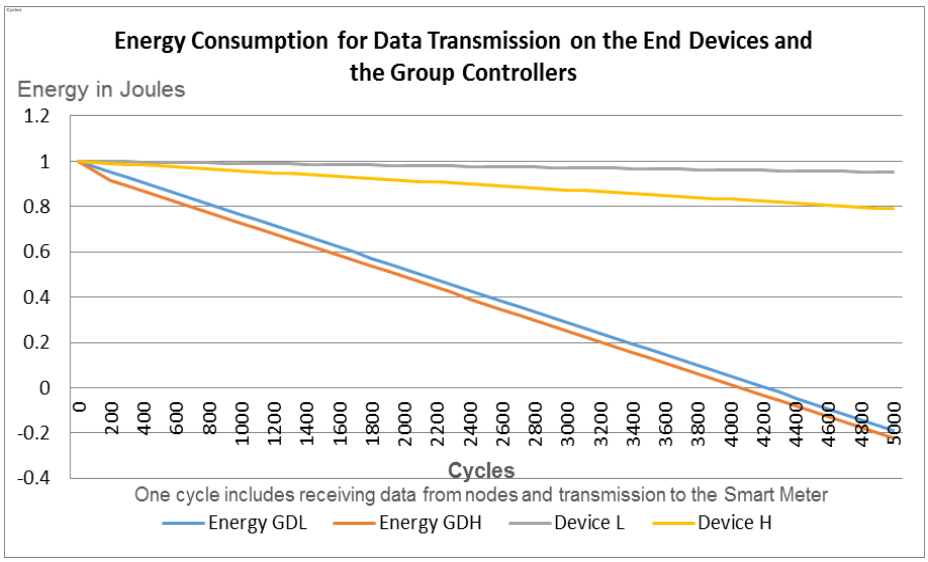

Figure 5-9: Energy consumption during the communications phase

5.2.3 Energy Consumption

The proposed scheme uses only symmetric keys therefore, it is economical on both storage as well as energy consumption unlike [44, 133]. In terms of storage, each device in Group L stores a maximum of two keys and a node ID whereas a device in Group H stores a maximum of three keys and a node ID. The energy consumption, based on the number of bits transmitted on the network; also it is significantly low since the encryption overheads are low. For example, using AES for encryption with a block cipher of 16, a data sample 16 bits long, when encrypted remains 16 bits long; a data sample 24 bits long, when encrypted is 32 bits long. The encryption overhead, therefore, is a maximum of 15 bits, for any input data size. Authentication functions give a fixed signature size (typically 128 bits or 8 bytes long) regardless of the input size. Therefore, when the signature is sent along with the encrypted data, the total number of bits transmitted increases and hence the energy consumption is higher. The energy per bit transmitted is calculated assuming a data rate of 250 Kbps and an active state current of 15 mA at 3.3V.For a Group L device $D_{L,i}$ the data sample size is 16 bits (2 bytes), the node ID is 16 bits and the time stamp is 16 bits, totaling to 48 bits (6 bytes) of data. Similarly, for a Group H device D_{Hi}, the data size is 16 bits, the node ID is 16 bits, the time stamp is 16 bits and the message authentication code is 160 bits, totalling to 208 bits (26 bytes). Note that the byte count increases by 20 bytes with authentication. AES is used for encryption and SHA-1 is used for authentication. With authentication turned on, the energy consumption is markedly higher than when only

encryption is used. The Group L is assumed to have twenty-five devices and Group H is assumed to have ten devices. The devices send data every ten minutes via the own group controllers. The group controllers receive data from the devices, decrypt them, encrypt them using the shared key of the smart meter and forward the data to the smart meter. A set of data from both the groups forwarded by the group controller to the smart meter is referred to as a cycle. Figure 5-9 shows that energy of the group controller for group L lasts around 4300 cycles and that of group H lasts for 4000 cycles. $D_{L,i}$and $D_{H,i}$ last far beyond 4300 cycles (4300 cycles at 600 secs per cycle implies 30 days.). However, the energy consumed by $D_{H,i}$ is more than that consumed by$D_{L,i}$.

5.2.4 Implementation of replay attack

A Replay attack involves a malicious node capturing authentication/data packets sent from a home devices and re-sending them at a later point in time, expecting to authenticate and gain entry into the home network [145]. A separate mote was programmed to sniff the packets and replay them. This program would receive packets in promiscuous mode, make a copy in a buffer and resend them after a specific time delay, which could be programmed. For our experiments, this delay was programmed as five seconds. The packets would not be verified for their signatures or for their authenticity. Packets originating from specific nodes could be replayed. An ideal packet replay program should be able to capture a set of packets into its buffers and play out the complete buffer when required. However, such a feature was not implemented due to the complexity of writing and reading data from a mote to an external file system. The following code illustrates the receiving of packets in promiscuous mode as well as in direct mode (packets addressed to the replay node). The direct mode provides a means of sending control packets to the reply node. The delay before transmitting the packet to be replayed is part of the code that queues the packet for replay, `radioSendTask()`.

Once the replayed packet reaches the HGC, the integrity check and the privacy checks are made and finally, the time stamp is verified. Upon verification of the time stamp, the time stamp of the replayed packet may not fall within the window of the next expected time stamp value. In a typical case, it will be less than the expected value and will cause the HGC to report an error and ignore the packet as well as the data it carries. The time stamp value is a

32-bit value and expressed as microseconds. This counter will wrap around after

```
event message_t *RadioSnoop.receive[am_id_t id](message_t *msg,

                                                void*payload,
                                                uint8_t len)
{
    call Leds.led1Toggle(); return receive(msg, payload, len);
  }

event message_t *RadioReceive.receive[am_id_t id](message_t *msg,
                                                  void *payload,
                                                   uint8_t len)
{
    call Leds.led1Toggle();
    return receive(msg, payload, len);
  }

message_t* receive(message_t *msg, void *payload, uint8_t len) {
    message_t *ret = msg;

//If the packet is from REPLAYTHISNODE, queue it for Tx in
//radioSendTask()
if (call RadioAMPacket.source(msg) == REPLAYTHISNODE) {
post radioSendTask();
atomic {
      if (!radioFull)
        {
          ret = radioQueue[radioIn];
          radioQueue[radioIn] = msg;
          radioIn = (radioIn + 1) % RADIO_QUEUE_LEN;
          if (radioIn == RADIO_QUEUE_LEN)
            radioFull = TRUE;
          if ((!radioBusy) && radioFull)
            {
              radioBusy = TRUE;
            }
        }
      else
        drop();
        }
      } return ret;
  }
```

Figure 5-10: The replay attack program with promiscuous receive and resend

a value of 2^{32} and this condition is take care of when making the time stamp comparison.

5.2.5 Implementation of node capture attack

Randomly turning off the end nodes and assessing if the rest of the nodes were reachable to the HGC implemented the node capture attack. Since the HGC and the end nodes form a tree of depth one, the failure of one or more nodes did not affect the working of the rest of the nodes. When the HGC does not receive an expected update in a specific period, it

marks the node as inactive and waits for three successive missing updates to mark the node as dead. Once a node is marked as dead, all state information pertaining to that node will be removed, until the node restarts and begins to transmit again.

5.2.6 Implementation of Sybil attack

The Sybil attack was emulated by adding a mote with the program for an end device. In this case, the attacker mote was programmed with valid node ID, secret key pairs as registered in the HGC. The mote was programmed to randomly pick a node ID and use the associated key to send data upstream. Like in the case of the replay attack, the time stamp of the attacker mote gave away since the time stamp value of the attacker mote varied quite significantly from those of the other motes it attempted to spoof.

5.3 Neighbourhood Area Network (NAN)

The proposed scheme was implemented on TelosB motes using TinyOS version 2.1[140]. Six motes were used, one each in a role as the NOC and as a GW and four others in a mesh communicating to the NOC, via the GW. The motes were pre-loaded with the addresses of the NOC and the GW nodes as well as the master key of the NOC.

Each of the motes had a separate program to receive a packet, check for its credentials and then forward it to the upstream or downstream node, as necessary. The intermediate nodes – the Proxy SM and the gateway performed the forwarding of packets. The NOC receives the packets and validates the identity and the time stamp sent along with the data and then provides an appropriate response. The NOC records the running time stamps in a circular buffer of size three; three previous time stamp values from a specific node are used to validate the time stamp received from a specific node. The code snippet below shows how

```
Ifndef NODES
#define NODES 5
endif

//Store the incoming TS; TSN is the n-th TS  from node NODEID
TSArr[NODEID][TSN % 3] = in_eblock.TS;
validate_TS(uint_8 NODEID, uint_32 recd_TS);
```

Figure 5-11 Recording the received time stamps and storing them for comparison

the time stamps from a specific node are stored in a two-dimensional array. Once a packet is received, its time stamp is validated using the `validate_TS()` call, which finds out the deviation of the received time stamp, with the earlier samples. If the deviation is below a threshold (set to 10 % amounting to 8 ms), the packet is accepted. This threshold value is based on the one-way application packet delay from the device to the NOC.

The intermediate nodes, ProxySM and the GW receive packets from downstream devices and forward them upstream. The ProxySM does one round of encryption for packets destined to upstream nodes and one round of decryption for packets destined to downstream nodes. Packets going upstream and packets going downstream are marked with different packet types for easy debugging. The functional packet types are assigned different packet types within the application packet.

```
//Define a AM type for upstream and downstream packets; Nodes do
//not accept packets with any other type from down/upstream nodes
//respectively
enum
{         AM_RADIO_UP = 6 // Active Message type is 6
};

enum
{         AM_RADIO_DN = 7 // Active Message type is 7
};
```

Figure 5-12 Different AM types for packets destined upstream and downstream with reference to the end device

```
//Define Packet Types
#ifndef AUTHREQ
#define AUTHREQ 1
#endif

#ifndef AUTHRESP
#define AUTHRESP 2    // indicates a successful authentication
#endif

//Define ERROR Status as a constant value 3

#ifndef AUTHERROR
#define AUTHERROR 3  // indicates a authentication error
#endif

#ifndef AUTHREJECT
#define AUTHREJECT 5 // indicates a authentication rejected
#endif
//---------------END ERROR Status Messages
```

Figure 5-13: Application packet types for the authentication process

In a similar manner, the authentication packets are identified with specific application packet types that are part of the application data. This helps in gathering and maintaining the state information for authentication status of each node.

The NOC and the GW nodes were switched on respectively and the GW authenticated with the NOC. Subsequently, the nodes were switched on, one-by-one. Note that the implementation on the motes did not use the link layer encryption facility. The nodes were physically located such that each node was in the radio range of only two other nodes. This ensured that there were at least two two-hop paths from the nodes to the GW. The network topology is illustrated in Figure 5-15.

Two specific measurements were made. The time taken for encryption, decryption (AES [147], with block size 16, key size 128 bits) was measured. Figure 5-14 provides a snapshot of the packet transit across the nodes labelled L-SM (leaf node), H-SM (intermediate node), GW (group gateway) and NOC (the NOC). Each line starts with a time stamp in microseconds, indicates the source and destination node addresses (L-SM and NOC only), followed by the application data size (33 Bytes), the time to encrypt/decrypt the packet contents on the node (in microseconds) and the name of the routine providing the information.

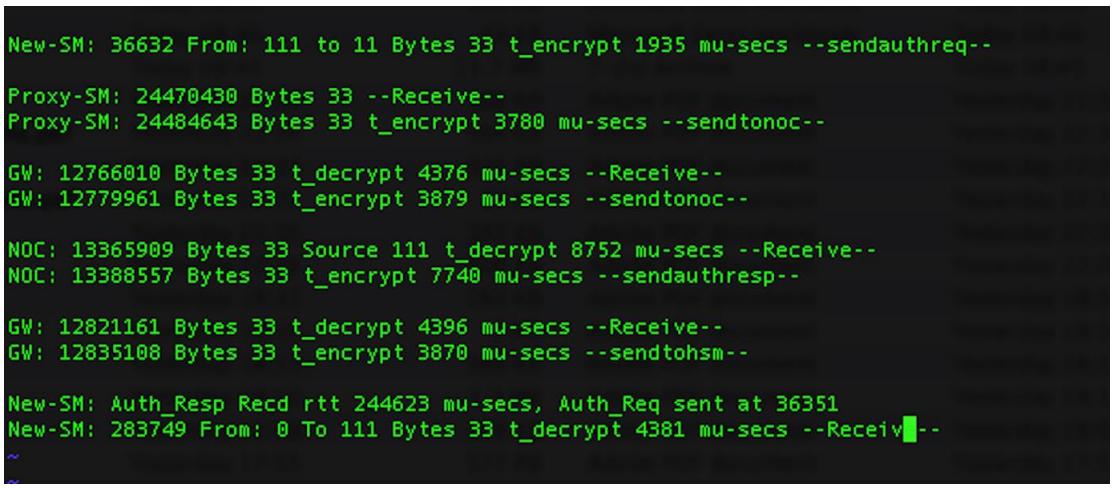

Figure 5-14: Output of the motes from L-SM to NOC and back

The corresponding outputs at each node in the path to the NOC is captured individually and illustrated in the Figures 5-16 to 5-19. Figure 5-16 represents the output at the mote labelled as NOC. The NOC node prints an output on receipt of a packet. It prints the timestamp when the packet was received, the immediate node from which it was received, the total number

of bytes and the action it takes. The output shows successful authentication response packets being sent (marked as `-sendauthresp--`).

Each node prints out the time taken to decrypt the data and re-encrypt the data with the appropriate key for the next hop in the path to the NOC or to the end node, L-SM. Note that the time is not synchronized across the motes and hence the timestamps across the motes do not correspond. They depend on when the mote has been turned on. If a packet has to be traced, we require to set a packet sequence number at source and track it. Since the NAN scheme does not require the data to be signed, the time required for signatures and the time required to verify them are not displayed.

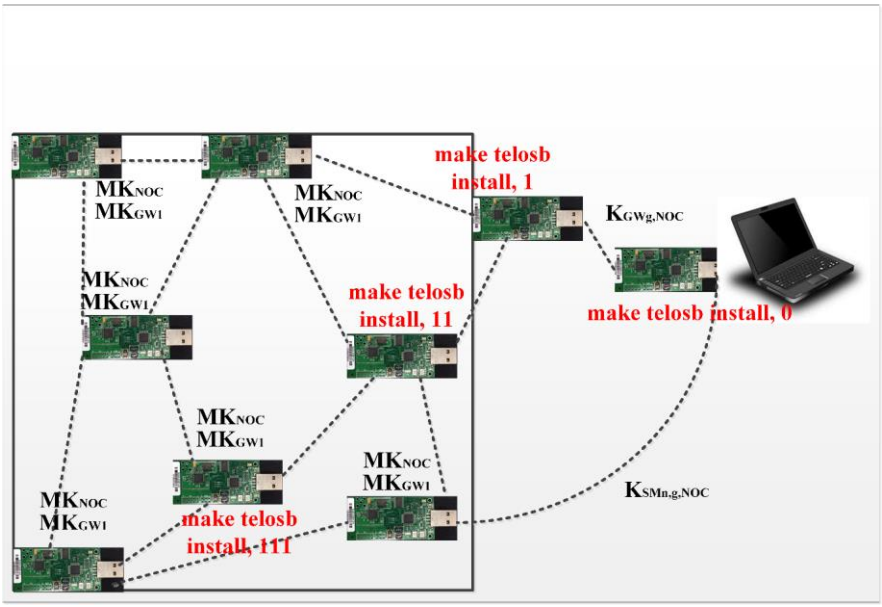

Figure 5-15: The topology of the NAN implementation using TelosB motes

```
GtkTerm - /dev/ttyUSB1 115200-8-N-1
NOC: NodeID: 0, TS: 21882 MaxBuf 32 Avail 32 Secure-mode? 1, Forward
 data to the NOC and to New SM
NOC: Node 0, TS 21882, Forwards data to the NOC and to New SM

NOC: 13365909  Bytes 33  _Source Node 163 Bytes 21_ t_decrypt 6498 m
icrosecs -Receive-
NOC: 13388557 Bytes 33 t_encrypt 8325 microsecs -sendauthresp-
\ NOC: Waiting 2710804632
NOC: 22572510  Bytes 33  _Source Node 163 Bytes 21_ t_decrypt 6499 m
icrosecs -Receive-
NOC: 22595458 Bytes 33 t_encrypt 8400 microsecs -sendauthresp-
\ NOC: Waiting 2710779719
NOC: 31792201  Bytes 33  _Source Node 163 Bytes 21_ t_decrypt 6499 m
icrosecs -Receive-
NOC: 31814754 Bytes 33 t_encrypt 8307 microsecs -sendauthresp-
\ NOC: Waiting 2710777391
NOC: 37622334  Bytes 33  _Source Node 94 Bytes 21_ t_decrypt 6499 mi
crosecs -Receive-
NOC: 37644740 Bytes 33 t_encrypt 8300 microsecs -sendauthresp-
\ NOC: Waiting 2710801157
```

Figure 5-16: Output of the mote labeled NOC

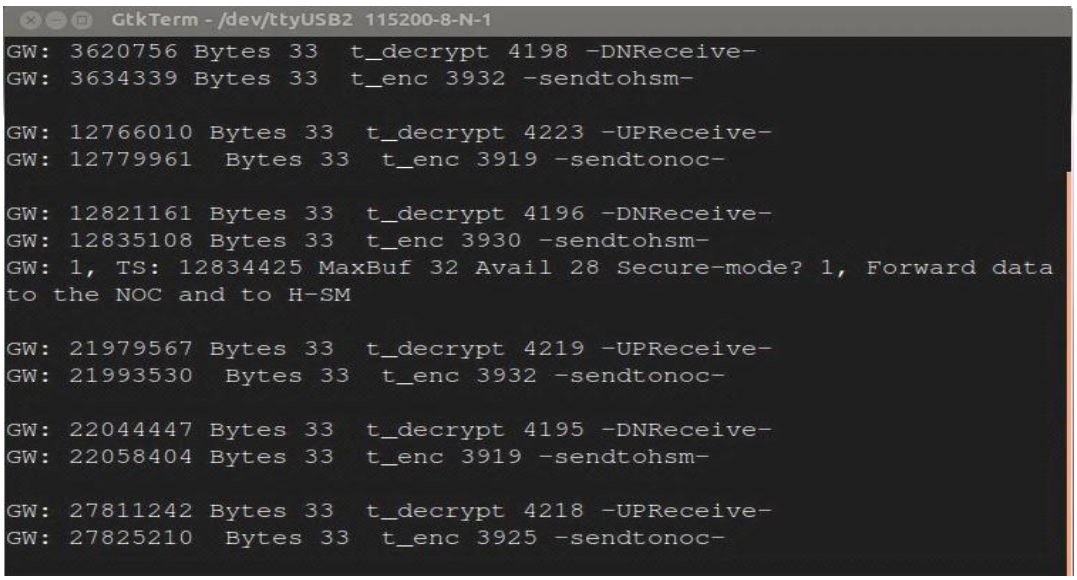

Figure 5-17: Output at the mote labeled GW

Figure 5-17 shows the output at the node labelled GW. This node received packets going to the NOC (`--UPReceive--`) as well as those going towards the end nodes (`--DNReceive--`). The packets being sent are labelled with the node they are sent to `sendtohsm` and `sendtonoc`. Other output details are similar to those on the NOC. The output at the H-SM is similar to that at the GW except that the packets being sent are labelled with the node they are sent to `sendtosm` and `sendtogw`.

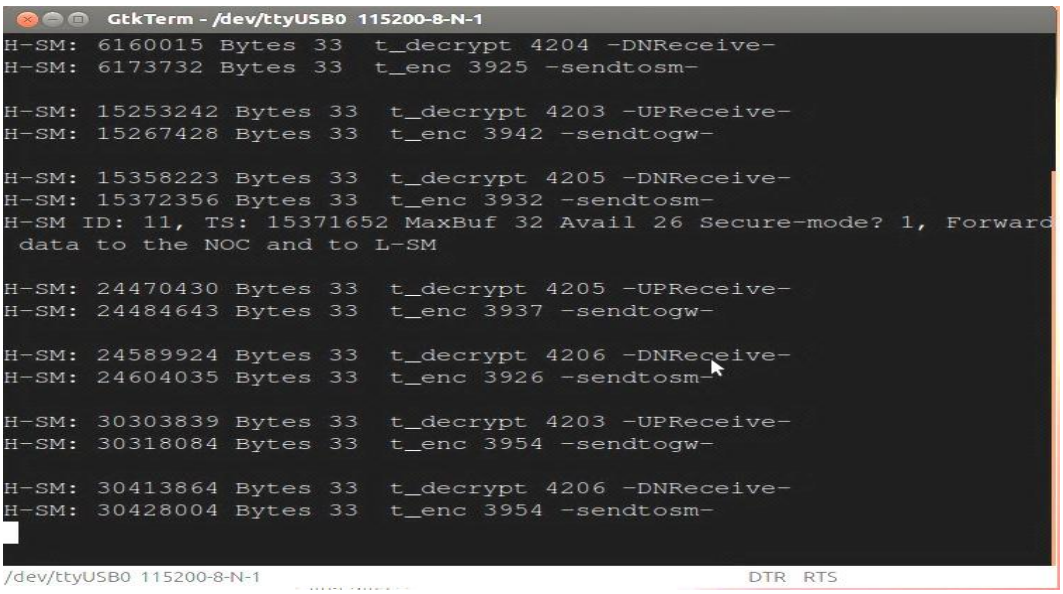

Figure 5-18: Output at the mote labeled H-SM

Figure 5-19 shows the output at the L-SM. It originates the authentication request (marked as `--sendauthreq--`) and forwards it to the upstream H-SM. Upon receiving a packet, it verifies the content and if an authentication response received, it prints the total time elapsed since the corresponding authentication request was sent as the round trip time for the authentication. All time units are in microseconds.

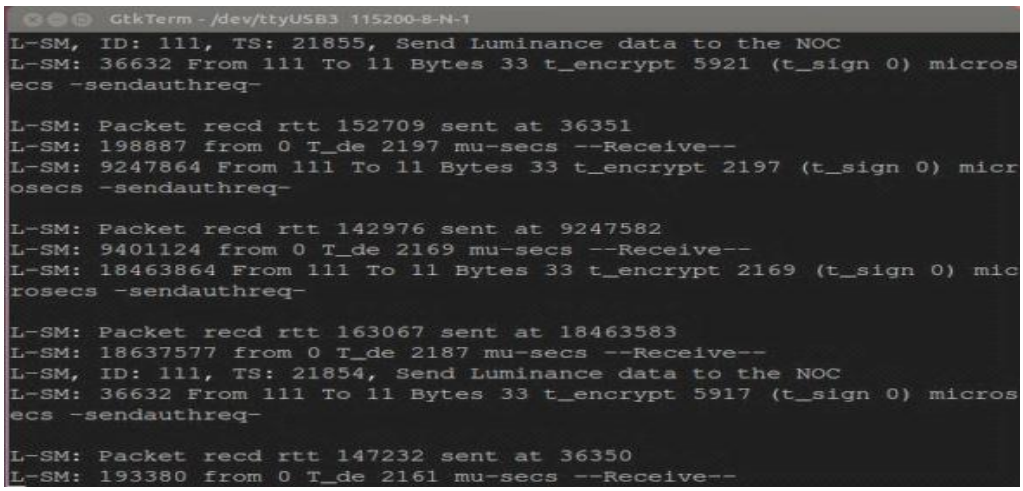

Figure 5-19: Output at the node labeled L-SM

Tables 5-2 and 5-3 list the time taken for encryption and decryption on each node as the packet traverses the network from the L-SM to the NOC and back. The total of these times subtracted from the measured round trip times gives the total network delay. This network delay is across a total of six hops in case 2 and three hops in case 1.

Table 5-2 Measurement of the scheme encryption and decryption times in Micro-seconds and RTT in Case1

	HN		GW		NOC		
	t_enc	t_dec	t_dec	t_enc	t_dec	t_enc	RTT
From HN to NOC	5783		4224	3960	6527		218470
From NOC to HN		7371	4182	3896		8354	225303
From HN to NOC	5883		4226	3923	6484		224103
From NOC to HN		7287	4201	3962		8322	
				174173	181006	179806	

Table 5-3 Measurement of the scheme encryption and decryption times in Micro-seconds and RTT in Case2

	New-SM		Proxy-SM		GW		NOC		
	t_enc	t_dec	t_dec	t_enc	t_dec	t_enc	t_dec	t_enc	RTT
From HN to NOC	1935			3870	4376	3870	8752		257136
From NOC to HN		4376	4376		4376	3870		7740	257648
From GW to L-SM		4376	4376			7740			253770
From L-SM to GW	1935				4376				
From GW to L-SMs		2188			1935				

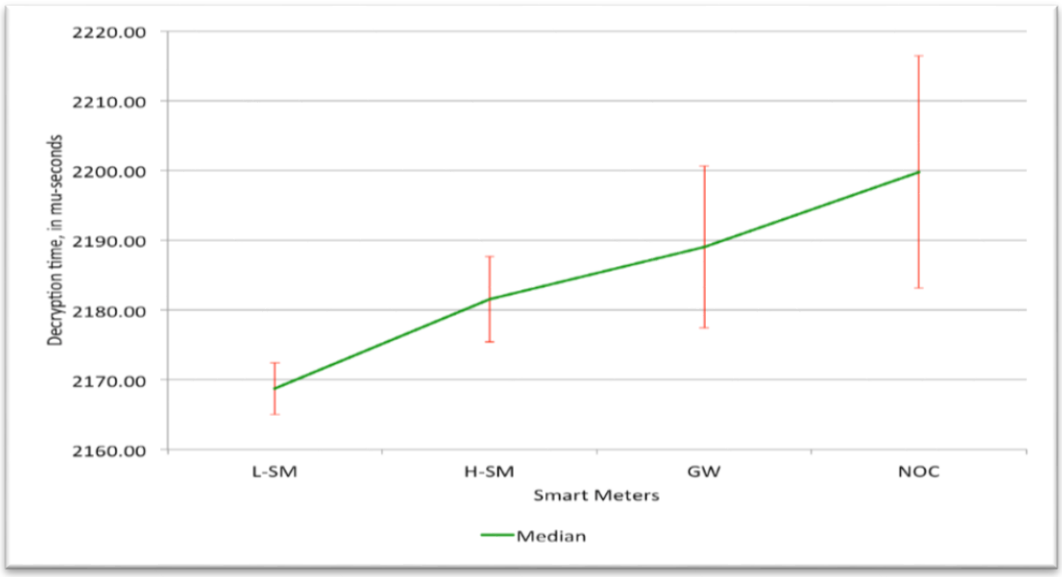

Figure 5-20: Time taken for AES dencryption of a 16-byte block on motes in a mesh topology

The total delay for the authentication process of a mote, using a two-hop path was measured. The average encryption and decryption times on end nodes are 6 ms and 6.2 ms, on intermediate nodes (authenticated forwarding), including the GW node 3.9 ms and 4.2 ms and on the NOC 8.2 ms and 6.5 ms. The average RTT from an end node to the NOC was 196 ms. The average RTT between a pair of nodes on the network was 25 ms. The entire authentication process took 331 ms.

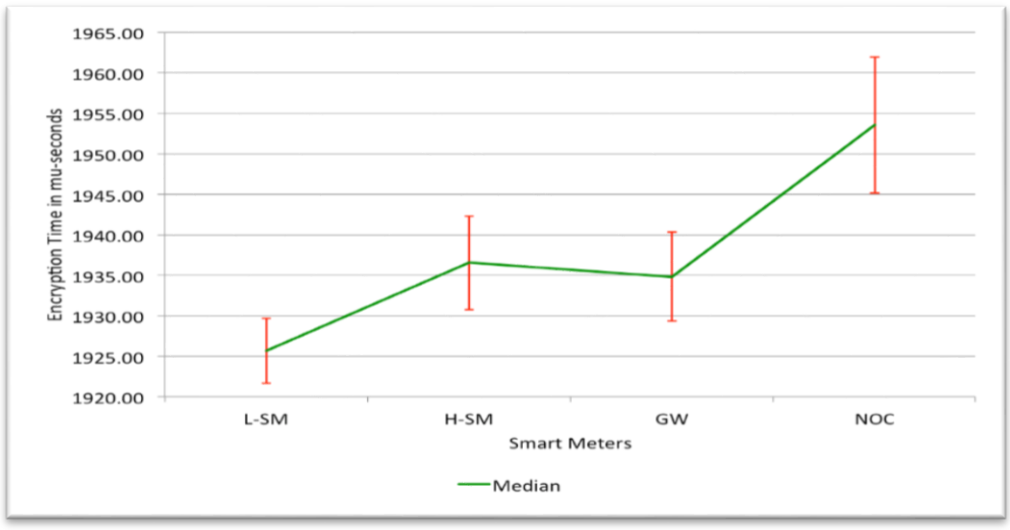

Figure 5-21: Time taken for AES encryption of a 16-byte block on motes in a mesh topology

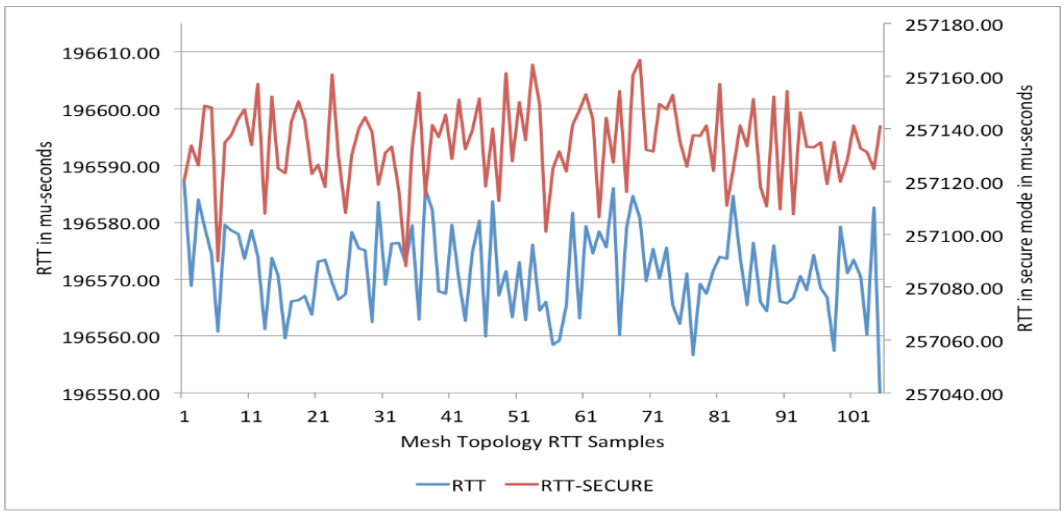

Figure 5-22: RTT from L-SM to NOC in mesh topology (3 hops)

The time taken for encryption and decryption of a 16-byte block of the application packet is shown in Figures 5-20 and 5-21 respectively. This measurement was done using the microsecond timer implemented in TinyOS. The timer was fired before and after the encrypt/decrypt operations, within the application. Therefore, the measurement includes the TinyOS overheads (interrupt servicing, packet reception, etc.). The data set contains a hundred measurements on each mote and indicates the mean of the data set and the standard deviation.

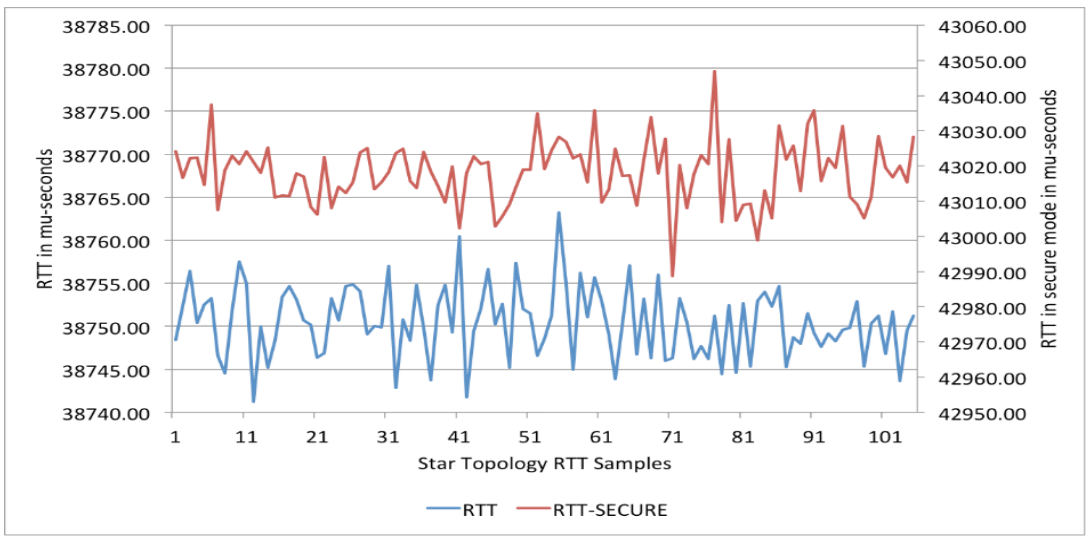

Figure 5-23:RTT from L-SM to NOC in star topology (1-hop)

The path from the L-SM to the NOC is a three-hop path. Each mote in the path will require to process packets from its downstream, in addition to its own packets, which leads to an increase in the overall encryption time. This is evident from the increasing encryption

and decryption times as well as the increasing value of the standard deviation of the data set, which is plotted as an error bar.

The round trip time (RTT) for an authentication packet (network transit time + processing time on each mote) from the L-SM to the NOC and back, was measured for the star and mesh topologies. Figures 5-22, 5-23 indicates the RTTs without and with the security turned on (labelled as RTT-SECURE). The RTT for the mesh (figure 5-23) topology is an order of magnitude higher than that for the star topology (figure 5-22). The limitation of the implementation is the inability to examine the performance of the authentication scheme when the number of nodes is scaled up. This requires physical configuration and deployment of a large number of motes. Specifically, the load on the gateway node and its impact on the authentication delay require evaluation.

Such an evaluation is currently being attempted as a simulation in OPNET [146]. A network of nodes interconnected using ZigBee is simulated. These nodes, in a cluster-tree topology, are scaled up to large numbers towards two specific objectives. First, to measure end-to-end network delays (from the leaf nodes to the NOC, multi-hop path) and second, to emulate the application (authentication and sensor data) packet flows and measure the authentication delays, when nodes join/leave the network. Subsequently, the intent is to study the effect of physical node capture and node failures in terms of the extent of impact on node reachability and hence the portion of the network that is effectively non-functional.

5.4 Replay attacks in a NAN

A replay attack involves a malicious node capturing authentication/data packets sent from a smart meter and re-sending them at a later point in time, expecting to authenticate and gain entry into the network [145].

In the event of a replay attack, the attacker will resend a valid captured packet to the GW. Upon receipt, the GW will require to decrypt the packet using the shared key of the L-SM that it claims to arrive from. Following that, it forwards the packet to the NOC, which performs the same procedure and then implements the necessary checks on the content of the packet.

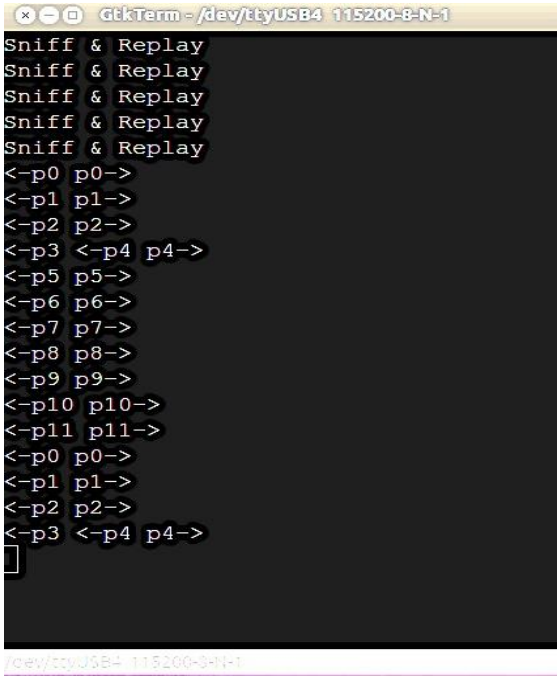

Figure 5-24: Screen capture of the output of the packet reply program (sniff and replay)

We have two specific concerns in the case of a replay attack. By definition, a replay attack involves resending a previously captured packet to gain access/privileges to the AMI. The security control is located at the central server, but the intermediate nodes have to process the packets they receive.

When the attacker repeatedly sends the replay packets, it causes the GW and the NOC to have to process the replayed packets to identify them. These packets are valid encrypted packets, which require being decrypted to examine the packet contents. This causes the processing load on the GW and NOC to increase. This increase can be substantial if the rate of the arrival of the replayed packets is sufficiently high, resulting in delays for traffic (authentication and data) from the other nodes, downstream.

Our concern is specifically on H-SM and GW nodes, which are in the path of the downstream nodes that send data to the NOC. In addition to delay, the H-SM and GW nodes consume energy to process the malicious packets and this could drain the resources on these nodes.

Both schemes present in [50, 51] show a vulnerability to replay attack. Our scheme is secure against replay attacks because it uses shared keys for communication and as well as time stamps. Both the communicating parties, based on a shared random secret, generate the

shared key. By knowing the shared random secret one cannot derive the shared secret key. Therefore, it will be computationally difficult for an attacker to generate data, which is validated with an appropriate time stamp. Similarly, replaying previously transmitted data will render the data invalid since the time stamps are encrypted along with the data and when verified at the receiving end will not match with the expected value of the time stamp recorded on the receiving device [139].

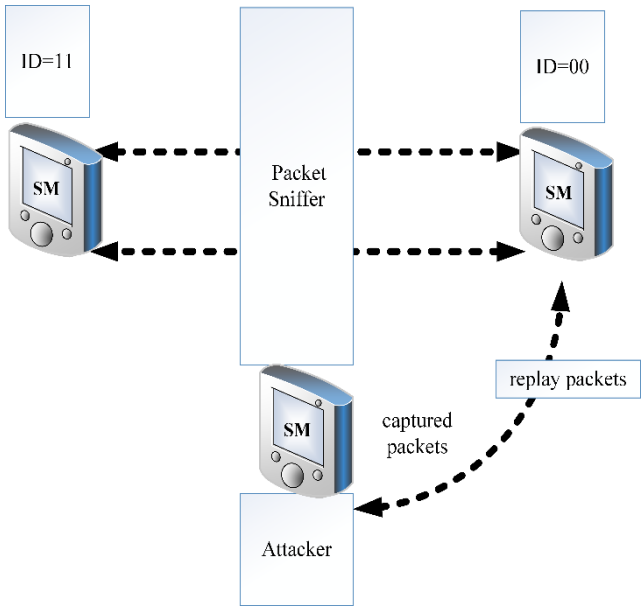

Figure 5-25: Modeling replay attack with the TelosB

```
if ( !AUTHDONE ) {
              dest_node_id=gwsm_inblock.ID_NSM;
              auth_at=call LocalTime.get();
              authed_node=gwsm_inblock.ID_NSM;
              post sendauthresponse();                                    }
              else
              {
              //DUP Auth request; Replay attack?
              printerror(DUP_err, NodeID, last_auth_at); }
              }
```

Figure 5-26: Flagging a duplicate authentication packet from the same node

The replay program used for attacks in the HAN scenario was used for the NAN scenario as well. The program sniffs packets from a particular node promiscuously, makes a copy and resends the same packet after a specified time delay. Figure 5-24 illustrates the output of the sniff and replay program. The output indicates the packet number received with an inward arrow (<-) and the same packet is then transmitted. The packet number sent is indicated with an outward arrow (->). The NOC examines the time stamps and accepts the packet only if the timestamp of the packet is within

the acceptable time stamp deviation threshold. If the time stamp is not within the acceptable threshold and the application packet type is an authentication request, the NOC responds with a warning mentioning a duplicate authentication request from the specific node. Figure 5-26 illustrates the code segment that flags the receipt of a duplicate authentication request from the same node that has been authenticated earlier. Such packets are discarded. Figure 5-27 illustrates a duplication authentication attempt from a node that is already authenticated. The output is from the mote labelled as NOC. The figure shows the duplicate authentication packet received as "DUP Auth packet" with the received packet's timestamp and timestamp at which the specific node was authenticated. Note that the received packet timestamp value could be higher or lower than the authentication epoch. This is to handle the timer counter overflow or wrap around at the remote nodes.

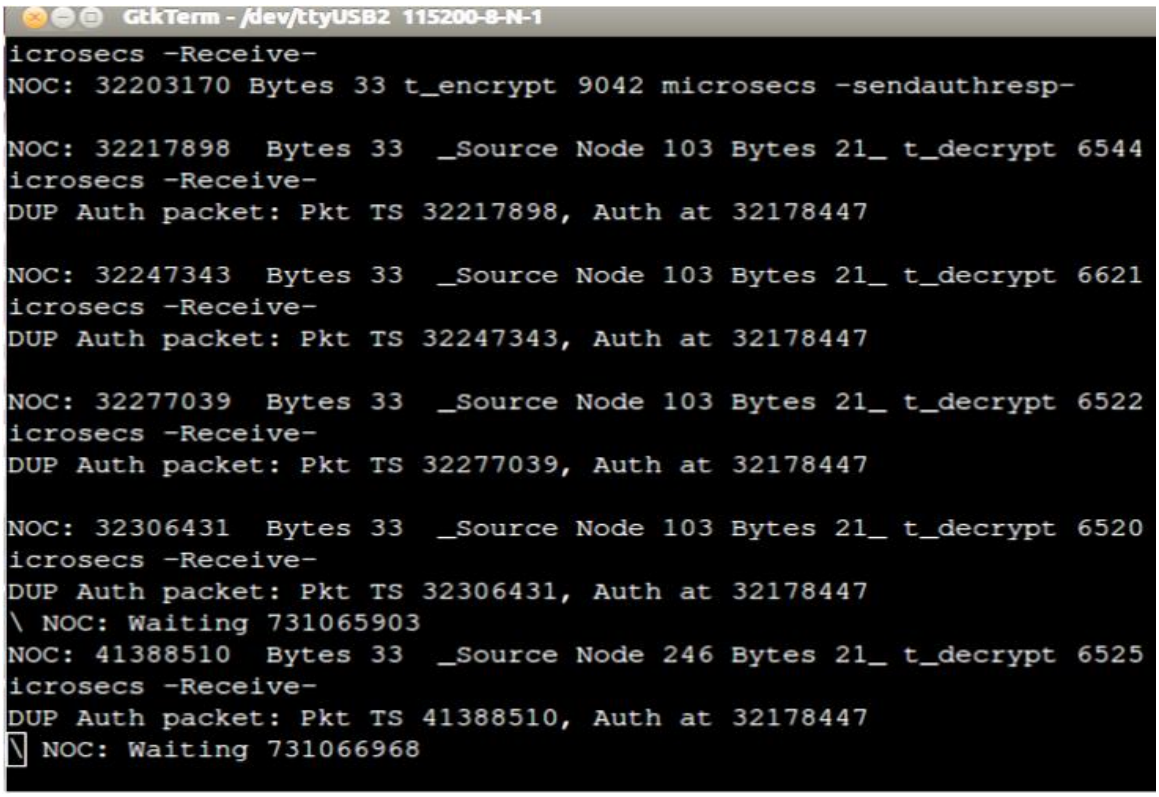

Figure 5-27: Output of the mote labeled NOC indicating duplicate authentication requests from the same node

5.4.1 Sybil attack

Generating a Sybil attack requires that one node be able to take on different identities and masquerade as those nodes. The key to mitigating a Sybil attack is to detect it. In order to implement this attack, we initially wrote a program that could enable the mote to take on different identities and generate authentication requests. The assumption is that a

compromised node has enabled the attacker to gain the keys of the nodes whose IDs will be masqueraded. Using this information, the attacker will attempt to authenticate as the original node.

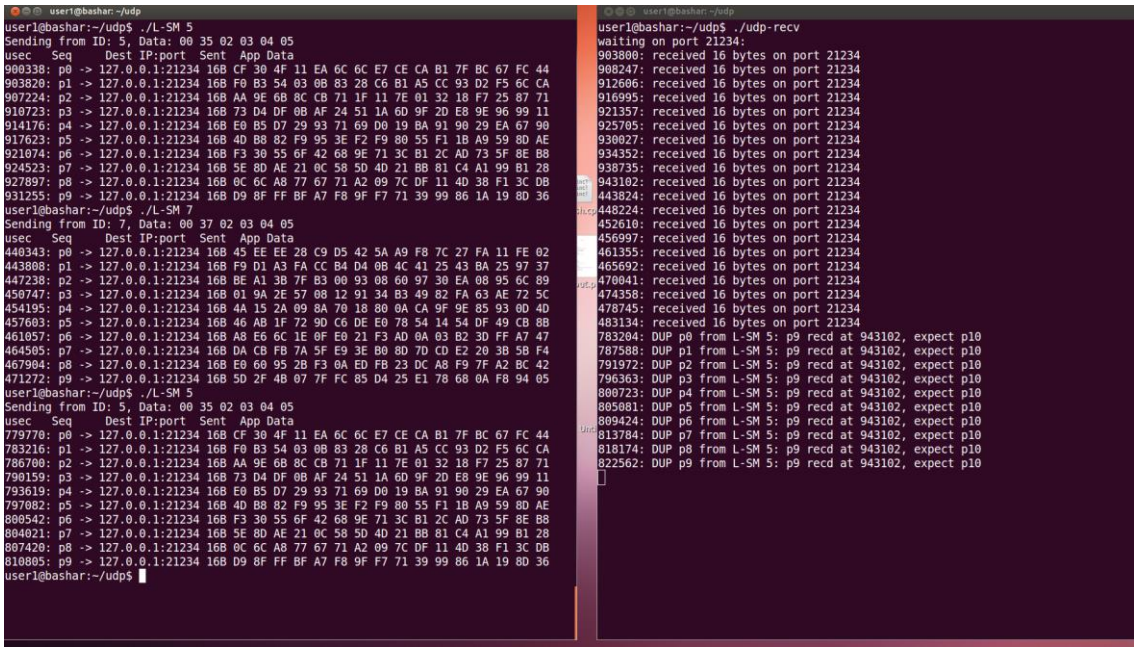

Figure 5-28: Output at a node labeled NOC when a node assumes another node's ID (Sybil attack)

Figure 5-28 shows the output of a test program that was initially used to realise the concept of the Sybil attack. The terminal on the left is the output of the program that is used by the attacker. The test program runs with the ID given to it and transmits ten packets to the receiver (NOC). The NOC tracks the packets received from each node and remembers when that node had authenticated last and what packets it expects from the node. It is therefore able to flag the receipt of unwarranted authentication request packets. In the first attempt, a node with ID successfully authenticates with the NOC, followed by the successful authentication of a node with ID 7. When the attacker masquerades with ID 5 (third attempt) and transmits a packet, the NOC (output on the terminal to the right in Figure 5-28) responds mentioning it expects packet number 10. It provides when the node had authenticated last. This program segments were then included in the programs on the mote and enabled launching a Sybil attack.

The figure 5-29 shows the output of the NOC during an emulated Sybil attack. The attack emulation was done using a TelosB mote, which was programmed to change its ID randomly, between IDs 110 and 115 and attempt to authenticate with the NOC. The NOC key and the gateway key were stored in the memory of the mote, emulating a capture of an

authenticated mote. The first two pairs of messages show successful authentications from node IDs 111 and 112. Node 110 is already authenticated. The captured node attempts to authenticate as node 110 in the third pair of messages. The NOC verifies the request and reports a duplicate (DUP) authentication request. The authentication for node 110 was done at the local time 31380917. The registered serial number of the node to the one that is received does not match (SeN mismatch). The timestamp (TS) expected from node ID 110

```
NOC: 32203170 Bytes 33 Source 111 t_decrypt 8752 mu-secs --Receive--
NOC: 32217898 Bytes 33 t_encrypt 7740 mu-secs --sendauthresp--

NOC: 32218561 Bytes 33 Source 112 t_decrypt 8760 mu-secs --Receive--
NOC: 32232714 Bytes 33 t_encrypt 7753 mu-secs --sendauthresp--

Waiting ... 43107653

NOC: 43108893 Bytes 33 Source 110 t_decrypt 8733 mu-secs --Receive--
NOC: DUP!: 110 Auth at 31380917 SeN mismatch, 110_TS 1981016; Recd_TS 1061893

Waiting ... 43133916

NOC: 43141245 Bytes 33 Source 112 t_decrypt 8785 mu-secs --Receive--
NOC: DUP!: 112 Auth at 32230114 SeN mismatch, 112_TS 33092; Recd_TS 1095254

NOC: 43361964 Bytes 33 Source 113 t_decrypt 8801 mu-secs --Receive--
NOC: 43376916 Bytes 33 t_encrypt 7819 mu-secs --sendauthresp--

Waiting ... 43411137

NOC: 43422817 Bytes 33 Source 112 t_decrypt 8775 mu-secs --Receive--
NOC: DUP!: 112 Auth at 32230114 SeN mismatch, 112_TS 315547; Recd_TS 1376876
```

Figure 5-29: Output at the node labeled NOC, to a Sybil attack

is 1981016 whereas the received TS in the packet is 1061893 and completely out of the allowed time drift margin of 500 microseconds. Similar messages are given when the authentication requests for 112 are repeated (4th and 6th pair of NOC messages). The fifth pair indicates a successful authentication of node with id 113 where all parameters match. That node was just turned ON.

5.5 Summary

This chapter dealt with the implementation of KM-HAN and KM-NAN on Telos-B motes. The functioning of the scheme was verified and several measurements were made. The end-to-end delays were measured for the HAN and NAN scenario in addition to measuring other parameters such as the encryption, decryption times, signature and verification times which form a part of the total end-to-end delay. The network delays were calculated. Along with

the measurements, the attack scenarios were implemented and KM-HAN and KM-NAN were evaluated to check whether they were able to detect the attacks and make sure that the data was not processed. The total time for authentication in a NAN was measured.

Chapter Six: Simulation Study and Protocol Verification

6. Introduction

This chapter discusses the simulations of the HAN and NAN segments and the observations with respect to performance. The simulations were done after the implementations of the security schemes on physical motes. Following the simulation results, details of verifying the group authentication protocol using a security protocol verification tool is discussed. The tool provides a means of verifying the security features of the scheme and determining whether they are vulnerable to attacks.

6.1 The need for simulation

The implementations were done using a small set of physical motes. They yielded typical measurements in terms of cumulative delays. With these measurements as the basis, it was necessary to estimate typical delays in networks of scale. This is the primary need for simulation. It provided us with a means of constructing a large network of nodes, initiating traffic end-to-end and measuring the overall delays. Such measurements were made with the network of nodes in different topologies such as star, mesh and grid.

The second reason is to understand the impact of topology on the availability of the nodes/network when nodes are attacked and rendered inoperative. This was studied specifically in the case of a NAN scenario, where the devices tend to form a more complex network to extend paths to the NOC. Reachability, in such an event, is an important criterion. Simulations provided a means of evaluating the availability of the network/service by estimating the reachability of nodes from the NOC, with and without attacks/failed nodes.

6.2 Tools, limitations & methodology

The simulations were done using the Riverbed Modeler 18.0 from Riverbed Technologies [146]. The modeller provides ZigBee nodes (end nodes, routers, and coordinators) with the IEEE 802.15.4 access protocol support. The modeller does not provide libraries to support the privacy functions, although there is support for secure sockets layer (SSL). Hence a specific application profile to emulate the security scheme was not possible. This was a limitation. We overcome this limitation by modelling the encryption, decryption, signature and verification as delays preceding the packet transmissions.

The ZigBee nodes without application profiles were used to form the networks of a hundred end devices interconnecting to ten coordinator nodes using 30 router nodes. This configuration was used for the NAN. A HAN was built on a similar scale with a hundred end devices. The following sections detail the topologies and the simulation results for the HAN and NAN, respectively.

6.3 Modelling the HAN with the Riverbed Modeller

6.3.1 Simulation set up

The basic scenario for the HAN segment is a campus network where of wireless IoT devices from one wireless network connect to the service offered by remote servers. Figure 6-1 shows the simulation HAN scenario using Riverbed Modeller 18. Two groups of devices, the L group and the H group are connected to their respective group controllers. The group controllers, in turn, are connected to the smart meter (not shown in Figure 6-1). The delay for the packets from the device to the NOC was considered as the performance measure of the security scheme, in that scenario.

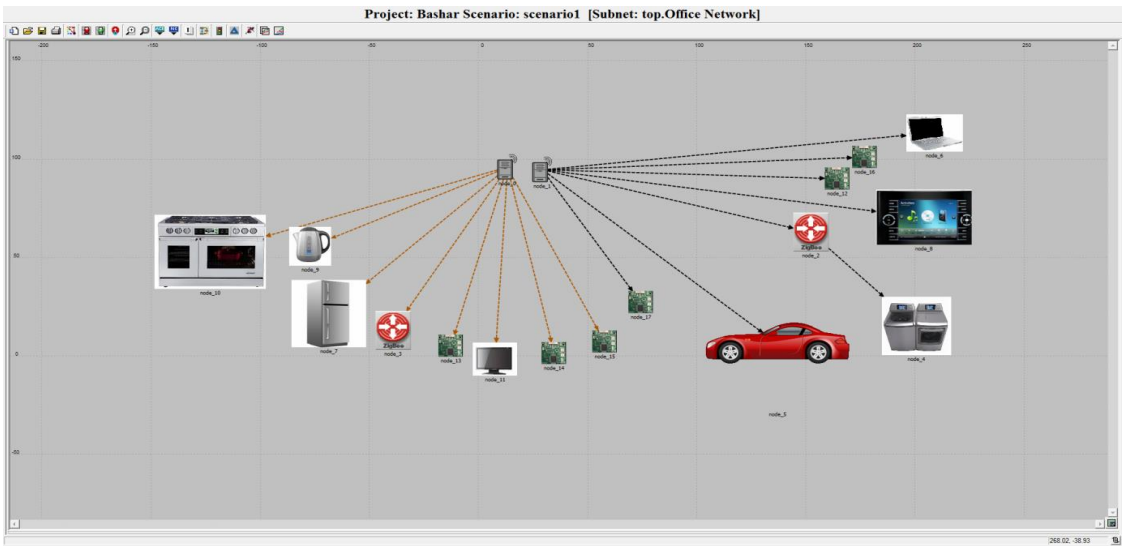

Figure 6-1: The simulated HAN scenario

6.3.2 End-to-end delays

The measured communication delay of the simulated HAN scenario, shown in figure 6-1 was 5 milliseconds. The throughput recorded for the run was 3.76 Kbps (Figure 6-2). Subsequently, additional nodes were created to emulate a replay attack and the delays were observed. The replay attacks were directed to the group controllers. The delay from the

devices to the controllers increased as well as varied substantially. The average value was 3.4 milliseconds with a deviation of +/-1.27 milliseconds (Figure 6-4). In effect, it clearly pointed out the processing load at the group controller causing the increased delay as well as the delay variations.

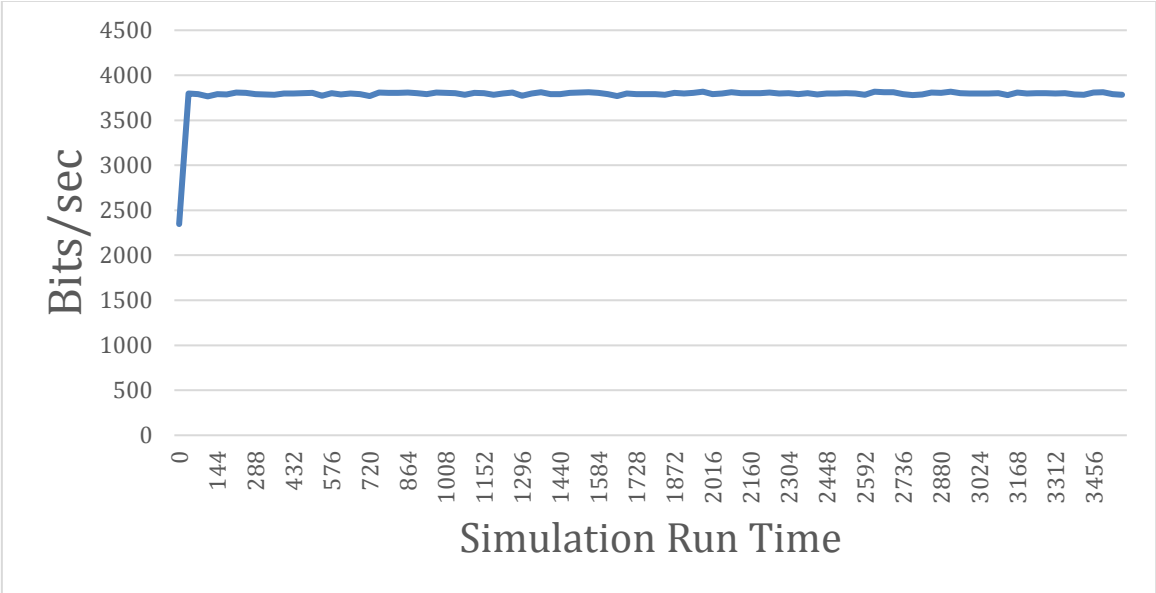

Figure 6-2: Throughputs in the HAN segment

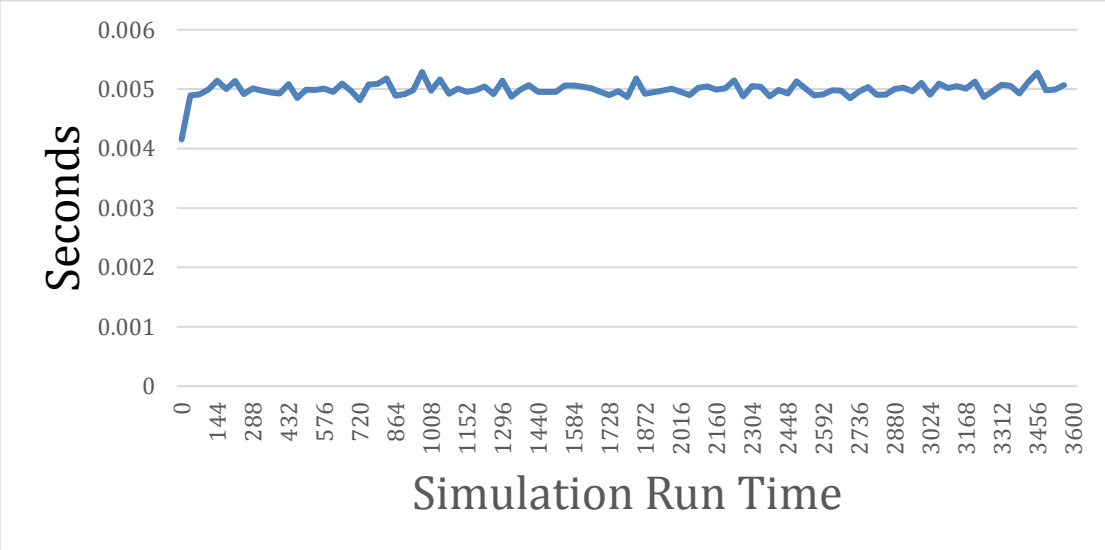

Figure 6-3: End-to-end delay in HAN scenario (seconds)

Similarly, the simulations were run, turning off nodes randomly and measuring the reachability. This emulated the node capture attack, where nodes are incapacitated. In such a case, the number of nodes reachable was measured against the number of failed nodes. The results were plotted (Figure 6-5). Predictably, the plot is a linear negative slope.

6.3.3 Simulation of Replay Attack

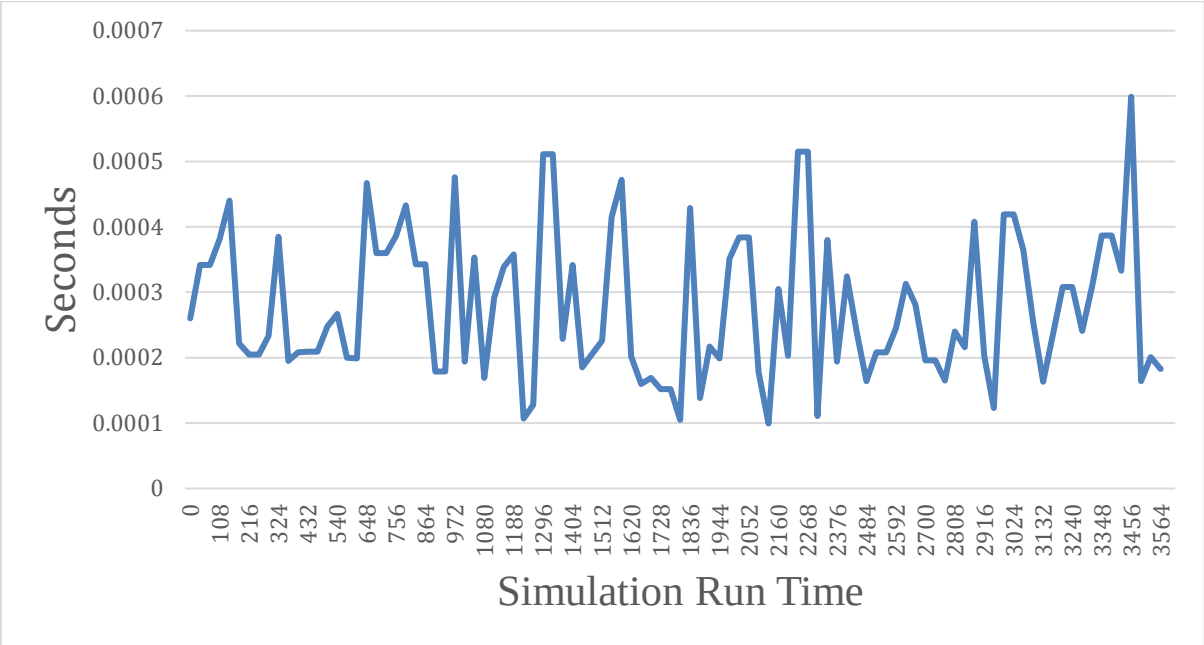

Figure 6-4: Increase in end-to-end delay in the HAN (device to GC) during a replay attack

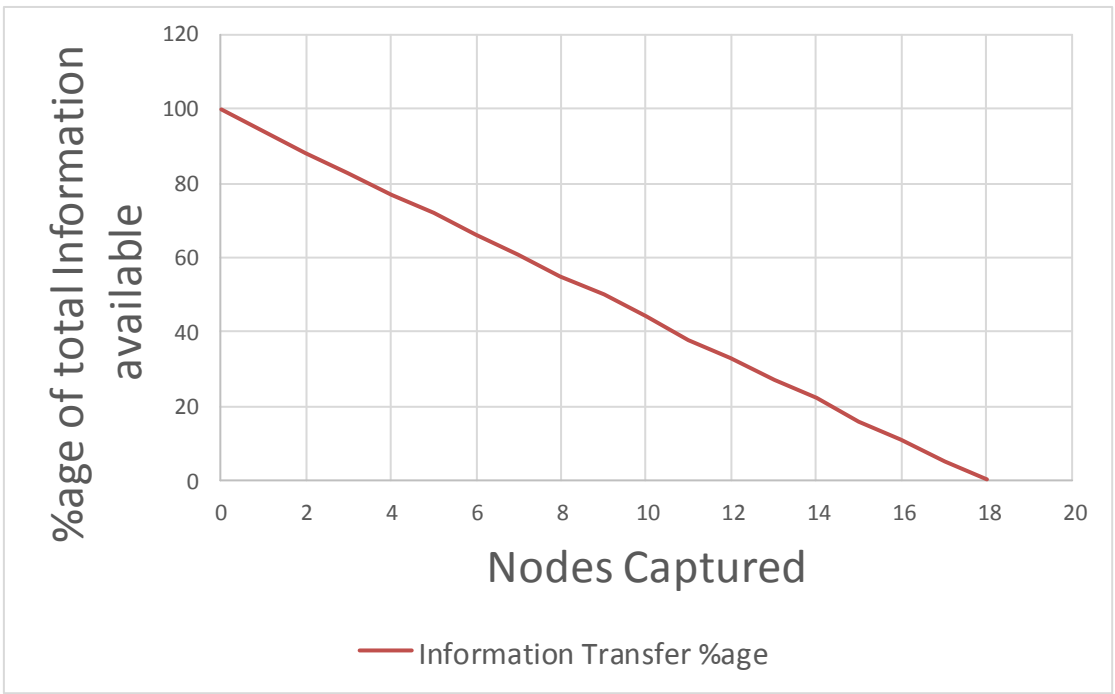

Figure 6-5: Information transfer %age during node captures in the HAN

6.4 Modelling the NAN with the Riverbed Modeller

The simulated network consisted of 10 groups. Each group had one ZigBee Coordinator, 3 ZigBee Routers and 10 ZigBee End Devices (table 6-1). In figures 6-6 and 6-7, we show the modelling of the NAN within two networks using Riverbed Modeller 18 and the simulation parameters. Our aim is to determine the communication performance results of the security group communication scheme in the NAN environment. In particular we determine the delay, throughput, load and other results.

Table 6-1 Simulation Parameters

Simulation time (sec)	3600
Number of Coordinator 3	10
Number of Routers	30
Number of End Devices	100

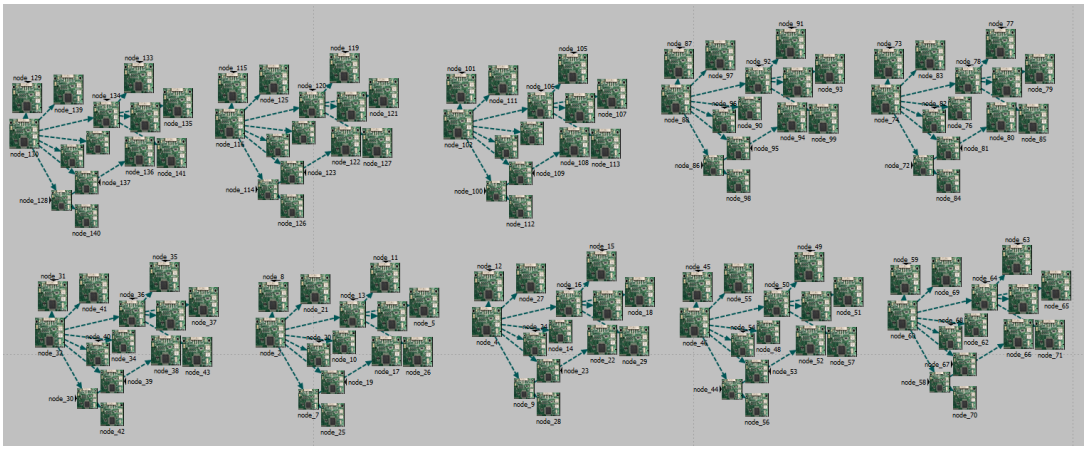

Figure 6-6: Modeling the NAN in the mesh topology

The simulations were carried out in two different network topologies: mesh and star. Moreover, the applications were configured based on the TelosB motes' measurement results. These results are mean values across 10 different random network topologies and group configurations.

6.4.1 Results

The results indicate that the end-to-end delay in a mesh topology has a mean value of 1.2 seconds due to the multi-hop paths whereas the star topology (single hop path) delay value has a lower average at 0.87 seconds.

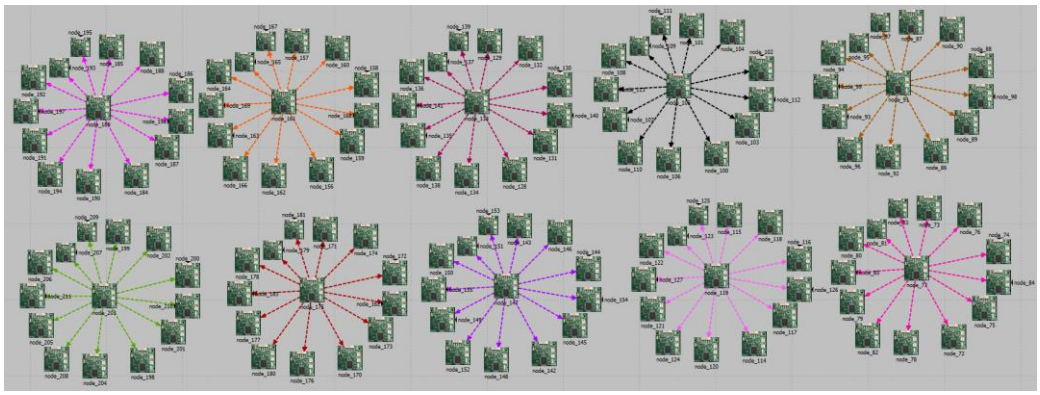

Figure 6-7: Modeling the NAN in a star topology

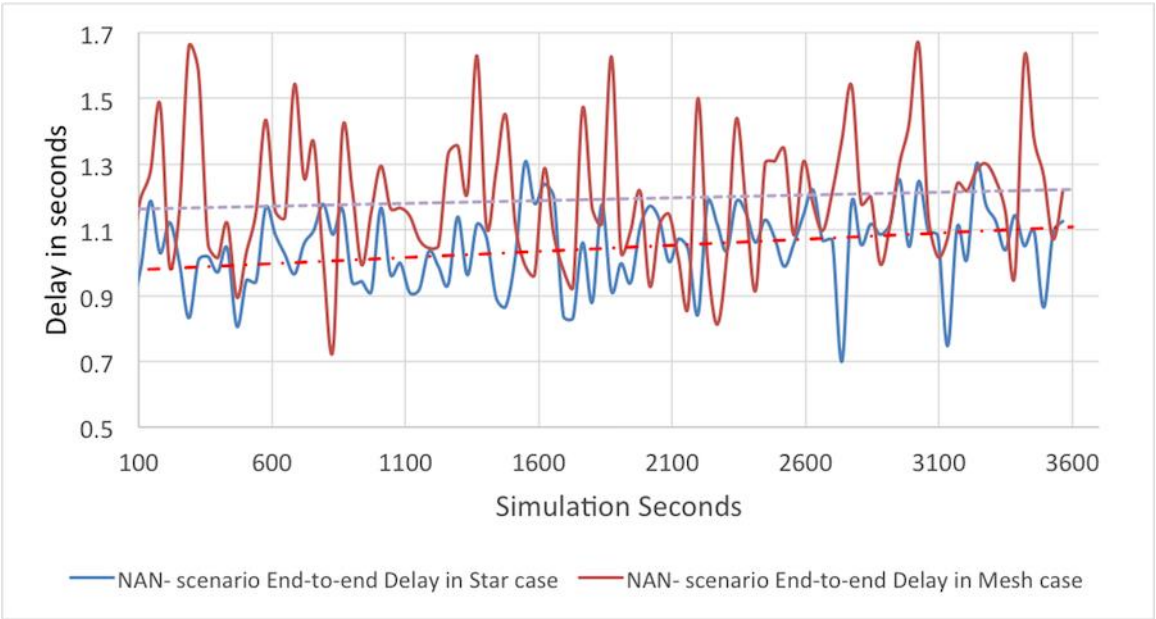

Figure 6-8: End-to-end delay in the NAN scenario

Moreover, the global throughput is a global statistic, and any entity may add to its value. Additionally, the throughput of the network may diminish to unacceptable levels. It provides an overall idea of the general throughput of the NAN simulation scenario. In this simulation the Tree topology had the highest global throughput (bits/second). Figure 6-9 shows that the mesh case had the highest global throughput compared to the star topology.

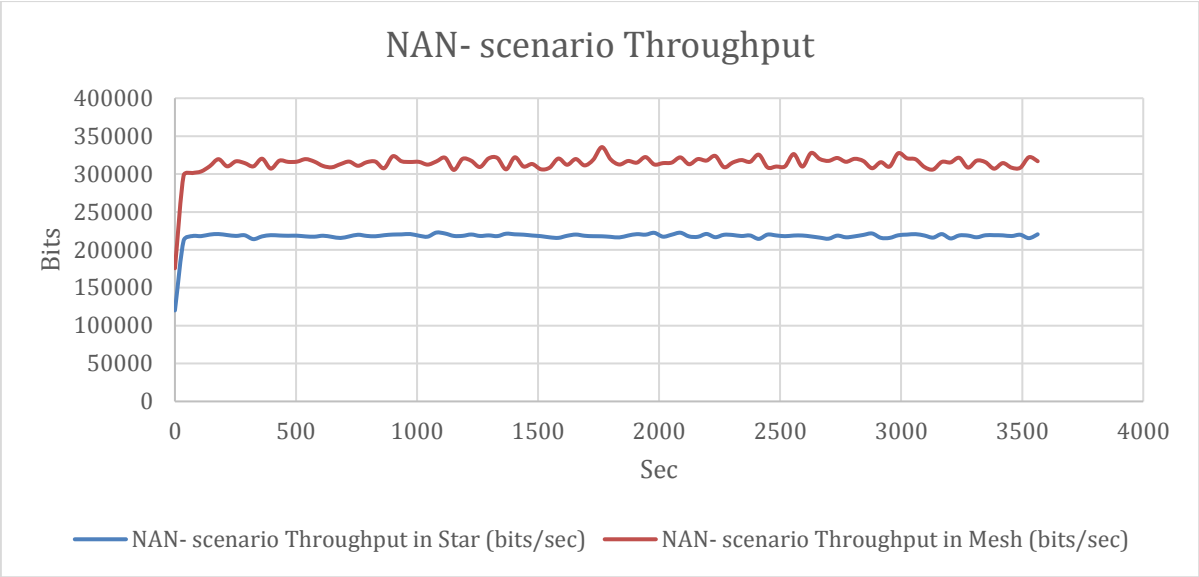

Figure 6-9: Throughputs in the NAN scenario

6.4.2 Node capture attack

In this section, we evaluate our proposed scheme by means of computer simulations. We use the Riverbed Modeller 18 simulation tool [146]. The simulated network consists of 10 groups. Each group has 10 ZigBee Coordinators, 50 ZigBee Routers, and 170 ZigBee End Devices. We generate 10 different mesh topologies and randomly assign nodes into groups. Our aim is to study the impact of the node capture attack on the proposed security of the group communication of Smart Grid. In particular, we determine the number of compromised nodes when an attacker has captured a subset of the nodes. That is, when the attacker has captured one or more nodes, attacker can attack other nodes of the group by exploiting the existing vulnerabilities of the group communication scheme in use. In this session, we compare our proposed secure group communications scheme with the [50] [51] based authentication. We simulate different numbers of captured nodes as follows: from 10 to 100 captured nodes to launch a high-intensity node capture attack. Afterwards, for each of the two approaches [50] [51], in figure 6-10 we determine how many nodes the attacker is able to compromise as a result of the node capture attack.

6.5 Performance study of the KM-NAN and illustration of the KM-NAN's resilience on different communication network topologies in the NAN

We tested our proposed scheme KM-NAN resilience against node capture attacks using different topologies (star, and mesh). The purpose of this is to determine the level of topology independence by simulating node capture attack using various topologies.

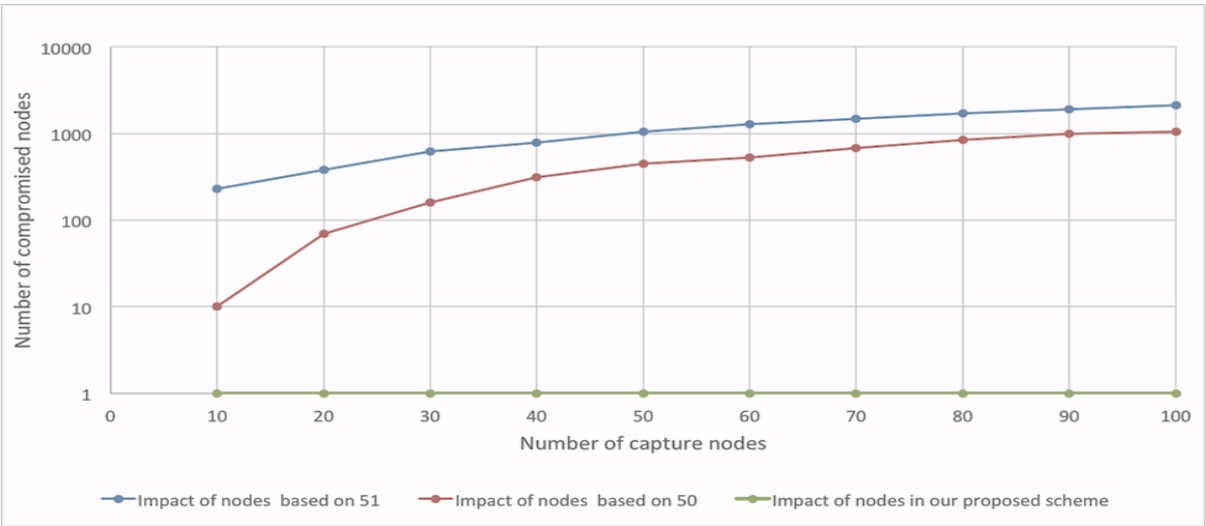

Figure 6-10: Comparing the number of compromised nodes in [50], [51], compared to KM-NAN

Among various attacks in Smart Grids, node capture attack is a severe threat due to unattended nature of the sensor nodes. In a node capture attack threat, an intruder can capture/compromise a node (SM) to get the access to secure cryptographic keys, node identification, communication between node and the network and monitor by re-deploying the compromised node into the network [109, 110]. Once a node is compromised, it allows an intruder to execute various operations/attacks on the network and easily compromise the entire network. According to [111], there are three critical factors as mentioned below, which can lead intruder to compromise the entire network while triggering the node capture threat.

The node deployment/topology play a critical role as it affects the scope of the node capture attacks. Generally, the scope can be defined based on the number of communication links such as, fewer the communication links between neighbouring nodes (i.e. tree topology), the greater the possibility that an intruder can threat entire network. At the other end, higher the communication links between neighbouring nodes (i.e. full/partial mesh topology), the smaller the possibility that an intruder can threat entire network. Therefore, node capture attacks seem to be less effective to mesh topology as compared to star topology, where there is only route from a child node to parent node.

The node density also plays a critical role as it affects the scope of the node capture attacks. A node compromised in the larger density network can threat the larger section of network

Star-based network deployment is characterized by central root node, connected at the highest level in the hierarchy as show in figure 6-34. Top-level node is connected to 2nd

level, whereas 2nd level nodes are connected to 3rd level and so forth. The levels of the star topology can be denoted by $n \in N: = \{1, 2, \ldots N\}$, where the 0^{th}level is for top root.

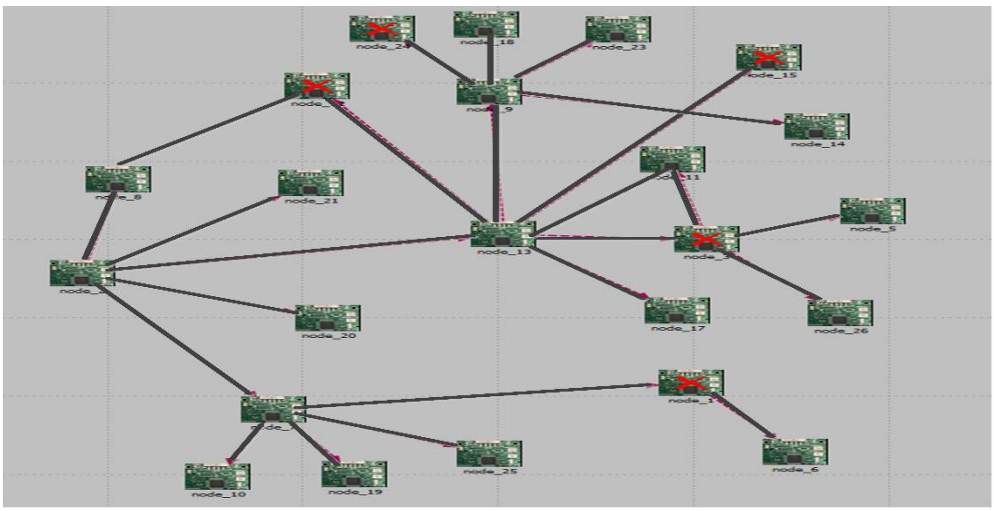

Figure 6-11: Network topology for simulating a node capture attack

In a mesh network deployment, a node in each of the smart meter in NANs will communicate (transmit / receive) data by hoping from one node to another node until either the receiving node is reached or transmitted data reaches the mesh gateway from node to node. The data from the gateway is typically transmitted to central data station via a backhaul network. The GWs are connected as start topology to backhaul network and SMs are connected as partial mesh as each SM is not directly connected to each of the other SM in the network.

6.5.1 Network Security Model

It is considered that a group of Smart Meters (SMs) with one SM taking on the role of a gateway (GW) are interconnected in a manner that some SMs have a multi hop path to the gateway (GW). The GW interconnects to the central authentication point over the backhaul network. SMs that are children of other SMs use the multi-hop path to reach the GW node as shown in figure 6-33. It is assumed the NANs use encrypted communication based on random redistribution key approach. Each node is configured with a set of (K) different keys from a key pool of (P) keys. A pair of nodes with the range (R) can initiate a secure connectivity only if appropriate assigned keys are shared between them. It is also assumed that every node is deployed in a promiscuous approach and is able to recognize sources of all messages initiating from its neighboring nodes. Based on this assumption, each node will inspect only the source node ID therefore this assumption will not incur significant communication overhead.

6.5.2 Network Threat Model and Performance Metrics

It is assumed that an intruder can physical capture a limited number of SM nodes in a target region ($\mathbb{R}$) and turn them into threat node by extracting secure keys and measured data for NAN. Considering (C) represents a set of nodes captured by intruder and for each node in set (C), a set of secure key (C_k) is considered as compromised. It also compromises all the links between nodes $(n_i, n_j \in N)$ in region ($\mathbb{R}$) to be exposed to intruder as a threat. It allows intruder to clone a capture node and collaboratively deploy them in the NAN. The resiliency of NAN star and mesh topology in Smart Grid against NC attack will be evaluated based on reachability of total nodes in the network after node captures.

6.5.3 Network Topology and Simulation Setup

To carry out evaluation of node capture attacks, two NAN topologies star and mesh. The NAN made of (N) nodes is deployed over a region of ($A \subseteq \mathbb{R}$). Considering the fact that SM nodes in AMI will be deployed fixed, therefore a static network deployment has been assumed. Each node is assumed to be equipped with an omni-directional radio with fixed communication range (R) based on Zigbee standard. To evaluate the resiliency of star and partial mesh topology in NAN in smart grid based on Zigbee network against node capture attack, Riverbed simulation tool [146] has been considered. In both star and mesh topology simulation of NAN, Zigbee network consist of coordinator (Gateway) and end devices (SMs).

Case 1 – Star Topology: In this case, Zigbee nodes are deployed as star topology for NAN. In a NAN tree topology, there is a relationship of root (GW) and child (SM) node. The child node can communicate only with their parent node whereas the parents can communicate with their child and their own parent node. Therefore, child node (SM) always depends on the parent node for data availability, as there are no alternative routes for SM node to get target.

Case 2 – Mesh Topology: In this case, Zigbee nodes are deployed as partial mesh topology for NAN. NAN Mesh topology is more flexible as it can allow each node to choose between multiple routes to transmit/receive data to the target location. It also allows the network to self-heal and search for other paths and so that data can be relay through.

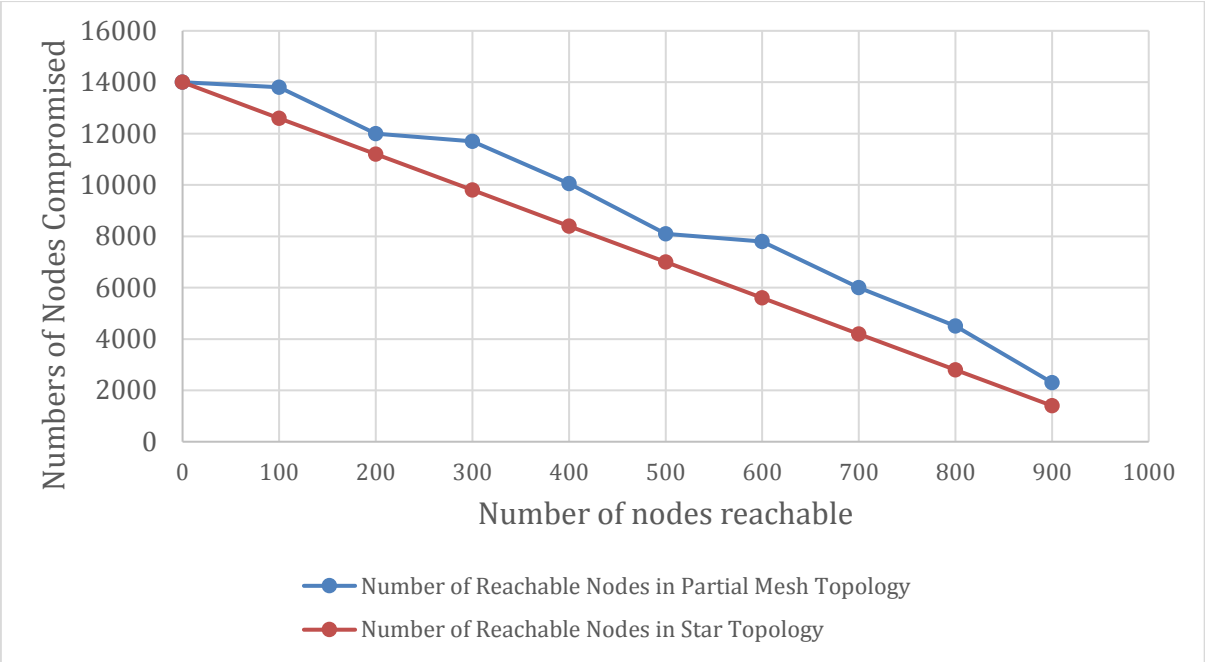

Figure 6-12: Reachability of nodes after node captures/failures

Node capture attacks in KM-NAN can significantly degrade network reachability. Based on the simulation results in figure 6-12, we observe that partial mesh topology is more resilient topology as compared to star topology for KM-NAN.

6.6 Summary of Simulations

We have resorted to simulations to explore the scale of end-to-end delays in the HAN and NAN scenario with the security overheads introduced by KM-HAN and KM-NAN, when their respective scenarios are scaled up to hundreds of nodes. Typical network configurations included ten coordinators, thirty routers and a hundred nodes. End-to-end delay measurements were made on both KM-HAN and KM-NAN. In case of HAN, we observe that the end-to-end delay from the devices to the SM are 5 milliseconds and that for the NAN in the two topologies are 0.89 seconds and 1.2 seconds, respectively, for star and mesh topologies. Subsequently, the increase in the end-to-end delay as a consequence of replay attacks is measured. Node capture attacks are simulated with random node failures and the number of nodes reachable is measured both for HAN and NAN.

6.7 Verifying security parameters

The final step after the implementation and simulations is the verification of the security scheme. There are several automatic security protocol verification tools such as CoProVe [159], AVISPA [160], ProVerif [161] and Athena [162]. Scyther is a more recent tool that improves on most of the approaches with its speed and features [163]. It is designed to formally analyse security protocols, their security requirements and potential vulnerabilities. It is designed under the perfect or unbreakable encryption assumption, which means that an adversary learns nothing from an encrypted message unless he knows the decryption key [164].

6.7.1 Language of Scyther

Scyther has its own specification language to describe protocols, roles, types of parameters, sending and receiving messages and so on. The code segment in figure 6-13 illustrates the various parameters and elements that we will use in our protocol formalization, including the definitions of predefined type, *usertype*, symmetric key, asymmetric keys, *hashfunction*, *role*, *protocol*, and message sending and receiving.

The protocol named P0 is between two communicating entities, an Initiator and a Responder. The entities are declared as roles I and R. The keyword fresh defines a value that exists in the session it is generated and Nonce is a keyword that defines a value that remains constant during the whole session. *var* defines a variable used to store a value received from the sender. *T* here are two types of keys, symmetric and asymmetric. A symmetric key defined by $k(I, R)$ is a long-term value shared between *A* and *B*, and a message *Ni* encrypted by it is described as $\{Ni\}k(I,R)$. Asymmetric keys are a key pair, including a private key denoted by ($sk(I)$) and a public key ($pk(I)$). *hashfunction* is a keyword used to define a hash function. If *H* is declared as a *hashfunction*, message $H(Nj)$ signed by *R* can be denoted by $\{H(Nj)\}sk(R)$. Message sending and receiving in Scyther can be specified by the pair $send(s,r,m)$ and $recv(s,r,m)$, where *s* is a sender, *r* is a receiver and *m* is a message. The *send* and *recv* functions are normally tagged with a number to indicate the corresponding messages. For example, a *send_1(I,R,message)* sent from *I* corresponds with a *recv_1(I, R, message)* in *R*. There are several other keywords and features in the language, but we have discussed here

only a few important ones that are mostly used in our verifications.

```
/*
* Secrecy protocol
*
* Uses symmetric encryption
*/

//The protocol description

     protocol  P0(I, R)
     {
     role I
     {
     fresh Ni: Nonce;

     send_1(I,R, {I,Ni}k(I,R) );
     claim_i(I,Secret,Ni);
     }

     role R
     {
     var Ni: Nonce;

     recv_1(I,R, {I,Ni}k(I,R) );
     claim_r(R,Secret,Ni);
     }
     }
```

Figure 6-13: Example Scyther code showing a two-agent protocol using symmetric keys

6.7.2 Specifying security requirements in Scyther

Having specified the security protocol actions, the security requirements that the protocol satisfies require to be checked. Scyther provides two keywords *claim* and *match* to specify security requirements. The security claims available are *Alive, Nisynch, Secret* and *Commit*. *Alive* is used to ensure that a party has executed some events (*claim (I, Alive)*). *Nisynch* indicates that all messages sent by the sender have been received by the recipient, e.g., (*claim (I, Nisynch)*). Any term that is intended to be a secret from an adversary is specified as *claim(R,Secret,Ni),* where the term Ni is intended to be a secret. Figure 6-13 illustrates this in the context of the simple protocol. Commit is used to make a commitment between the parties; *claim(I,R,Commit,TS)* means that role *I* promises *TS* to role *R*.

In contrast to *claim, match* is used for two different purposes. This is similar to the "=" operator and its use for assigning a value to a variable as well as to check equality. In

Scyther, a dependency on an equality (e.g., *if (x == y), then…*) for executing following events can be specified by using *match(v1, v2)*. The events following that statement will be executed only if the values of *v1* and *v2* match. The other use is to assign a value. If the value of *v2* is to be assigned to *v1, match (v1, v2)* will provide for it. Using these two keyword constructs, the security requirements are specified for checks.

6.7.3 Executing the security protocol in Scyther

Scyther tool provides a windowed interface to run the protocol specification. The specifications are stored in security protocol description files (`.spdl` files). These files are loaded into the windows interface, which interprets the specification and checks for the security requirements. The output is windows based and indicates whether the claims made have passed or there is a potential attack available. If available, the tool provides a visual summary of the run and illustrates how the attack is successful.

The number of runs can be configured. Typically, the number of runs is set to five. The authors suggest that the number of runs should be at least one more than the number of roles [158]. If Scyther is able to clearly establish that the claims have passed, it responds with "`No attacks`" against the claims. If it is not able to commit there are no attacks, with the available number of runs (bounded state), it displays "`no attacks within bounds`". This indicates that the protocol could require an higher number of runs or an unbounded run.

6.7.4 Verification of KM-HAN and KM-NAN

Both these protocols were specified and run. In the case of KM-HAN, three roles are used, one each for the end device, the group gateway and the smart meter. The objective is to ensure that the data generated at the device is kept a secret until it reaches the smart meter. The claim for data being kept a secret is made in the protocol description language. The verification is run for the default number of runs configured as well as unbounded runs. The runs were made for both groups L-group and H-group. The output for the unbounded runs indicates that there are no attacks for the L-group (figure 6-15) and no attack within bounds for the H-group (figure 6-14).

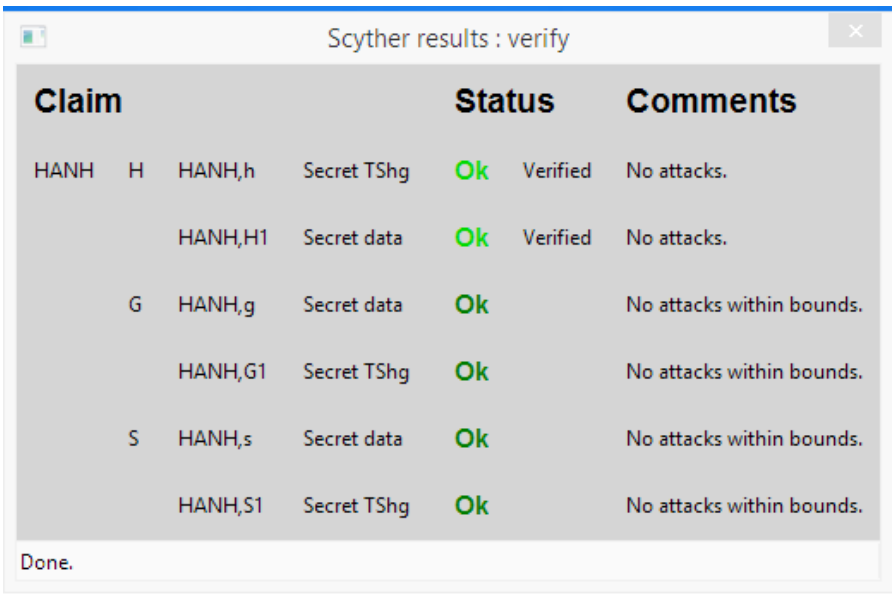

Figure 6-14: Output of unbounded runs for the H-group in the HAN

In the case of KM-NAN, there are four roles, one each for the end smart meter, the intermediate smart meter, the gateway smart meter and the NOC. The elements that require to be secret are – the data from the end SM, intended for the NOC, the gateway key sent by the NOC to the end SM and the authentication value sent by the gateway to the end SM. The verification was done for these claims as well as all claims were automatically verified in separate runs. Every verification run consisting of the default number of runs (five), took over 5 – 7 minutes. The results indicated the status as OK and that there were no attacks within bounds.

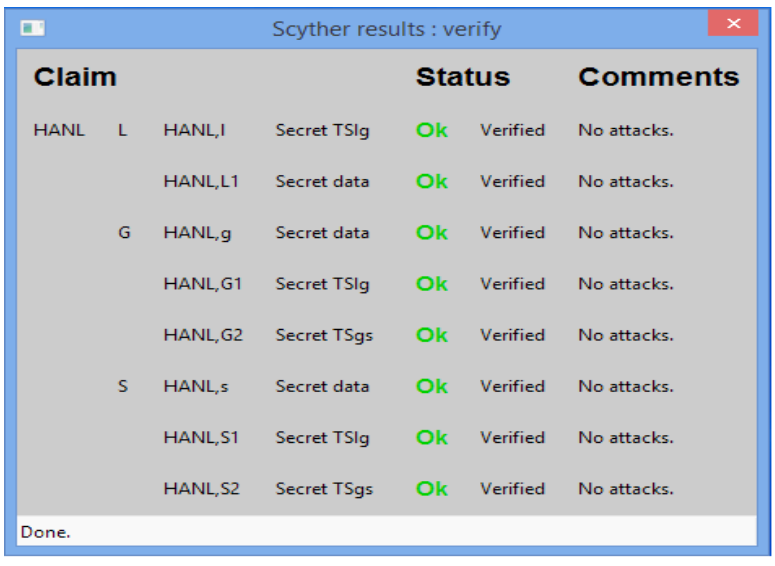

Figure 6-15: Output of unbounded runs for the L-group in the HAN

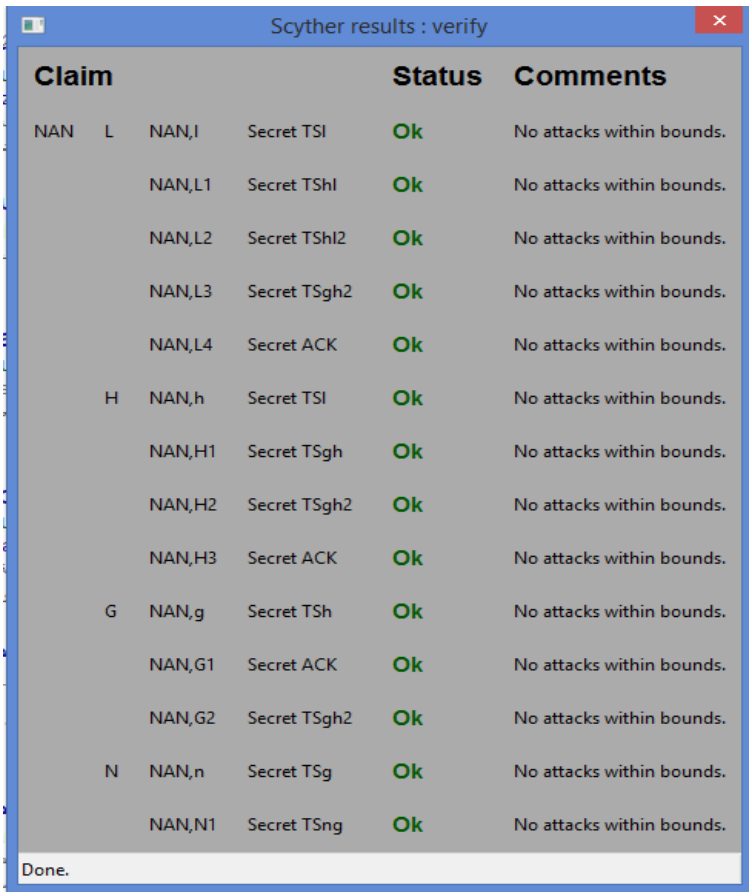

Figure 6-16: Output of the runs for KM-NAN

Figure 6-16 is the output of the verification run for the KM-NAN. While the status indicates OK, the verification indicates that there are no attacks within the bounds of the number of runs.

6.8 Summary

In this chapter we have presented two specific efforts – simulation studies of our proposal in the context of a large network and verifying the security of our proposed scheme using a security protocol verification tool. The simulation studies illustrated that the end-to-end delays in the network remain fairly consistent in the case of the HAN. The increase in the delays in the presence of the replay attacks was measured and found to be not very high. In case of node capture attacks, the number of nodes unreachable were linear. This was due the inherent star connectivity of the HAN segment.

In the case of the NAN, the topology made a significant difference in terms of end-to-end delay. It impacted the delays observed during attacks. However, it demonstrated that a mesh/partial mesh topology is more resilient in the context of a node capture attack, compared to a star topology. When the reachability of the KM-NAN in the presence of node

capture attacks was compared with two other schemes [50], [51], KM-NAN performed better than both the schemes.

The security claims of KM-HAN and KM-NAN were evaluated using the Scyther tool. Both the schemes verified as OK for the claims. However, they will require to be verified with a larger number of runs to ensure that there are indeed no attacks and verify them completely.

Chapter Seven: Conclusion and Future Work

7. Introduction

This thesis has presented a new key management scheme for Communication Layer in the Smart Grid (KMS-CL Smart Grid), to fulfil the proactive security needs of Smart Grids. This scheme is an integration of different communication layers of the SG including HAN and NAN. The aim of the scheme is to provide a key management for a large scale SG infrastructure based on the communication layer requirements, which can provide end-to-end secure communication, resilience against node capture and replay attacks, Sybil attack and lightweight authentication protocol. This chapter provides a summary of thesis and mentions the future research in the subject area. This chapter has organized as follows. First we present the contributions of the research in Section 7.1. A summary of the KMS-CL Smart Grid scheme and thesis contributions is presented in Section 7.2. Several of research gaps have been highlighted in future work section 7.3. Finally, the conclusions are in Section 7.4.

7.1 Contributions

In completing the basic research objectives mentioned in section 1.5, we make the five following contributions.

1. **Key management framework for a HAN, based on the HAN requirements:**

   Our proposed key management solution is designed for fulfilling HAN security requirements. Towards that purpose we identify the various devices in a home, which are networked. After that we group the devices based on operational/functional factors such as their power consumption and the control functions required. Then, we identify the resource availability on each device and assess the impact of an attack on the device type. We then list the security requirements of each device group. Based on that we design a secure key management interaction scheme for the groups in HAN. The protocol has been evaluated by an implementation using TelosB motes and simulating a large scale SG using Riverbed Modeler 18.0. The evaluation results show an improvement in terms

of data confidentiality and resilience against node capture attacks. A detail of this security analysis is detailed in in chapter five.

2. **Key management framework for a NAN, based on the NAN network requirements**

The main components in NAN segment are smart meters, which form a large-scale network. Therefore, to manage a large scale NAN, organising the NAN into groups of SMs is considered in our scheme. Group key management for NAN has been proposed. In order to achieve a secure end-to-end communication we assign a unique key to each node in the group. This unique key is shared only with the utility company server, and sends encrypted data through other nodes to the utility company Server without decryption at any non-utility company server. We have shown in chapter 4 that using this technique we achieve end-to-end confidentiality.

3. **A light-weight authentication scheme for devices in the NAN**

We have proposed a new, secure, group authentication scheme for NAN for Smart Grid. The main feature of our scheme is the ability to address security of all communication, which takes place in the network. A detailed of the scheme found in chapter 4 of this thesis.

4. **Implementation and evaluation of the key management and authentication scheme in typical Smart Grid scenarios using real environment by using TelosB motes, in chapter 5**

5. **Performance study of the proposed KM-NAN and illustration of the KM-NAN's resilience on different communication network topologies in the NAN.**

Node capture attacks in the proposed KM-NAN can significantly threaten security and degrade network performance. Based on the simulation results, it is identified that partial mesh topology is more resilient topology as compared to star topology for KM-NAN against node capture attacks. As compared to KM-NAN star, KM-NAN mesh topology is more flexible as it can allow smart nodes to choose between multiple routes to transmit/receive data to the target location, if one of the

node(s) compromised. Due to the flexibility offered by mesh topology, it is not only resilient but also an ideal solution, easy to deploy in KM-NAN.

7.2 Future work

In this section, several of research issues have been highlighted for future work including

7.2.1 Prevention in the Wide Area Network (WAN)

It is a core network that covers a broad geographical area and uses communication circuits to connect several subsystems and smart meters with a control centre that is far from the subsystem and customer-side network [93]. In addition, it has to support the applications and the corresponding requirements in each of the different networks it connects. The WAN can connect using WiMAX, 3G/GSM/LTE or fibre optics. In the WAN, the characteristics and security requirements are fairly complex due to the hosts of grid applications and applications that are related to the operation of a utility, such as SCADA [152].

Because WANs have enormous network traffic, traditional security solutions are not efficient for handling such a large data flow. A common issue exists regarding how cryptographic keys can manage a large load of data as well as how to balance the scale of traffic, analysis and data. In addition, logically, the overhead and the load on it increases as the number of hosts increases [153].

7.2.2 Economics and Energy Storage Technology issues

One of the challenges in the development of a Smart Grid is to balance all of the critical variables associated with the dynamic load control powered by ever-increasing renewable sources. The requirement to balance critical variables can be achieved through energy storage technology throughout the smart grid. With the advancement in smart grids, energy storage has become a key technology to develop a low-carbon physical-cyber power system [154]. An energy storage system can help to supply more flexibility and balance to the smart grid, providing a back-up to intermittent renewable energy and improving the management of distribution networks, reducing costs and improving energy efficiency and grid management. However, the development and deployment of energy storage technology has various barriers: technological barriers (increasing capacities and efficiencies, developing new technology for local and decentralised systems, integration with smart grid), market

and regulatory barriers (creating appropriate market signals and regulations), and strategic barriers (systematic and holistic approach). In addition to that, the main challenge in the development of energy storage is an economic one, which will be a main driver of how soon distributed storage solutions are adopted in a smart grid. The economic challenge can vary from case to case depending on various parameters, including where the storage is needed, its generation, transmission, distribution or consumer end.

7.2.3 Big Data Challenges

The upgrade of a traditional power grid into a Smart Grid provides utility service providers with exceptional capabilities for forecasting demand, consumer usage patterns, avoiding blackouts, improving unit assurance, energy market prices, control and maintenance data and more[155]. However, these advancements also generate exceptional volumes of data, speed and complexity, and it is expected that by 2020 the number of smart meters will grow rapidly, for example, to 240 million in Europe, 150 million in North America, 400 million in China and 60 million in Japan. The dynamic nature of the Smart Grid means that it requires constant adjustment based on the real-time information. Therefore, Smart Grid data architecture must be capable of coping with big data volumes for real-time response and sophisticated data analytics [156].

7.2.4 Substation Distribution/Automation System

This is another important system, which is directly involved in substations towards the consumer and smart meters via AMI. Communication and monitoring systems will incorporate demand response and real-time pricing systems in order to improve the system reliability. Moreover, increasing Smart Grid communication integration through merging the current distinct hardware and software systems decreases cost and lowers redundancy [55].

The substation automation system helps to enhance the system reliability and communication between substations. To ensure a seamless data communication and information exchange across all the distribution networks, the substation automation system is aimed to define the scope to the whole network and provide compatibility with the common information model (CIM) for system reliability and communication [157]. Due to the heterogeneity and interoperability nature of the grid systems, the Common Information

Models (CIM) provides a standardised format to allow reliable communication within grid systems [26].

7.3 Conclusion

In this thesis, we have proposed a security scheme for communication layer in Smart Grid in particularly for a HAN and a NAN. The enhanced scheme can be used to enable secure group-to-group communication of low-capability Smart Grid devices and to mitigate the negative effects of physical attacks and node capture attacks. Moreover, we proposed a groups of SMs in a Neighbourhood Area Network that enable entire groups to authenticate themselves, rather than on at a time. In particular, the scenario of a multi-hop network is considered where the nodes require multiple hops to communicate with the NOC, which is the entity that issues the keys. Two topology scenarios, star-star and mesh are considered and separate authentication processes are defined for their operation. We propose a hierarchical control scheme for authentication; all nodes initially authenticate with the NOC and subsequently, the group gateway autonomously issues an authentication token to the authenticated members in its group. We mention how the proposed approach is two-way secure as both involved parties, the group controller and the smart meters, are able to successfully verify each other.

The authentication scheme was implemented on real world environment using TelosB motes. We found out that the average encryption and decryption times on end nodes are 6 ms and 6.2 ms, on intermediate nodes (authenticated forwarding), including the GW node 3.9 ms and 4.2 ms and on the NOC 8.2 ms and 6.5 ms. The entire authentication process took 331 ms.

We have also studied the performance of our scheme against node capture attacks, replay attacks and Sybil attack. Our results show that significant security improvements over traditional approaches can be achieved. Moreover, we have studied node capture attacks in the proposed KM-NAN can significantly degrade threaten network security. We identify that partial mesh topology is more resilient topology as compared to star topology for NAN, against node capture attacks. As compared to KM-NAN star, KM-NAN mesh topology is more flexible as it can allow smart nodes to choose between multiple routes to transmit/receive data to the target location, if one of the node(s) compromised. Due to the

flexibility offered by mesh topology, it is not only resilient but also an ideal solution with easy to deploy in KM-NAN.

A security protocol verification tool, Scyther, was used to verify KM-HAN and KM-NAN security schemes. The tool indicates that the security scheme is verifies against any attacks that it can generate. This validates the security scheme, in addition to the analysis and implementation.

Appendix

Publications

B. Alohali, K. Kifayat, Q. Shi, and W. Hurst, "Group Authentication Scheme for Neighbourhood Area Networks (NANs) in Smart Grids," *Journal of Sensor and Actuator Networks*, vol. 5, p. 9, 2016.

B. Alohali, K. Kifayat, Q. Shi, and W. Hurst, "A Survey on Cryptography Key Management Schemes for Smart Grid," *Journal of Computer Sciences and Applications*, vol. 3, pp. 27-39, 2015.

M. Merabti, B. Alohali, and K. Kifayat, "A New Key Management Scheme Based on Smart Grid Requirements." Advances in Information Science and Computer Engineering ISBN: ISBN: 978-1-61804-276-7, 2015.

B. Alohali, M. Merabti, and K. Kifayat, "A Cloud of Things (CoT) Based Security for Home Area Network (HAN) in the Smart Grid," in Next Generation Mobile Apps, Services and Technologies (NGMAST), 2014 Eighth International Conference on, 2014, pp. 326-330.

B. Alohali, M. Merabti, and K. Kifayat, "A secure scheme for a smart house based on Cloud of Things (CoT)," in *Computer Science and Electronic Engineering Conference (CEEC), 2014 6th*, 2014, pp. 115-120.

B. Alohali, M. Merabti, and K. Kifayat, "A New Key Management Scheme for Home Area Network (HAN) In Smart Grid." 15 Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet 2014), Liverpool, UK, 23-24 June 2014.

Alohali, B., Merabti, M., & Kifayat, K. Key Management in Smart Grid: A Survey. Proceedings of the PGNet 2014, Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting (PGNet 2013), Liverpool, UK, 24-25 June 2013.

8. References

[1] M. Nabeel, J. Zage, S. Kerr, E. Bertino, N. A. Kulatunga, U. S. Navaratne*, et al.*, "Cryptographic Key Management for Smart Power Grids-Approaches and Issues," *arXiv preprint arXiv:1206.3880,* 2012.

[2] Y. Ye, Q. Yi, H. Sharif, and D. Tipper, "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges," *Communications Surveys & Tutorials, IEEE,* vol. 15, pp. 5-20, 2013.

[3] E. D. Knapp and J. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*: Syngress, 2011.

[4] Y. Xiao, *Security and Privacy in Smart Grids*: Taylor & Francis, 2013.

[5] W. Meng, R. Ma, and H.-H. Chen, "Smart grid neighborhood area networks: a survey," *Network, IEEE,* vol. 28, pp. 24-32, 2014.

[6] E. D. Knapp and R. Samani, "Chapter 1 - What is the Smart Grid?," in *Applied Cyber Security and the Smart Grid*, ed Boston: Syngress, 2013, pp. 1-15.

[7] Q. C. Zhong and T. Hornik, *Control of Power Inverters in Renewable Energy and Smart Grid Integration*: Wiley, 2013.

[8] X. Lv, Y. Mu, and H. Li, "Key management for Smart Grid based on asymmetric key-wrapping," *International Journal of Computer Mathematics,* vol. 92, pp. 498-512, 2015/03/04 2014.

[9] krebsonsecurity. (3/5/2013). *FBI: Smart Meter Hacks Likely to Spread*. Available: https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

[10] N. Saxena and B. Choi, "State of the Art Authentication, Access Control, and Secure Integration in Smart Grid," *Energies,* vol. 8, p. 11883, 2015.

[11] S. Ruj and A. Nayak, "A Decentralized Security Framework for Data Aggregation and Access Control in Smart Grids," *Smart Grid, IEEE Transactions on,* vol. 4, pp. 196-205, 2013.

[12] M. Jung, T. Hofer, S. Dobelt, G. Kienesberger, F. Judex, and W. Kastner, "Access control for a Smart Grid SOA," in *Internet Technology And Secured Transactions, 2012 International Conferece For*, 2012, pp. 281-287.

[13] M. B. Line, I. A. Tondel, and M. G. Jaatun, "Cyber security challenges in Smart Grids," in *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*, 2011, pp. 1-8.

[14] E. Pallotti and F. Mangiatordi, "Smart grid cyber security requirements," in *Environment and Electrical Engineering (EEEIC), 2011 10th International Conference on*, 2011, pp. 1-4.

[15] M. Yilin, T. H. H. Kim, K. Brancik, D. Dickinson, L. Heejo, A. Perrig*, et al.*, "Cyber–Physical Security of a Smart Grid Infrastructure," *Proceedings of the IEEE,* vol. 100, pp. 195-209, 2012.

[16] S. Rautmare, "SCADA system security: Challenges and recommendations," in *India Conference (INDICON), 2011 Annual IEEE*, 2011, pp. 1-4.

[17] L. TOMKIW. (2016, 8/1/2016). *Russia-Ukraine Cyberattack Update: Security Company Links Moscow Hacker Group To Electricity Shut Down*. Available: http://www.ibtimes.com/russia-ukraine-cyberattack-update-security-company-links-moscow-hacker-group-2256634

[18] T. M. Chen and S. Abu-Nimeh, "Lessons from Stuxnet," *Computer,* vol. 44, pp. 91-93, 2011.

[19] T. A. Rizzetti, A. S. Rodrigues, B. M. d. Silva, B. A. Rizzetti, P. Wessel, and L. N. Canha, "Security of communications on a high availability mesh network applied in Smart Grids," in *Power Engineering Conference (UPEC), 2015 50th International Universities*, 2015, pp. 1-6.

[20] M. Wan, W. Shang, P. Zeng, and J. Zhao, "SRDA: A Secure Routing and Data Aggregation Approach for Wireless Smart Meter," *Journal of Communications,* vol. 11, 2016.

[21] Z. M. Fadlullah and N. Kato, "Security Challenge in the Smart Grid," in *Evolution of Smart Grids*, ed: Springer, 2015, pp. 77-90.
[22] L. Husheng, L. Lifeng, and R. C. Qiu, "A denial-of-service jamming game for remote state monitoring in smart grid," in *Information Sciences and Systems (CISS), 2011 45th Annual Conference on*, 2011, pp. 1-6.
[23] L. Zhuo, W. Wenye, and C. Wang, "Hiding traffic with camouflage: Minimizing message delay in the smart grid under jamming," in *INFOCOM, 2012 Proceedings IEEE*, 2012, pp. 3066-3070.
[24] Z. Wang, B. Chen, J. Wang, and C. Chen, "Networked Microgrids for Self-Healing Power Systems," *IEEE Transactions on Smart Grid,* vol. 7, pp. 310-319, 2016.
[25] M. M. H. Tapase and A. N. Jadhav, "A Review–Usage of Self-Healing System For Smart Grids," 2016.
[26] F. Skopik and P. D. Smith, *Smart Grid Security: Innovative Solutions for a Modernized Grid*: Elsevier Science, 2015.
[27] Z. Zhang, H. Liu, S. Niu, and J. Mo, "Information security requirements and challenges in smart grid," in *Information Technology and Artificial Intelligence Conference (ITAIC), 2011 6th IEEE Joint International*, 2011, pp. 90-92.
[28] H. Xingze, P. Man-On, and C. C. J. Kuo, "Secure and efficient cryptosystem for smart grid using homomorphic encryption," in *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*, 2012, pp. 1-8.
[29] L. Yee Wei, M. Palaniswami, G. Kounga, and A. Lo, "WAKE: Key management scheme for wide-area measurement systems in smart grid," *Communications Magazine, IEEE,* vol. 51, pp. 34-41, 2013.
[30] M. Badra and S. Zeadally, "Key management solutions in the smart grid environment," in *Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP*, 2013, pp. 1-7.
[31] A.-S. Khan Pathan, Z. M. Fadlullah, M. M. Fouda, M. M. Monowar, and P. Korn, "Information integrity in smart grid systems," *Information Systems,* vol. 53, pp. 145-146, 2015.
[32] M. Garcia, A. Giani, and R. Baldick, "Smart grid data integrity attacks: Observable islands," in *Power & Energy Society General Meeting, 2015 IEEE*, 2015, pp. 1-5.
[33] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. Al Ali, "Smart grid cyber security: Challenges and solutions," in *2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, 2015, pp. 170-175.
[34] P. E. Weerathunga, J. Samarabandu, and T. Sidhu, "Implementation of IPSec in substation gateways," in *Information and Automation for Sustainability (ICIAfS), 2012 IEEE 6th International Conference on*, 2012, pp. 327-331.
[35] A. Mohan and H. Khurana, "Towards addressing common security issues in smart grid specifications," in *Resilient Control Systems (ISRCS), 2012 5th International Symposium on*, 2012, pp. 174-180.
[36] R. Dawson, C. Boyd, E. Dawson, and J. M. Gonz, "SKMA: a key management architecture for SCADA systems," presented at the Proceedings of the 2006 Australasian workshops on Grid computing and e-research - Volume 54, Hobart, Tasmania, Australia, 2006.
[37] F. F. Demertzis, G. Karopoulos, C. Xenakis, and A. Colarieti, "Self-organised Key Management for the Smart Grid," in *Ad-hoc, Mobile, and Wireless Networks*, ed: Springer, 2015, pp. 303-316.
[38] C. Donghyun, K. Hakman, W. Dongho, and K. Seungjoo, "Advanced Key-Management Architecture for Secure SCADA Communications," *Power Delivery, IEEE Transactions on,* vol. 24, pp. 1154-1163, 2009.
[39] C. Donghyun, L. Sungjin, W. Dongho, and K. Seungjoo, "Efficient Secure Group Communications for SCADA," *Power Delivery, IEEE Transactions on,* vol. 25, pp. 714-722, 2010.

[40] Z. Fangming, Y. Hanatani, Y. Komano, B. Smyth, S. Ito, and T. Kambayashi, "Secure authenticated key exchange with revocation for smart grid," in *Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES*, 2012, pp. 1-8.

[41] D. J. Kang, J. J. Lee, B. H. Kim, and D. Hur, "Proposal strategies of key management for data encryption in SCADA network of electric power systems," *International Journal of Electrical Power & Energy Systems,* vol. 33, pp. 1521-1526, 2011.

[42] L. Yong-Hun, "IKMS — An ID-based key management architecture for SCADA system," in *Networked Computing (INC), 2011 The 7th International Conference on*, 2011, pp. 139-144.

[43] M. Waldvogel, G. Caronni, S. Dan, N. Weiler, and B. Plattner, "The VersaKey framework: versatile group key management," *Selected Areas in Communications, IEEE Journal on,* vol. 17, pp. 1614-1631, 1999.

[44] G. A. Tizazu, H. R. Hussen, and K. Ki-Hyung, "Secure session key exchange scheme for Smart Grid Home Area Networks," in *ICT Convergence (ICTC), 2013 International Conference on*, 2013, pp. 1116-1120.

[45] L. Nian, C. Jinshan, Z. Lin, Z. Jianhua, and H. Yanling, "A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid," *Industrial Electronics, IEEE Transactions on,* vol. 60, pp. 4746-4756, 2013.

[46] M. M. Fouda, Z. M. Fadlullah, N. Kato, L. Rongxing, and S. Xuemin, "A Lightweight Message Authentication Scheme for Smart Grid Communications," *Smart Grid, IEEE Transactions on,* vol. 2, pp. 675-685, 2011.

[47] V. Aravinthan, V. Namboodiri, S. Sunku, and W. Jewell, "Wireless AMI application and security for controlled home area networks," in *2011 IEEE Power and Energy Society General Meeting*, 2011, pp. 1-8.

[48] R. Lu, X. Liang, X. Li, X. Lin, and X. S. Shen, "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *Parallel and Distributed Systems, IEEE Transactions on,* vol. 23, pp. 1621-1631, 2012.

[49] D. Pan and Y. Liuqing, "A secure and privacy-preserving communication scheme for Advanced Metering Infrastructure," in *2012 IEEE PES Innovative Smart Grid Technologies (ISGT)*, 2012, pp. 1-5.

[50] E. Ayday and S. Rajagopal, "Secure, intuitive and low-cost device authentication for smart grid networks," in *Consumer Communications and Networking Conference (CCNC), 2011 IEEE*, 2011, pp. 1161-1165.

[51] J. Choi, I. Shin, J. Seo, and C. Lee, "An efficient message authentication for non-repudiation of the smart metering service," in *Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference on*, 2011, pp. 331-333.

[52] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "PASS: Privacy-preserving authentication scheme for smart grid network," in *Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on*, 2011, pp. 196-201.

[53] BP. (2013, 5/2/2016). *BP Energy Outlook 2030*. Available: http://www.bp.com/content/dam/bp/pdf/energy-economics/energy-outlook-2015/bp-energy-outlook-booklet_2013.pd

[54] T. N. I. o. S. a. T. (NIST). (2012). *Smart Grid: A Beginner's Guide*. Available: http://www.nist.gov/smartgrid/beginnersguide.cfm

[55] S. F. Bush, *Smart Grid: Communication-Enabled Intelligence for the Electric Power Grid*: Wiley, 2014.

[56] S. S. S. R. Depuru, L. Wang, and V. Devabhaktuni, "Smart meters for power grid: Challenges, issues, advantages and status," *Renewable and Sustainable Energy Reviews,* vol. 15, pp. 2736-2742, 8// 2011.

[57] J. A. Cardenas, L. Gemoets, J. H. Ablanedo Rosas, and R. Sarfi, "A literature survey on Smart Grid distribution: an analytical approach," *Journal of Cleaner Production,* vol. 65, pp. 202-216, 2/15/ 2014.

[58] M. D. Hadley, J. B. McBride, T. W. Edgar, L. R. O'Neil, and J. D. Johnson. (2007). *Securing Wide Area Measurement Systems* Available: http://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/8-Securing_WAMS.pdf

[59] G. Cai, D. Yang, and C. Liu, "Adaptive Wide-Area Damping Control Scheme for Smart Grids with Consideration of Signal Time Delay," *Energies,* vol. 6, p. 4841, 2013.

[60] L. T. B. a. K. Iniewski, *Smart Grid Apllications, Communication and Security*. Hoboken, New Jersy Wiley, 2012.

[61] L. T. Berger and K. Iniewski, *Smart Grid Applications, Communications, and Security*: Wiley, 2012.

[62] Fadi Aloula, A. R. Al-Alia , Rami Al-Dalkya, M. Al-Mardinia, and a. W. El-Hajjb, "Smart Grid Security: Threats, Vulnerabilities and Solutions " *International Journal of Smart Grid and Clean Energy* vol. 1, 2012.

[63] B. Shahid, Z. Ahmed, A. Faroqi, and R. M. Navid-ur-Rehman, "Implementation of smart system based on smart grid Smart Meter and smart appliances," in *Smart Grids (ICSG), 2012 2nd Iranian Conference on*, 2012, pp. 1-4.

[64] M. Z. Huq and S. Islam, "Home Area Network technology assessment for demand response in smart grid environment," in *Universities Power Engineering Conference (AUPEC), 2010 20th Australasian*, 2010, pp. 1-6.

[65] E. Hossain, Z. Han, and H. V. Poor, *Smart Grid Communications and Networking*: Cambridge University Press, 2012.

[66] M. Miller, *The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World*: Pearson Education, 2015.

[67] J. Kamto, L. Qian, W. Li, and Z. Han, "-Augmented Tree for Robust Data Collection in Advanced Metering Infrastructure," *International Journal of Distributed Sensor Networks,* vol. 2016, 2016.

[68] Q.-D. Ho, Y. Gao, G. Rajalingham, and T. Le-Ngoc, "Smart Grid Communications Network (SGCN)," in *Wireless Communications Networks for the Smart Grid*, ed Cham: Springer International Publishing, 2014, pp. 15-30.

[69] Y. Wang, "Smart grid, automation, and scada systems security," *Security and Privacy in Smart Grids,* pp. 245-268, 2013.

[70] S. G. McCrady, *Designing SCADA Application Software: A Practical Approach*: Elsevier Science, 2013.

[71] H. Farhangi, "Cyber-Security Vulnerabilities: An Impediment Against Further Development of Smart Grid," in *Smart Grids from a Global Perspective*, ed: Springer, 2016, pp. 77-93.

[72] J. D. Fernandez and A. E. Fernandez, "SCADA systems: vulnerabilities and remediation," *J. Comput. Small Coll.,* vol. 20, pp. 160-168, 2005.

[73] D. A. Gratton, *The Handbook of Personal Area Networking Technologies and Protocols*: Cambridge University Press, 2013.

[74] H. Chaouchi, *The Internet of Things: Connecting Objects*: Wiley, 2013.

[75] K. Curran, *Recent Advances in Ambient Intelligence and Context-Aware Computing*: IGI Global, 2014.

[76] K. Rose, S. Eldridge, and L. Chapin, "The internet of things: An overview," *The Internet Society (ISOC),* 2015.

[77] R. Stackowiak, A. Licht, V. Mantha, and L. Nagode, *Big Data and The Internet of Things: Enterprise Information Architecture for A New Age*: Apress, 2015.

[78] M. A. Matin, *Handbook of Research on Progressive Trends in Wireless Communications and Networking*: IGI Global, 2014.

[79] L. Hua, Z. Junguo, and L. Fantao, "Internet of Things Technology and its Applications in Smart Grid," *TELKOMNIKA Indonesian Journal of Electrical Engineering,* vol. 12, pp. 940-946, 2014.

[80] A. Al-Ali and R. Aburukba, "Role of Internet of Things in the Smart Grid Technology," *Journal of Computer and Communications,* vol. 3, p. 229, 2015.

[81] E. Spanò, L. Niccolini, S. Di Pascoli, and G. Iannacconeluca, "Last-meter smart grid embedded in an Internet-of-Things platform," *Smart Grid, IEEE Transactions on,* vol. 6, pp. 468-476, 2015.

[82] E. Sun, X. Zhang, and Z. Li, "The internet of things (IOT) and cloud computing (CC) based tailings dam monitoring and pre-alarm system in mines," *Safety Science,* vol. 50, pp. 811-815, 2012.

[83] P. Parwekar, "From Internet of Things towards cloud of things," in *Computer and Communication Technology (ICCCT), 2011 2nd International Conference on*, 2011, pp. 329-333.

[84] S. Karnouskos, "Smart houses in the smart grid and the search for value-added services in the cloud of things era," in *Industrial Technology (ICIT), 2013 IEEE International Conference on*, 2013, pp. 2016-2021.

[85] M. Dastbaz, C. Pattinson, and B. Akhgar, *Green Information Technology: A Sustainable Approach*: Elsevier Science, 2015.

[86] G. Liassas, "Privacy Enhancing Mechanisms in the Smart Grid," Master, Aalto University & Technical University of Denmark. , 2013.

[87] P. Siano, "Demand response and smart grids—A survey," *Renewable and Sustainable Energy Reviews,* vol. 30, pp. 461-478, 2014.

[88] K. Moslehi and R. Kumar, "A Reliability Perspective of the Smart Grid," *IEEE Trans. Smart Grid,* vol. 1, pp. 57-64, 2010.

[89] F. Ye, Y. Qian, R. Q. Hu, and S. K. Das, "Reliable energy-efficient uplink transmission for neighborhood area networks in smart grid," *Smart Grid, IEEE Transactions on,* vol. 6, pp. 2179-2188, 2015.

[90] S. Kaboli, *Reliability in Power Electronics and Electrical Machines: Industrial Applications and Performance Models: Industrial Applications and Performance Models*: IGI Global, 2016.

[91] C. W. Gellings, *The smart grid: enabling energy efficiency and demand response*: The Fairmont Press, Inc., 2009.

[92] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," *Communications Surveys & Tutorials, IEEE,* vol. 14, pp. 998-1010, 2012.

[93] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renewable and Sustainable Energy Reviews,* vol. 57, pp. 302-318, 2016.

[94] S. Karapostolakis, E. S. Rigas, N. Bassiliades, and S. D. Ramchurn, "EVLib: A Library for the Management of the Electric Vehicles in the Smart Grid," in *Proceedings of the 9th Hellenic Conference on Artificial Intelligence*, 2016, p. 13.

[95] I. L. Pearson, "Smart grid cyber security for Europe," *Energy Policy,* vol. 39, pp. 5211-5218, 2011.

[96] K.-C. Chen, P.-C. Yeh, H.-Y. Hsieh, and S.-C. Chang, "Communication infrastructure of smart grid," in *Communications, Control and Signal Processing (ISCCSP), 2010 4th International Symposium on*, 2010, pp. 1-5.

[97] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. Wang, "Impact of cyber-security issues on smart grid," in *Innovative Smart Grid Technologies (ISGT Europe), 2011 2nd IEEE PES International Conference and Exhibition on*, 2011, pp. 1-7.

[98] B. Krebs. (2008). *Cyber Incident Blamed for Nuclear Power Plant Shutdown*. Available: http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.htm

[99] D. Kushner, "The real story of stuxnet: how kaspersky lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program," *IEEE spectrum,* 2013.

[100] D. V. Dollen. (June 17, 2009). *Report to NIST on the Smart Grid Interoperability Standards Roadmap*. Available: http://www.nist.gov/smartgrid/upload/InterimSmartGridRoadmapNISTRestructure.pdf

[101] A. Chakrabarti, A. Damodaran, and S. Sengupta, "Grid computing security: A taxonomy," *IEEE Security & Privacy,* pp. 44-51, 2008.

[102] Z. A. Baig and A.-R. Amoudi, "An Analysis of Smart Grid Attacks and Countermeasures," *Journal of Communications,* vol. 8, pp. 473-479, 2013.

[103] B. Moussa, M. Debbabi, and C. Assi, "A detection and mitigation model for PTP delay attack in a smart grid substation," in *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2015, pp. 497-502.

[104] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM,* vol. 26, pp. 96-99, 1983.

[105] E. Rescorla, "Diffie-Hellman key agreement method," 1999.

[106] J.-Y. Kim and H.-K. Choi, "An efficient and versatile key management protocol for secure smart grid communications," in *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, 2012, pp. 1823-1828.

[107] W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," *Computer Networks,* vol. 57, pp. 1344-1371, 2013.

[108] A. Wagner, S. Speiser, and A. Harth, "Semantic web technologies for a smart energy grid: Requirements and challenges," in *Proceedings of the 2010 International Conference on Posters & Demonstrations Track-Volume 658*, 2010, pp. 33-36.

[109] M. V. Bharathi, R. C. Tanguturi, C. Jayakumar, and K. Selvamani, "Node capture attack in Wireless Sensor Network: A survey," in *Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on*, 2012, pp. 1-3.

[110] K. Venkatraman, J. V. Daniel, and G. Murugaboopathi, "Various attacks in wireless sensor network: survey," *International Journal of Soft Computing and Engineering,* vol. 3, 2013.

[111] K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones, "Security in wireless sensor networks," in *Handbook of Information and Communication Security*, ed: Springer, 2010, pp. 513-552.

[112] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-service (DoS) attacks on load frequency control in smart grids," in *Innovative Smart Grid Technologies (ISGT), 2013 IEEE PES*, 2013, pp. 1-6.

[113] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J.-C. Tan, "An intrusion detection system for IEC61850 automated substations," *Power Delivery, IEEE Transactions on,* vol. 25, pp. 2376-2383, 2010.

[114] D. Jin, D. M. Nicol, and G. Yan, "An event buffer flooding attack in DNP3 controlled SCADA systems," in *Proceedings of the Winter Simulation Conference*, 2011, pp. 2619-2631.

[115] C. Taylor and T. Johnson, "Strong authentication countermeasures using dynamic keying for sinkhole and distance spoofing attacks in smart grid networks," in *Wireless Communications and Networking Conference (WCNC), 2015 IEEE*, 2015, pp. 1835-1840.

[116] S. Golestani Najafabadi, H. R. Naji, and A. Mahani, "Sybil attack Detection: Improving security of WSNs for smart power grid application," in *Smart Grid Conference (SGC), 2013*, 2013, pp. 273-278.

[117] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil Attacks and Their Defenses in the Internet of Things," *Internet of Things Journal, IEEE,* vol. 1, pp. 372-383, 2014.

[118] T.-T. Tran, O.-S. Shin, and J.-H. Lee, "Detection of replay attacks in smart grid systems," in *Computing, Management and Telecommunications (ComManTel), 2013 International Conference on*, 2013, pp. 298-302.

[119] S. McLaughlin, D. Podkuiko, and P. McDaniel, "Energy theft in the advanced metering infrastructure," presented at the Proceedings of the 4th international conference on Critical information infrastructures security, Bonn, Germany, 2010.

[120] Z. Xiao, Y. Xiao, and D. H.-C. Du, "Non-repudiation in neighborhood area networks for smart grid," *Communications Magazine, IEEE,* vol. 51, pp. 18-26, 2013.

[121] W. Wang and Z. Lu, "Survey Cyber security in the Smart Grid: Survey and challenges," *Comput. Netw.,* vol. 57, pp. 1344-1371, 2013.

[122] W. Dapeng and Z. Chi, "Fault-Tolerant and Scalable Key Management for Smart Grid," *Smart Grid, IEEE Transactions on,* vol. 2, pp. 375-381, 2011.

[123] H. Nicanfar, P. Jokar, and V. C. M. Leung, "Smart grid authentication and key management for unicast and multicast communications," in *Innovative Smart Grid Technologies Asia (ISGT), 2011 IEEE PES*, 2011, pp. 1-8.

[124] Sungjin Lee, Donghyun Choi, a. Choonsik Park, and S. Kim, "An Efficient Key Management Scheme for Secure SCADA Communication," *World Academy of Science, Engineering and Technology,* vol. 45, 2008.

[125] S. Mittra, "Iolus: a framework for scalable secure multicasting," presented at the Proceedings of the ACM SIGCOMM '97 conference on Applications, technologies, architectures, and protocols for computer communication, Cannes, France, 1997.

[126] W. Chung Kei, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," *Networking, IEEE/ACM Transactions on,* vol. 8, pp. 16-30, 2000.

[127] C. L. Beaver, D.R. Gallup, W. D. NeuMann, and a. M. D. Torgerson. Key Management for SCADA [Online]. Available: http://energy.sandia.gov/wp/wp-content/gallery/uploads/013252.pdf

[128] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sen. Netw.,* vol. 2, pp. 500-528, 2006.

[129] J. Kamto, Q. Lijun, J. Fuller, and J. Attia, "Light-weight key distribution and management for Advanced Metering Infrastructure," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, 2011, pp. 1216-1220.

[130] S. Das, Y. Ohba, M. Kanda, D. Famolari, and S. K. Das, "A key management framework for AMI networks in smart grid," *Communications Magazine, IEEE,* vol. 50, pp. 30-37, 2012.

[131] J. Ekanayake, N. Jenkins, K. Liyanage, J. Wu, and A. Yokoyama, *Smart Grid: Technology and Applications*: Wiley, 2012.

[132] V. Namboodiri, V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell, "Toward a Secure Wireless-Based Home Area Network for Metering in Smart Grids," *Systems Journal, IEEE,* vol. PP, pp. 1-12, 2013.

[133] H. Nicanfar, P. Jokar, and V. C. M. Leung, "Efficient authentication and key management for the Home Area Network," in *Communications (ICC), 2012 IEEE International Conference on*, 2012, pp. 878-882.

[134] B. Alohali, M. Merabti, and K. Kifayat, "A Cloud of Things (CoT) Based Security for Home Area Network (HAN) in the Smart Grid," in *Next Generation Mobile Apps, Services and Technologies (NGMAST), 2014 Eighth International Conference on*, 2014, pp. 326-330.

[135] M. D. H. Abdullah, Z. M. Hanapi, Z. A. Zukarnain, and M. A. Mohamed, "Attacks, Vulnerabilities and Security Requirements in Smart Metering Networks," *TIIS,* vol. 9, pp. 1493-1515, 2015.

[136] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 238-243.

[137] F. Li, B. Luo, and P. Liu, "Secure information aggregation for smart grids using homomorphic encryption," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 327-332.
[138] S. Kim, E. Y. Kwon, M. Kim, J. H. Cheon, S.-h. Ju, Y.-h. Lim*, et al.*, "A secure smart-metering protocol over power-line communication," *Power Delivery, IEEE Transactions on,* vol. 26, pp. 2370-2379, 2011.
[139] M. Merabti, B. Alohali, and K. Kifayat, "A New Key Management Scheme Based on Smart Grid Requirements."
[140] P. Levis, S. Madden, J. Polastre, R. Szewczyk, K. Whitehouse, A. Woo*, et al.*, "Tinyos: An operating system for sensor networks," in *Ambient intelligence*, ed: Springer, 2005, pp. 115-148.
[141] P. Levis and D. Gay, *TinyOS Programming*: Cambridge University Press, 2009.
[142] A. D. Wood and J. A. Stankovic, "AMSecure: secure link-layer communication in TinyOS for IEEE 802.15.4-based wireless sensor networks," presented at the Proceedings of the 4th international conference on Embedded networked sensor systems, Boulder, Colorado, USA, 2006.
[143] H. M. Ammari, *The Art of Wireless Sensor Networks: Volume 1: Fundamentals*: Springer Berlin Heidelberg, 2013.
[144] S. S. Iyengar, N. Parameshwaran, V. V. Phoha, N. Balakrishnan, and C. D. Okoye, *Fundamentals of Sensor Network Programming: Applications and Technology*: Wiley, 2011.
[145] B. Alohali, K. Kifayat, Q. Shi, and W. Hurst, "A Survey on Cryptography Key Management Schemes for Smart Grid," *Journal of Computer Sciences and Applications,* vol. 3, pp. 27-39, 2015.
[146] Riverbed. (2014). *Riverbed Modeler Version 17.5, PL6,, Riverbed Software*. Available: http://www.riverbed.com/
[147] N. i. o. S. a. Technology, "Data Encryption Standard," 1999.
[148] I. Broustis, G. S. Sundaram, and H. Viswanathan, "Group Authentication: A New Paradigm for Emerging Applications," *Bell Labs Technical Journal,* vol. 17, pp. 157-173, 2012.
[149] L. Harn, "Group authentication," *Computers, IEEE Transactions on,* vol. 62, pp. 1893-1898, 2013.
[150] F. Wang, C.-C. Chang, and Y.-C. Chou, "Group Authentication and Group Key Distribution for Ad Hoc Networks," *International Journal of Network Security,* vol. 17, pp. 199-207, 2015.
[151] H. Yang, L. Jiao, and V. A. Oleshchuk, "A General Framework for Group Authentication and Key Exchange Protocols," in *Foundations and Practice of Security*, ed: Springer, 2014, pp. 31-45.
[152] L. Berrio and C. Zuluaga, "Concepts, standards and communication technologies in smart grid," in *Circuits and Systems (CWCAS), 2012 IEEE 4th Colombian Workshop on*, 2012, pp. 1-6.
[153] Y. Simmhan, A. G. Kumbhare, C. Baohua, and V. Prasanna, "An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds," in *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, 2011, pp. 582-589.
[154] G. Venkataramani, P. Parankusam, V. Ramalingam, and J. Wang, "A review on compressed air energy storage–A pathway for smart grid and polygeneration," *Renewable and Sustainable Energy Reviews,* vol. 62, pp. 895-907, 2016.
[155] S. Joseph, E. A. Jasmin, and S. Chandran, "Stream Computing: Opportunities and Challenges in Smart Grid," *Procedia Technology,* vol. 21, pp. 49-53, // 2015.
[156] K. Zhou, C. Fu, and S. Yang, "Big data driven smart energy management: From big data to big insights," *Renewable and Sustainable Energy Reviews,* vol. 56, pp. 215-225, 4// 2016.
[157] T. Sauter and M. Lobashov, "End-to-End Communication Architecture for Smart Grids," *IEEE Transactions on Industrial Electronics,* vol. 58, pp. 1218-1228, 2011.

[158] C.J.F. Cremers. The Scyther tool: Automatic verification of security protocols. http://people.inf.ethz.ch/cremersc/scyther/index.html.

[159] J.K. Millen and V. Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. In Proc. 8th ACM Conference on Computer and Communications Security, pages 166–175. ACM Press, 2001.

[160] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, L. Cuellar, P.H. Drielsma, P. He´am, O. Kouchnarenko, J. Mantovani, S. Mo¨dersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Vigan`o, and L. Vigneron. The AVISPA tool for the automated validation of internet security protocols and applications. In Proc. Computer Aided Verification'05 (CAV), volume 3576 of Lecture Notes in Computer Science, pages 281–285. Springer, 2005.

[161] B. Blanchet. An Efficient Cryptographic Protocol Verifier Based on Prolog Rules. In Proc. 14th IEEE Computer Security Foundations Workshop (CSFW), pages 82–96, Cape Breton, June 2001. IEEE Computer Society.

[162] D. Song. An Automatic Approach for Building Secure Systems. PhD thesis, UC Berkeley, December 2003

[163] Cremers, C.J., 2008, October. Unbounded verification, falsification, and characterization of security protocols by pattern refinement. In *Proceedings of the 15th ACM conference on Computer and communications security* (pp. 119-128). ACM.

[164] Yang, H., Oleshchuk, V. and Prinz, A., 2016. Verifying Group Authentication Protocols by Scyther. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *7*(2), pp.3-19..

[165] A. R. Abdallah and X. S. Shen, "A lightweight lattice-based security and privacy-preserving scheme for smart grid," in *2014 IEEE Global Communications Conference*, 2014, pp. 668-674.