# Privacy and Security for Applications and Services in Future Generation Smart Grids

by

**Khumalo Zephania Philani**

(**Student Number: 20250262**)

Dissertation Submitted to the Faculty of Engineering and the Built Environment in Fulfillment of the Requirements for the Degree of

Doctor of Engineering in Electrical Engineering

at the

Durban University of Technology

May 2022

Approved for Final Submission

Supervisor: Professor B Nleya

_____

Date 06/05/2022

Student: Zephania Philani Khumalo

_____

Date 04/05/2022

**Declaration**

The thesis is my original work, hence proclaiming it as such. It has not been partially or wholly submitted to any other university pursuant to a similar qualification.

I give the University permission to lend this work to any other parties for academic research-related purposes only.

| | |
|---|---|
| [redacted] | 04/05/2022 |
| Signature | Date |
| Philani Khumalo | 20250262 |
| Name | Student number |

**Acknowledgments**

Prof B Nleya (Ph.D.) my academic supervisor from the Durban University of Technology, deserve special appreciation for his devotion to supporting me with my studies throughout. His advice, knowledge, and support have assisted me successfully in achieving my goals within the stipulated time frames. The same is extended to Dr A. Musvangwa on North West University.

In addition, I'd like to express my gratitude to DUT for sponsoring my studies throughout. I sincerely have acquired lots as a result of embarking on this project (research). Last but not least, I extend my gratitude to my family members as well.

Finally, I thank God for assuring me excellent health, strength, wisdom, and endurance throughout this time.

*Zephania Phitlani Khumalo*

**Dedication**

Dedicate to all my family, and specifically to my children.

**Abstract**

Growing energy demands together with the urge to supply available power in a reliable, as well as efficient manner, has led to the gradual upgrading and modernizing of existing power grid systems into Smart Grids (SGs) by way of incorporating supporting information and communication technology (ICT) subsystems. The latter facilitates the two-way flow of both energy (power) and information related to the grid's performance, as well as the end user's requirements. Notably, the ICT subsystem enables key entities such as generation, distribution, transmission, and end-user subsystems to interrelate in real-time, and in the process, this achieving a well reliable, robust as well as efficiently managed SG system. The interactions of the various entities constituting the grid result in the emergence of various services and applications exchanging data throughout the interconnected systems. Whereas the SG is quite efficient in rendering its services, it, however, is exposed to various cyber security threats by adversaries. Notably, security threats vary depending on the applications. On the user end networks, the mandatory aggregation of power consumption as well as exchange of power consumption-related information on individual household area networks (HANs) or among HANs and utility's control canter (CC) can result in adversaries tempering with the processes. In particular key security concerns being that during these operations, individuals' privacy, as well as aggregated data integrity, can be compromised as a result of attacks. The resource-constrained nature of associated devices, objects, and elements of the SG at the user side networks and in the SG core, in general, brings about challenges in implementing robust security measures that inevitably involve the performing of complex crypto-operations. For this reason, any measures in the form of schemes and mechanisms implemented to preserve security and privacy must be lightweight, i.e., they should minimize the generation of computational and communication overheads during operations. Nevertheless, the SG cyber-attack surface has expanded thus necessitating data security automation. In this regard, the adoption of multi-layered as well as multi-factor authentication to enhance both security privacy is necessary. Similarly, the adoption of new cybersecurity technology stack trends means will serve as an impetus and general guidance on the architecture framework needed to secure both privacy and security. Further challenges are in that some SG elements and devices are mobile and hence this necessitates mobile software security enhancements. Periodic cybersecurity awareness training will ensure that both manufacturers and utility operators operate at the same pace and direction in combating security threats and vulnerabilities in modern SGs.

In light of what has been outlined, this work mainly addresses the security and privacy concerns within the ICT subsystem's architectures. On the customers' side networks, both data security,

confidentiality, privacy, and integrity must be ensured at all times. In the grid's core, measuring and monitoring units must be protected against integrity attacks, such as false data injection (FDI) attacks.

To this end, the initial part of the dissertation explores the general architectures as well as operations of SGs concerning security concerns.

The second part of the dissertation reviews the various security categories and threats. Exploration is carried out on existing security solutions that are primarily based on procedures, such as encryption schemes, authentication mechanisms, physical security methods, and anonymization techniques.

The final part proposes a lightweight encryption-based security framework that ensures both privacy and security for the various applications and services in modern SGs. The framework incorporates techniques that aim to protect the integrity and availability of the data acquired from key sensors and other measuring entities whilst being relayed to control centres for processing. Overall, the framework aims to maintain the acceptable performance of the SG. Security analysis and performance evaluation of the framework in the form of two proposed schemes is carried out. Overall, the proposed framework, by comparison, is more computational as well as energy efficient. It also reduces latencies as well as at the same time requires relatively lowered storage overheads for initialization irrespective of key sizes.

**Keywords**: Privacy, security, backward/forward secrecy, lightweight encryption, Fog-cloud paradigm, energy efficiency, cyber space

**Table of Contents**


Declaration ..... i

Acknowledgments ..... ii

Copyright ..... iii

Dedication ..... iv

Abstract ..... v

Table of Contents ..... vii

**1. Introduction ..... 1**

1.1 Overview ..... 1

1.2 Microgrids ..... 3

1.3 Impact of SG Services ..... 4

1.4 Privacy and Security in Smart Grids ..... 7

1.5 Motivation ..... 9

1.6 Summary Contributions ..... 9

1.7 Key Objectives ..... 10

1.8 Summary Dissertation Outline ..... 11

1.9 Publications ..... 11

1.10 Summary Chapter ..... 11

**2. Smart Grid Architecture, Operations, and Security Overview ..... 12**

2.1 Introduction ..... 12

2.1.1 Coordinated Management ..... 14

2.2 Architectural Trends ..... 16

2.2.1 Islanded Microgrids ..... 19

2.2.2 IMG Model ..... 23

2.3 Communication Subsystem and Technologies ..... 37

2.3.1 Architecture ..... 37

2.3.2 Operation and Services ..... 41

2.3.3 Applications and Communications Requirements ..... 42

2.3.4 Example SG Services and Applications ..... 43

2.4 Security Issues ..... 49

2.4.1 Overview ..... 49

2.4.2 Key Security Objectives and Requirements in SGs ..... 49
2.4.3 Network Security Threats in the Smart Grid ..... 51
2.4.4 Tampering with Metering Data ..... 56
2.5 Attack Detection for Power Networks ..... 57
2.6. The IoT and Security Features. ..... 58
2.6.1 Privacy ..... 59
2.7 Summary Chapter ..... 59
**3. Privacy Preservation in Smart Grids ..... 61**
3.1 Introduction ..... 61
3.2 Privacy and Smart Grids ..... 62
3.2.1 Key-based attacks ..... 62
3.2.2 Data-based attacks ..... 62
3.2.3 Impersonation Related Attacks ..... 63
3.2.4 Physical Based Attacks ..... 63
3.2.5 Impersonation Related Attacks ..... 63
3.2.6 Solution Approaches ..... 64
3.3 Privacy Preservation/ Cryptographic Approaches ..... 65
3.3.1 Aggregation Based Schemes ..... 65
3.4 Lightweight P rivacy Preserving Scheme for SG HANs ..... 67
3.4. 1 Introduction ..... 67
3.4.2 Model Requirements and Design Objectives ..... 68
3.4.3 Proposed Scheme ..... 72
3.4.4 Protocol Evaluation ..... 76
3.5 Chapter Summary ..... 83
**4. Physical Security Considerations in Smart Grids ..... 84**
4.1 Introduction ..... 84
4.2. Literature Survey on Security in SGs ..... 85
4.3 Security Goals in SG Metering Networks ..... 86
4.4 SG Metering Network and System Level Threats ..... 88
4.4.1 SG Metering Network ..... 88
4.4.2 SG Metering Network Security ..... 89

4.4.3 Security Threats Via AMI ..... 90
4.5 A Group Authentication and Data Security Scheme for Smart Metering In SGs ..... 92
4.5.1 D2D Communication Phases ..... 92
4.5.2 Existing Group Authentication and Key Agreement Schemes ..... 95
4.5.3 IoT Communication Subsystem ..... 96
4.5.4 Model and Group Authentication ..... 97
4.5.5 Data Access Control Using CP-ABE ..... 103
4.5.6 Performance Analysis ..... 109
4.5.7 Overall Security Analysis ..... 115
4.6 Chapter Summary ..... 116
**5. Towards Security and Privacy Guarantees in Future Generation Smart Grids ..... 118**
5.1 Introduction ..... 118
5.2 Architectures ..... 118
5.3 Communication Subsystem ..... 121
5.4 Security and Privacy Framework ..... 124
5.4.1 A D2D Lightweight Customer Side Data Aggregation Scheme ..... 126
5.4.2 A Fog- Cloud-Based Lightweight Authentication Scheme ..... 136
5.5 Chapter Summary ..... 149
**6. Conclusion and Future Work ..... 150**
6.1 Introduction ..... 150
6.2 Key Findings ..... 150
6.3 Future Research Direction ..... 153
References ..... 154
Appendix A: Particle Swarm Optimization (PSO) Codes in MATLAB ..... 166
Appendix B: NTRUEncrypt and NTRUSign Implementation in Java ..... 169
Appendix C: Journals and Publication ..... 170

## List of Figures


Figure 1-1: An SG Comprising Several Interconnected MGs 1

Figure 1-2: Generic MG Architecture 3

Figure 1-3: SG Framework Showing Potential Applications & Services [10] 5

Figure 2-1: Cooperating Individual Microgrids to Form an SG 12

Figure 2-2: Shared Energy Storage Systems 13

Figure 2-3: Energy Cost Versus Storage Capacity Required 14

Figure 2-4: Different Connection Cooperative Modes 15

Figure 2-5: Generalised Model of an Islanded Microgrid 24

Figure 2-6: Forecasted Load and Utility Market Price 28

Figure 2-7: Classification of Demand Side Management Programs 30

Figure 2-8: QPSO Flowchart for Solving Non-Convex EMS Problem 30

Figure 2-9: Non-Convex Cost 33

Figure 2-10: Case II, Non-Convex Cost 33

Figure 2-11: Case III, Non-Convex Cost 34

Figure 2-12: Simulated Results of Case 4 35

Figure 2-13: Convergence Characteristics for the Base Case 36

Figure 2-14: Convergence Characteristics of QPSO with DSM Participation 37

Figure 2-15: Energy Management Using Various Technologies in an SG 39

Figure 2-16: Generalized Communications Network Infrastructure 40

Figure 2-17: Integrated Energy Infrastructure Representative of a Typical SG 41

Figure 2-18: SG Applications Roadmap 43

Figure 2-19: SG AMR Application 44

Figure 2-20: Demand Response Options 45

Figure 2-21: Vehicle to Grid 48

Figure 2-22: Security Objectives for an SG 50

Figure 2-23: Potential Attacks 52

Figure 2-24: Key use Cases in Distribution and Transmission Systems in an SG 54

Figure 2-25: Key use Cases in the AMI and HANs 56

Figure 2-26: Classification of DoS Attack Detection Schemes 57

Figure 2-27: Generalized Secured Communications Architecture 58

Figure 3-1: Smart Grid 61
Figure 3-2: Classification of Attacks 62
Figure 3-3: MITM Attack Illustration 63
Figure 3-4: Taxonomy of Cryptographic Primitives 64
Figure 3-5: Scheme's Model Illustration 68
Figure 3-6: Algorithm 76
Figure 3-7: Comparisons of Communication Overheads (c) Proposed (b) Traditional 78
Figure 3-8: Communication Overhead Considering for Various Scenario Cases 79
Figure 3-9: Computation Overhead Traditional vs. Proposed Scheme. 81
Figure 3-10: Computation Overhead Traditional vs. Proposed Scheme. 82
Figure 3-11: Computation Overheads Comparisons. 82
Figure 4-1: An Architectural and Service Level of the SG 84
Figure 4-2: SG's AMI 86
Figure 4-3: Summary of Security Goals 87
Figure 4-4: SG Metering System Conceptualization 88
Figure 4-5: Potential Attacks 90
Figure 4-6: Summary IoT's D2D Communication Phases 93
Figure 4-7: SG IoT Enabled Communication Subsystem Architecture. 96
Figure 4-8: Abstracted AMI Service 97
Figure 4-9: Sequence Events for the Proposed Framework 99
Figure 4-10: Units ( *SMs*) Joining or Exiting 103
Figure 4-11: Data Aggregation 104
Figure 4-12: KDC Connected in a Distributed Fashion 104
Figure 4-13: Tree Based Access Control Structure for CP-ABE. 105
Figure 4-14: Master Key and Published Key Generation. 106
Figure 4-15: Message encryption. 107
Figure 4-16: Key Generation. 108
Figure 4-17: Key Distribution and Decryption in Smart Meters 109
Figure 4-18: Required Bit Rates as a Function of the Number of SM Devices 111
Figure 4-19: Required Transmission Speeds as a Function of the Number of SM and Number of Groups 112
Figure 4-20: Signaling Overhead in the Network 113

Figure 4-21: Multilevel (4) key Tree for Group Formation During Data Collection 114
Figure 5-1: Proliferation of Objects and Devices in SGs 119
Figure 5-2: SG Vulnerabilities 120
Figure 5-3: Key ICT Subsystem Categories 122
Figure 5-4: Key Logical Infrastructure 123
Figure 5-5: Data Flow Diagram for the Reactive Power Use Case 124
Figure 5-6: Typical cloud-fog Computing Architecture 125
Figure 5-7: 3GPP Coverage in an IoT Network 126
Figure 5-8: Model Configuration 128
Figure 5-9: Communication Loads per Data Reading Cycle 134
Figure 5-10: Communication Loads per 24-hour Cycle 134
Figure 5-11: Plot of Computational Delay Times 135
Figure 5-12: Computational Delays 136
Figure 5-13: Fog Computing Paradigm Alternative 138
Figure 5-14: Authentication Delegation at Fog Layer 139
Figure 5-15: D2D Aided Fog Computing 140
Figure 5-16: Computational Time Comparisons 145
Figure 5-17: Transmission Overheads 146
Figure 5-18: Average Mean Execution Delays 147
Figure 5-19: Energy Efficiency of the Various Schemes 148
Figure 5-20: Storage Overheads Versus Key Size 149

## List of Tables

Table 2.1: Standardization approaches [45] 17

Table 2.2: DG Power Limits with Non-Convex Cost Coefficients 27

Table 2.3: Day-Ahead Forecast Data 31

Table 2.4: Day-Ahead Forecast Data cont' 32

Table 2.5: Performance of QPSO and PSO 35

Table 2.6: Optimized Costs in Rands with Different DSM Participation Levels 36

Table 2.7: Comparison of Security Requirements: SG versus IoT 51

Table 2.8: Denial of Service Attacks in SGs 53

Table 2.9: False Data Injection Attacks in SGs 54

Table 2.10: Key usage Cases with Critical Security Requirements in Distribution/Transmission system 55

Table 2.11: Comparison Between the Distribution/Transmission System and the AMI Networks 56

Table 2.12: Potential Uses and Applications of Existing Attack Detection Methods for the Smart Grid 57

Table 4.1: Latency Requirements for Services 86

Table 4.2: Evaluation Parameters 110

Table 4.3: Computational Parameters (SM side) 115

Table 4.4: Computational Parameters (core network) 115

Table 5.1: Summary of Cryptographic Operations 135

# 1. Introduction

## 1.1 Overview

The ever-increasing world population has led to global attention towards addressing environmental problems that among others seek to address new approaches to energy generation. In that way, carbon pollution will be reduced. It is generally noted that power demands are ever-increasing in both urban and rural areas. According to United Nations (UN) statistics, approximately 1 billion people mostly in developing and poor countries are currently living without electricity. It is therefore important to promote the development of energy-efficient power systems and grids that will maintain environmental friendliness [1].

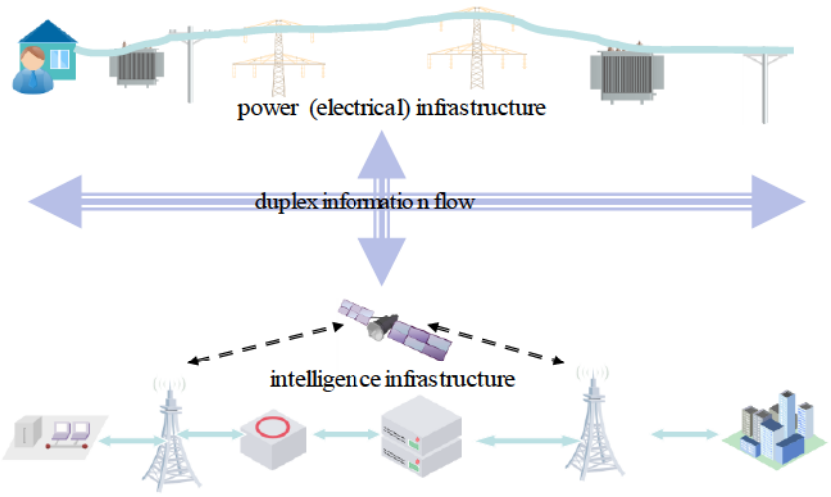


Figure 1-1: An SG Comprising Several Interconnected MGs

This has turned attention to the incorporation of renewable energy sources (RESs) in smart grids (SGs). As a result, SGs are gradually increasing in popularity due to their simplicity and high energy efficiency and becoming an appealing solution for the coordination of multiple conventional generators (CGs) and renewable generators (RGs). In the long term, this gradual increase in the incorporation of RESs might trigger instability issues in power systems grids if they are not regulated and managed properly. In this regard, the SGs are gradually gaining attention in this sector.

One distinct advantage of SGs is in their ability to improve power supply and demand efficiencies by utilizing information and communication technologies (ICTs). The ICT also aids in improving any fault detections, reduction of unnecessary energy wastages as well as enhancing the self-healing capabilities of the power grid. To this end, various supporting related ICT technologies such as

the Internet of Things (IoT), power line carrier (PLC), Wi-Fi, ZigBee, assist in the facilitating as well as provisioning of connectivity to the various entities of the grid [2]. These entities include but are not limited to key components such as end-user systems, transmissions, distribution as well as generation systems. This connectivity will facilitate bi-directional power and information flow among the entities.

As earlier cited, the goal of an SG is to minimize electrical energy losses through theft or physical dissipation (i.e., due to incorrect power factor operations). In the process it maintains a balance between generation and consumptions, hence stabilizing the grid. In that way, the grid's operations become efficient as well as reliable. Key measuring elements such as smart meters (SMs), frequency meters (FMs), as well as phasor measurement units (PMUs) are incorporated to achieve the grid's efficiency objective [3], [4]. These three key units periodically update the SGs central control and management center with information regarding the power grid status in its entirety. E.g., SMs are located at end-user side networks to aggregate the power usage for each user and relay it is billing centers. FMs will generally detect as well as measure frequency fluctuations in various sections of the grid and thus loading can easily be detected in real-time. Similarly, PMUs are also securely placed throughout the grid transmission lines to detect any power factor degradations as well as anomaly behaviors. Therefore, the incorporation, as well as operation of ICT subsystems and entities in an SG result in the emergence of new networks such as vehicle-to-grid (V2G), home area networks (HANs), and neighborhood area networks (NANs).

The three, interconnect, resulting in a much larger network spanning over distances (WAN). Notably, a HAN facilitates connectivity between the user's SM and all his/her smart appliances. The SM periodically aggregates the energy consumptions for the individual appliances and relays them to the billing center. Several HANs interconnect resulting in a NAN or industrial area network (IAN). Typically, NANs interconnect connect one or more neighboring HANs. NANs oversee the operations of HANs connected to them; hence they periodically relay reports regarding each HAN to the grid operator's control center (CC) via the SG's owned ICT subsystem's infrastructure or IoT. The introduction of electrical vehicles (EVs) brought about the need to operate an associated V-2-G link (connection), that the SG (grid) operator utilizes to communicate with the EVs when scheduled for charging/discharging depending on existing power demands. In the process, this arrangement helps to stabilize power levels in the SG system. Figure 1.1 illustrates the integration between the existing power grid and communication architectures resulting in an SG. A microgrid

(MG) is a subunit of an SG that mostly supplies power within its domain. It incorporates a microgrid controller (MC) to collect and aggregate data from the various SMs within the MG. In that way, it can assist in balancing demand and supply. It links with the MG via an MG control center (MGCC).

## 1.2 Microgrids

As stated in the previous section, the basic building block of any SG is an MG. An MG is a domain of distributed energy generators (DEGs) and interconnected loads with a common controllable entity concerning the grid and can operate in autonomous (islanded) mode. Whereas an MG can function in both islanded and non-islanded modes, the earlier provides a more appropriate solution to electrifying rural areas. In other words, an islanded MG (IMG) is ideal for supporting the provisioning of power supply in the countryside, and at the same time, facilitating the integration of RESs into a reliable electricity supply system. In the process, this results in the reduction of the carbon footprint, and well as energy prices/tariffs. A typical IMG will comprise distributed generators (DGs) such as micro-turbines (MTs) diesel generators (DGs), and renewable generators (RGs). In addition, energy storage systems (ESSs) in the form of battery banks stored strategically around the IMG will store energy during daylight time, for later discharging to the grid when the need arises. Illustrated in Figure 1.2 is a generic block diagram of an MG. As mentioned before, the high penetration of RGs, result in issues such as the overall resilient and efficient operation of the IMG [5].

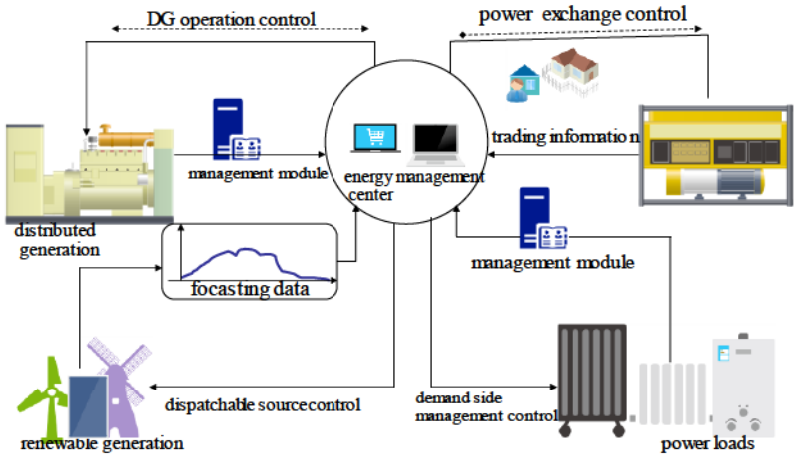


Figure 1-2: Generic MG Architecture

Significant challenges related to this penetration include stability as well as efficiency of energy supply; fluctuations of the grid power frequency due to intermittent load variations; problems associated with the interconnected operation of different RGs; EMS and demand-side management

(DSM) coordination; controlling of the system and the managing of heterogeneous multiple RGs whose operation requirements differ significantly; resilient protection mechanisms taking into account the two-way energy flows; precession modeling of system components; energy storage systems (ESSs) management; system scalability in terms of new technology rollouts e.g. incorporating electric vehicles (EVs). Figure 1.2 illustrates a typical MG architecture [6].

## 1.3 Impact of SG Services

The two proceeding subsections overviewed both an SG and its building block, namely an MG. Overall, the SG can be abstracted as a self-healing, resilient, and adaptive bidirectional (full-duplex) electrical energy exchange system [7], [8], [9]. Its overall current and future design philosophy take into consideration, interoperability with legacy, current as well as new standards of elements, entities, and devices that are protected from various forms of possible cyber-attacks. Overall, and the need for SGs was brought about by:

- The necessity to grab advantages of advancements in ICT and related technologies to resolve the limitations and prohibitive running costs of the legacy (or traditional) power grids.
- Concerns over continued environmental degradations or damage dues to the use of fossil energy-powered power generating systems.
- The gradual declining costs of RGs has triggered a paradigm shift to the distributed generation of power
- Overall, the migration, as well as the evolution of SG infrastructures, will yield the following advantages:
- Enhancement of both reliability and robustness of the power grid as power quality disturbances as well as consequences such as the probability of widespread blackouts will diminish.
- SGs facilitate unlimited advancements and efficiencies of supply-demand balances.
- Power retailing, as well as electricity costs per kWhr (unit) paid by end-users, will drastically drop. This will make the power affordable for most consumers.
- Improved options of supply choices and related information are readily availed to end-users.

- Integration of renewable generation sources and, hence promoting distributed generation. This on its own, will further enhance resilience in a generation.
- Improvement of overall security by way of the reduction of the repercussions and probability of natural disasters and man-made attacks.
- Facilitation of higher penetration levels of distributed electrical energy generation sources.
- Reductions in fatalities (such as electrocutions) in utility grid-related events, thereby reducing safety issues.
- Integration of EVs as power buffers for SGs. This effectively the public transportation sectors
- Improvements in the overall efficacy of operating the SG by way of minimizing losses as well as wasteful consumption of power.
- Reductions in environmental pollution, since greenhouse gas emissions are reduced because of the reliance on cleaner renewable DERs.

Overall, the SG is geared towards employing innovative products, applications, and services, together with sophisticated operation and management to bring about efficiency in power supply and demands.

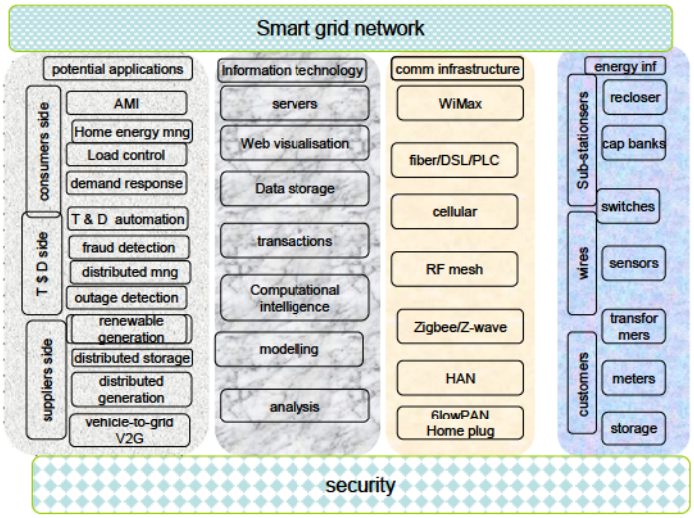


Figure 1-3: SG Framework Showing Potential Applications & Services [10]

As a result, the operation functions of a standard SG will result in numerous innovative applications and services associated with the following:

- Exchanging electricity generation-related data and processing it at various servers specially dedicated for the purpose.
- Integrating multitudes of smaller power generating elements from individual households or private power producers.
- Periodic balancing of grid power fluctuations caused by the injection of extra renewable sources (most from households).
- Processing of logged data acquired from sensors and actuators to promote an improved overall degree of coordination within the grid system to prevent fault occurrences that otherwise may escalate to levels enough to cause disruptions.
- Usage of synchronized sensors as well as communication in data processing at key servers within the grid.
- Near real-time determining of an element's ability to continue normal functioning in coping with the rendered load. This is mostly dependent on environmental factors.
- Utilizing flexible alternating current (ac) transmission systems (FACTS), power factor regulating transformers (PFRs), surge suppressors in the form of series-connected capacitances, and ultra-low resistance superconductors.
- Re-adjustable protective relay settings can change in real-time based on the control (feeder) sensor and control signals.
- Automating isolation and reconfiguring of faulted sections of distribution transmission lines. This will normally be implemented with the help of specialized dedicated sensors, and the existing ICT subsystem.
- Automating the transmission and distribution network sections.
- Coordinated regulation of reactive power resources with sensors, controls, and as well as the ICT subsystem.
- Real-time monitoring of the grid to detect abnormal conditions.
- Improved high-precision detection of faults, through locating and isolating them, with the aid of triangulated measurement-based techniques.

- Instant measuring of end-user power consumption via AMI systems.
- Incorporation of appliance controllers that assist end-users to make informed decisions.
- Fast feeder reconfigurations to possibly ease the load on equipment, improvement s in assets utilization, distribution system efficiency, thus in the process enhancing the system's overall performance.
- End users are well informed so that they can make informed decisions regarding power usage.

## 1.4 Privacy and Security in Smart Grids

The gradual shift to SGs has brought about numerous advantages such as efficiency in demand and supply management, increased reliability of the grid system, reduced operational as well capital costs, and a more environmentally friendly energy generation as there is a lesser dependency on fossils-based generation [11]. We note the rolling out of AMI residential networks has afforded the indispensable residential smart metering that allows smart monitoring of power consumption of all household smart electrical appliances. There is, however, a heavy reliance on ICT infrastructure to provide connectivity among the various entities of the SG. This is to imply that the heterogeneous network must facilitate open connectivity, characterized by availability, reliability efficiency as well as security [12]. Security and privacy aspects are concerns that automatically creep in. Addressing both privacy and security is quite a key issue regarding the successful deployment of the ICT subsystem that facilitates vital communication in an SG. The resource-constrained nature of the devices in the IoT networks means that the traditional security and privacy protocols cannot be applied directly since they are intensive resource demanding. Typically, they will require more memory and processing power. IoT networks deployed communicating devices and objects are often deployed and operate in adverse environments, thus being readily vulnerable and susceptible to both physical and semantic security attacks [13]. An important aspect of the successful running of SG communication-based services and applications is that they are reliably authenticated. A typical example service or application will involve several devices collaborating as a group. In such a scenario, mutual authentication within the group is mandatory to exclude intruding actions by adversaries [13], [14].

The overall aim is to ensure identity privacy, as well as security for the data, are not compromised. The multi-domain nature of a fully fletched SG means that a given service or application may run

in the form of several deployed groups, spanning over a few MG network domains. This will require linking them across the domains which are independently administered. They are independently administered in the sense that the security policies might differ from one network domain to another. The vast geographical spread may contribute adversely to the maximum acceptable delay latencies.

With the aforesaid issues and challenges, this necessitates a thorough investigation of group authentication as well as a key agreement protocol for SG communications that is assumed to operate among multiple domains as well as operators. In this case, we will advocate for cloud computing-based paradigms. However, ultimately, we will rely more on the Fog layer-assisted computing paradigm to reduce the end-to-end latencies as well as turnaround times among the various entities comprising the SG. In so doing our focus is on ensuring the following:

- That the proposed security and privacy framework can carry out group authentication and as such all members of a group of participating devices are authenticated concurrently.
- That it preserves security as well as privacy requirements. In particular, the forward and backward secrecy must be preserved when a device vacates or joins a group.
- Taking cognizance of the resource-contained nature of the operational environment, we propose some lightweight forms of cryptography. We will also lean towards the usage of symmetric keys to keep computational as well as signaling overheads loads minimal.
- Summarily the privacy and security concerns in an SG can be categorized as follows:
- The end user's privacy and information confidentiality must be maintained. This is crucial for those dwelling in individual (standalone) houses, residential block units, or industrial buildings.
- Data integrity is also a concern. Adversaries will always try to modify billing-related data.
- Thirdly, the SG's resources availability can be vulnerable to attacks. Adversaries may direct malicious acts to the ICT subsystem's resources by way of DoS attacks. Notably, they can always try to cause delays or corrupt the data whilst in transit to processing centers.

In conclusion, we summarily note that blending legacy and, current and future power system grids with ICT technologies exposes them to security threats. Overall, the security risks in an SG are denial of service, data integrity, and end user's data confidentiality and privacy. Thus, it is key to study, analyse security threats [15], [16], [17], [18], [10], [20].

## 1.5 Motivation

The work herein will center on addressing privacy and security threats in the SG for the various applications and services. Ultimately, efficient security and privacy-preserving framework will be proposed and evaluated, the efficiency is in terms of computational simplicity as well as minimized latency (turn-around times).

Initially, the work explores the general architectures as well as operations of MGs and SGs. At an operational level, we explore the associated applications and services. The work will also explore the various ways of data aggregating and relaying to billing centers. The focus would be on security concerns.

The second part of the thesis reviews the various security categories and threats. We will then carry on an extensive survey as well as comparisons of various privacy and security frameworks and protocols applicable to modern SGs. All this is concerning the various applications and services in SGs. We also explore existing security solutions that are primarily based on procedures, such as ciphering/deciphering, confidentiality-related mechanisms, cyber security methods, and anonymization techniques.

The final part will propose a security framework based on lightweight encryption that ensures both privacy and security for the various applications and services in modern SGs. The framework incorporates techniques that aim to protect the integrity and availability of the data acquired from key sensors and other measuring entities whilst being relayed to control centers for processing. Overall, the framework aims to maintain the acceptable performance of the SG. Security analysis and performance evaluation of the framework and associated schemes will be carried out and the results analyzed.

## 1.6 Summary Contributions

The dissertation mainly focuses on security and privacy for the various operational applications and services of SGs. An architectural design trend of modern SGs and MGs is carried out in the

initial stages of the work. We address security issues relating to the vulnerabilities faced by various services as data is exchanged among entities within the SG.

Summarily, the dissertation contributes the following:

- An overview of architectural trends and operations of modern power systems grids.
- Operational issues such as data collection, aggregating as well as relaying to key processing canters. The focus is on possible security risks.
- Modeling techniques for various categories of privacy and security schemes. Emphasis is on the application of tools such as lightweight forms of homomorphic encryption and differential privacy to address potential security in SG systems.
- The proposition as well as evaluation of a Fog-Cloud paradigm-based security framework that balances security guarantees and practical, scalable techniques to provide privacy for real-time implementation. Our focus is on computational simplicity as well as minimal turnaround times. Both numerical, as well as simulation analyses, are provided to show the efficacy of the proposed framework.
- Lastly, taking cognizance of the resource-contained nature of the operational environment, we propose some lightweight forms of cryptography-based schemes. We will also lean towards the usage of symmetric keys to keep computational as well as signaling overheads loads minimal.

## 1.7 Key Objectives

Summary, objectives of the work herein are as follows:

- Embarking on an extensive literature survey on architectures, operational issues, as well as security and privacy in SGs.
- The ICT subsystem and related technologies facilitate connectivity within the SG.
- Survey on privacy and security threats in SGs. The focus is on comparisons as well as efficacies of schemes that provide privacy as security (semantic).
- Evaluation of a proposed security framework by way of simulation as well as general analysis. Note that the proposed framework will be based on both Cloud and Fog layer-assisted computing paradigms.

## 1.8 Summary Dissertation Outline

The dissertation is structured as follows. Chapter 1, introduces, issues related to SGs as well as motivation for the work done in subsequent chapters. Chapter 2 presents a detailed account of architectural trends in SGs and associated security concerns. Chapter 3 explores the main privacy as well as security in the key communication architectures in an SG and related work in various literature. Chapter 4 explores privacy schemes applicable to current and future SGs. This is at both the end-user-side networks and core. Both security analysis and performance evaluation are carried out. Chapter 5 focuses on a proposal, as well as an evaluation of a Fog-Cloud paradigm-based security framework that balances security guarantees and practical, scalable techniques to provide privacy for real-time implementation. Chapter 6 concludes the dissertation and discusses future directions.

## 1.9 Publications

Related research outputs are as follows:

[1]. **P. Khumalo**, L. Bopape, B. Nleya, and A. Mutsvangwa, "A Group Authentication and Data Security Scheme for Smart Metering in Smart Grids," International Scientific Research Journal, vol. 76, 01/01 2020.

[2] **P. Khumalo**, B. Nleya, and A. Mutsvangwa, "A controllable deflection routing and wave-length assignment algorithm in OBS networks." Journal of Optics vol. 48, no. 4, pp. 539-548, 2019.

[3]. B. Nleya., **P. Khumalo** and R. Chidzonga, " Power Demand and Supply Optimization in Islanded Microgrids with Distributed Generation. , Journal of Management Information and Decision Sciences, September 2021.

## 1.10 Summary Chapter

In the power sector, a shift from the present dominated fossil-based generation to renewable as well as energy-efficient generation and distribution has commenced. The transmission is mostly driven by the digitalization of the energy sector, thus providing numerous benefits for both utility and end-users (consumers). Digitalization will enable more activity in the power trading market and a large amount of data will soon be available in the energy sector. However, voluminous data exchanges lead to privacy and data concerns. The chapter mainly previewed SGs and privacy and security threats in the SG for the various applications and services. Motivation as well as key aims, and objectives were also spelled out.

# 2. Smart Grid Architecture, Operations, and Security Overview

## 2.1 Introduction

The possible combined impacts, as well as repercussions of elevated carbon gas emissions due to the increased demand for electrical energy, have shifted focus to DG with RERs rather than the traditional fossil fuel-based generation [21]. The RERs are mostly dominated by, solar, wind, and hydro energy-based generators. The generated power is stored in conveniently located ESSs mostly comprised of battery storage units (BSUs) and EVs.

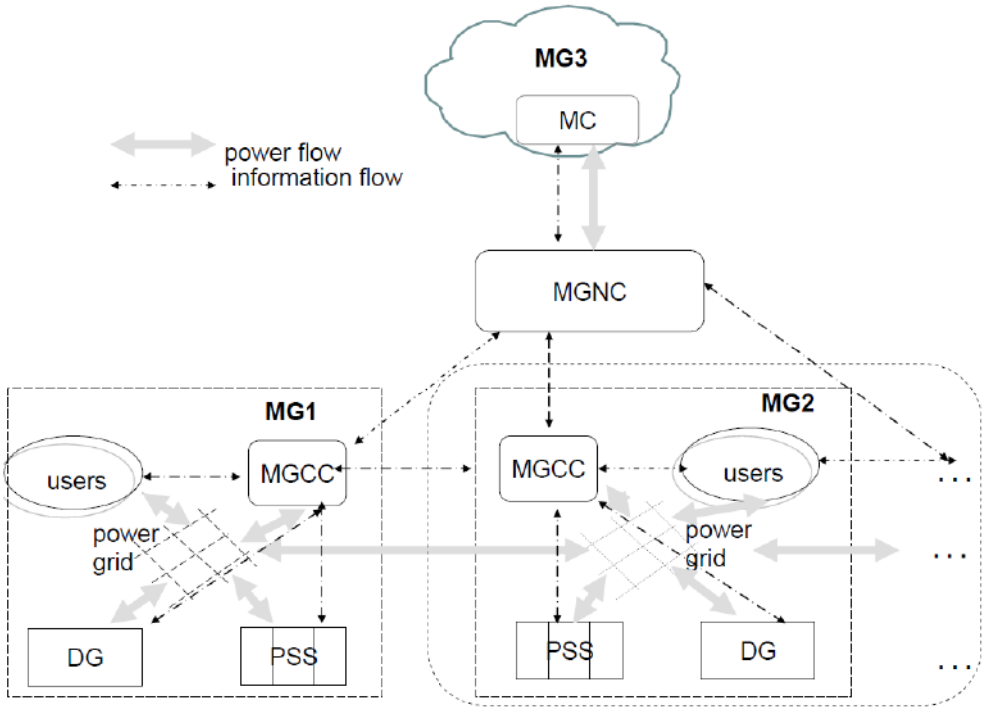


Figure 2-1: Cooperating Individual Microgrids to Form an SG

The MGs' power generation is mostly dominated by RERs. By comparison, DGs are efficient and have flexible integration capabilities with the main power grid. Often MGs can operate in isolation, especially in remote areas (IMGs). However, such configuration will often be constrained in terms of demand and supply. For this reason, often individual MGs are interconnected to make a larger power distribution network, typically as SG [22], [23]. This is illustrated by Figures 2.1 and 2.2.

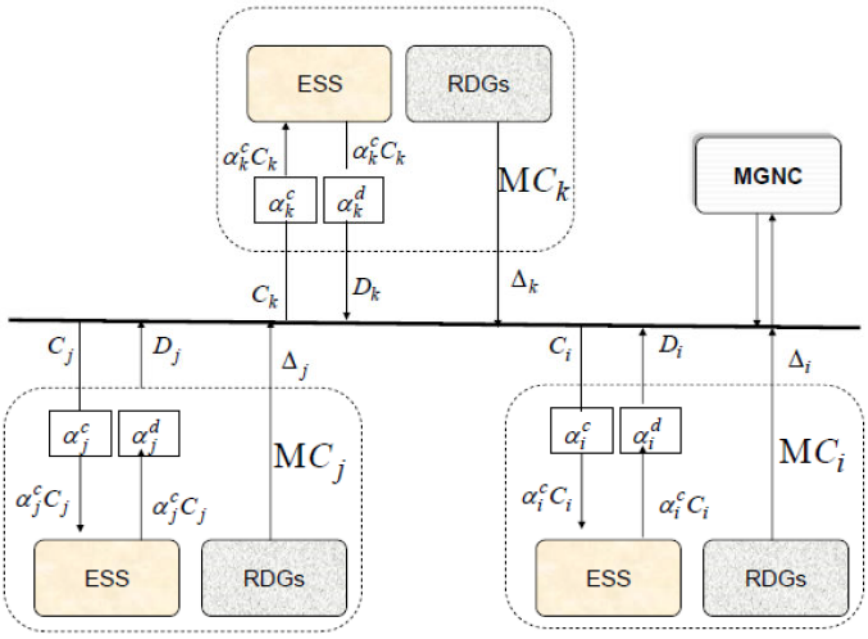


Figure 2-2: Shared Energy Storage Systems

In that way, the integrated system becomes relatively reliable, efficient as well as resilient. Nevertheless, each MG remains autonomous in optimizing its operations. Hence, the SG operator (SGO), has the responsibility of properly coordinating the individual MGs such that a poorly managed MG cannot be catered for ahead of those that are efficiently managed. By this, we mean that because of the uncertainties of both load demands and renewable generation, each MG must satisfy its domain before provisioning any surplus power externally (i.e., to other MGs who are currently in short supply).

Overall, it has been proven that when MGs are operating cooperatively, each will require relatively fewer resources such as ESSs and DGs to satisfy the desired levels of customer satisfaction. This is illustrated in Figure 2.3.

Notably, for cooperating MGs to operate efficiently, it is desirable that a supporting communication infrastructure be scalable enough as this will enhance energy supply. Furthermore, automating the system given limited DG sources would further enhance efficiency and optimization [24]. In that way, such systems will be operationally cost viable [25]-[28].

Energy costs versus capacity requirements is graphically analyzed in Figure 2.3, [27].

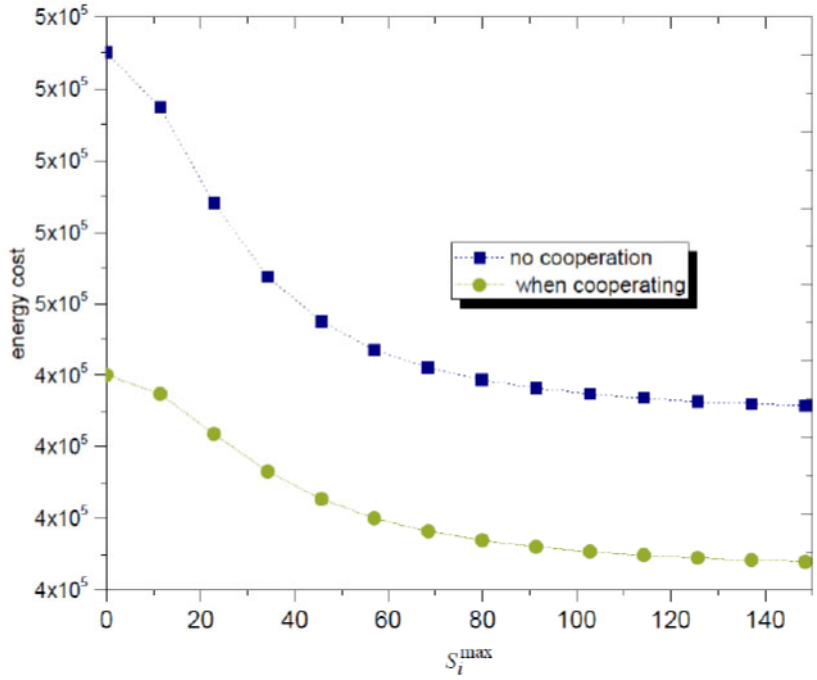


Figure 2-3: Energy Cost Versus Storage Capacity Required

It is for that reason, that in the next section, we briefly review work that has been done in regards to MGs operating in a cooperative manner and under coordinated management.

### 2.1.1 Coordinated Management

We commence this section by clarifying the difference between SG versus MG grids in the context of discussions herein. An SG grid is an intelligent power system grid that is enhanced with an ICT subsystem infrastructure to provide the necessary communications for its normal operations, whereas an MG is a relatively localized and small power system grid. An SG grid is not necessarily enhanced with an ICT subsystem and mostly generates energy for a relatively small locality. An SG can be viewed as a system of multiple cooperating individual MGs. Of late various coordinated management architectures for the operation of SGs have been proposed to cater for normal and faulted operations. Three common architectural topologies (structures) namely: radial, chain, and mesh have been explored [29]. Each MG connects directly to the main grid's bus and control center. Depending on the connections, this results in either a radial, star, or radial structure. Each MG attaches to the main bus to facilitate electrical energy flow between it and the main power grid [30], [31], [32]. As such, direct energy trading between individual MGs is not facilitated. In each of the connection topologies, each MG can operate in the island, grid-connected or networked modes.

Therefore, the MGNC in these operation modes is crucial for the functioning of individual MGs [21].

The various modes of operations are illustrated in Figure 2.4.

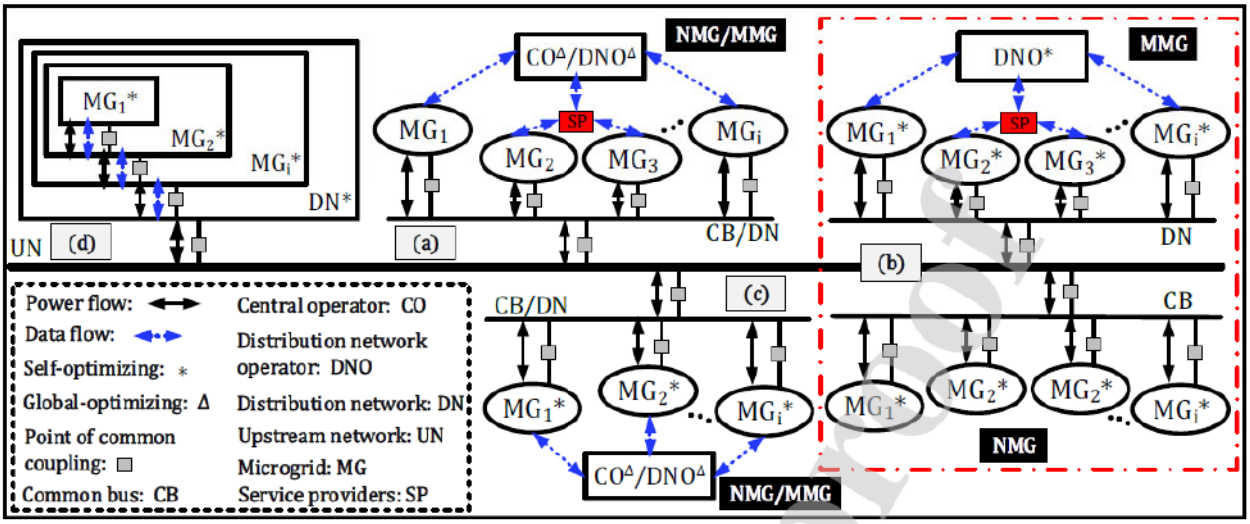


Figure 2-4: Different Connection Cooperative Modes

Similarly, energy management models such as centralized, decentralized, hybrid, and nested SG have been comprehensively studied [33]. In a centralized management model, each MG has its management entity and in turn, is connected to an overall centralized management entity (MGNC). This is partly illustrated in Figure 2.4 (a). Whilst autonomous operation is preserved for each MG, however the same does not apply to potential profits resulting from power trading [34]. Furthermore, a fault in the MGNC will affect all individual MGs connected. Thus, such an architecture is not very reliable and at the same time has elongated latencies.

The authors in [35] argue that the approach nevertheless is for managing outages. For instance, the latencies experienced by such an architecture impacts quite significantly on the coordinated outage management strategy. In light of these shortcomings, other researchers have advocated for a decentralized approach. It is illustrated in Figure 2.4 (b). Notably, each MGC manages its operational issues, but at the same time sharing them with the rest of the other participating MGs (MGCs). In that way, it is possible to localize any operational issues, whilst at the same time, a global optimal solution for the entire system can easily be achieved [36]. To achieve a global optimum solution for the entire SG, each MG is required to try by all means to generate as well as store adequate capacities during operating times. In [37], a weighted multi-objective function-based approach is

suggested in which multiple MG operators can increase or decrease the weight of functions according to the state of the SG. For instance, they will direct on the capacities of ESSs as well as the number and capacities of (DERs). The approach appears to have gained wide recognition, even though elementary issues such as demand and supply balances and outage management are not considered. Thus in [38] decentralized architectures are explored in which a coordinated outage management strategy is emphasized. The simulation results carried herein demonstrate multiple contingencies of outages are effectively managed by such an architecture. A study in [39], investigates an outage management strategy for SGs that focuses on elevating the stability of the SG. In this regard, a generalized optimization model is formulated as a mixed-integer linear programming problem.

The authors in [40], further extend the work already done on decentralized system architectures. Their focus is on enhancing the self-healing capabilities of both SGs and MGs. Each MG quantifies its supporting power capability autonomously. A double stage decentralized MGNC for the SG is proposed in [41]. Management-related data is periodically shared. In this respect, the work in [42] further advances this study by employing a game theory-based decentralized in analyzing the impact of incorporating private ESSs (mostly owned by individual households) in improving the resilience and stability of a single MGC. Proposed in [43], is a power-sharing algorithm for hybrid SGs under different operating scenarios, notably normal versus emergency operating modes.

To further enhance the resilience of the SG, a peer-to-peer power bartering framework is proposed in [44]. In this case electrical energy sharing is fascinated directly between peer MGs without the involvement of the SG operators. The authors, however, did not take into consideration, incorrect power factor operations as well as load fluctuation controls. In any case, a major deficiency of the proposal is that the overall algorithm involves too many iterative calculations before attaining convergence.

## 2.2 Architectural Trends

The essence of standards and reference architectures is to promote and facilitate the representation and analysis, as well as systematic deployment SG architectures. Furthermore, this instantiation helps in providing a global view in depicting the different design and development scenarios as well as performing security analysis and risk assessment in a specific deployment context.

Table 2.1 summarizes these standardization and architectural design approaches.

Table 2.1: Standardization approaches [45]

| Domains | Responsibi lity towar ds SG technol ogy |
|---|---|
| T & D system operators | Develop business models, provide optimul planning for future T & D |
| Technology & solution providers | Provide technolog y solutions, develop standards with indusrty and government stakeholde rs |
| Internatio nal Governmen t al Organisati ons | Support th e RD & D of smart solutions, roadmap Smart Grid plans |
| Consumers | Actively participat e to Smart Grid; may generate, store, and manage the use of energy |
| Governemen t regulators | Collaborat e with sector stakeholde rs, provide Smart Grid deployment s |

Collectively the standardization and architectural design standards are geared towards achieving the following:

- Improvement of reliability and efficiency of the SG by way of enhancing synergy between increased network information and control technology.
- Promote the best possible degree of automation and its optimization of all available SG grid resources and operations.
- Integration as well as improved utilization of distributed resources and generation.
- Optimization of power supply demand and supply, by way of the utilization of effective demand/response techniques.
- Utilization and integration of modern electricity fueled transport
- We summarise some of these standards as follows;
- Institute of Electrical and Electronics Engineers (IEEE): This is a US based professional association that has developed study and working groups that focus on SG interoperability standardization [45]. These include IEEE P2030, a sub-working group's standard that provides a roadmap and directives (guidelines) for defining smart grid interoperability [46]. It

has since developed an SG interoperability reference model (SGIRM) which spells out desirable characteristics, for SG interoperability and general architectural design and operations to ensure reliability and flexibility. The IEEE P2030 looks at the main integrated architectural entities in the SG, such as; the power grid systems, and the ICT subsystem [56]. The IEEE P2030.1 (which is an addendum to the IEEE P2020) specifies equipment and planning requirements for power transmissions within the SG.

- International Electrotechnical Commission (IEC) specifies the general requirements of smart grid architectures and SG efforts. These efforts were delegated to a subgroup called the IEC Smart Grid Strategic Group in 2008 [47] and has since defined twelve service areas, identified over 100 IEC standards, and at the same time examined 44 recommendations. In addition, IEC 61970 and IEC 61968 address the relaying of information, handling of heterogeneous as well as diverse legacy devices in the distribution grid and ensuring successful SG deployment [48]. The IEC 61850, specifies electrical substation automation covering data modeling [49]. IEC 62351 standard focuses of security issues in the SG. [50].

Other standardizing bodies include,

- American National Standards Institute (ANSI [52].
- National Institute of Standards and Technology (NIST [51].
- International Council on Large Electric Systems (CIGRE): [52].
- International Telecommunication Union Standardization Sector (ITU-T) [53].
- Japanese Industrial Standards Committee (JISC [54].
- European Standardization Mandate M441 and the Smart Meter Coordination Group [55]:
- Smart Grid Standardization Mandate M/490 to European Standardization Organizations (ESOs [56].
- State Grid Corporation of China: [57].
- International Organization for Standardization (ISO [58]).

### 2.2.1 Islanded Microgrids

In the long term, this gradual increase in the incorporation of RESs might trigger instability in power grids if it is not regulated and managed properly. In this regard, the MGs are gradually gaining popularity in the sector. By definition, an MG is a domain of interconnected loads and DERs. It can operate in autonomous (islanded) mode [59], [60], or grid-connected mode. Whereas an MG can operate in on-grid or islanded modes, the islanded mode provides a more appropriate solution to electrifying rural areas or isolated communication facilities or military posts. In other words, an islanded MG (IMG) is ideal for supporting the provisioning of power supply to isolated loads, and at the same time, facilitating the integration of RESs into a reliable electricity supply system, reducing carbon footprint, and ultimately lowering energy prices [61]. A typical IMG will comprise of distributed generators (DGs) such as micro-turbines (MTs) diesel generators (DGs), and renewable generators (RGs) such as PV panels and Wind turbines. In addition, various strategically located ESSs in the form of battery banks, fuel cells, flywheel technologies, etc. are under intensified development. This offsets the lack of inertial storage inherent in traditional rotary synchronous generators.

As mentioned before, the uncontrolled high penetration of RGs, may compromise voltage stability, resiliency, robustness, and operation management optimization of the IMG. Significant challenges related to this penetration span supply reliability; frequency fluctuations induced by load intermittency; operational coordination of multiple RGs with possible conflicting requirements; coordination between supply EMS and DSM; robustness of entire system; and protection scheme co-ordination; ESSs sizing and optimization; incorporation of EVs and IoT related technologies.

Thus, to mitigate these issues and challenges, several control and energy management frameworks are being investigated. Both centralized and decentralized control framework architectures have been explored. The latter implemented as a hierarchical control architecture appear more practical given that they are organized in multiple distinct levels which can individually differentiate the multiple response times of IMGs. The first level of control is characterized by the quickest turnaround time (typically in the order of milliseconds) and is mostly associated with local measurements. The middle-level control layer (secondary control) is relatively slower (in the order of minutes) and typically oversees the PC [62]. The last control layer (tertiary control) is relatively sluggish and guarantees long-term operations [63], [64]. The operating policies of the IMG are set by external agents. Normally the external agents take into consideration factors, such as energy pricing, and energy consumption in the IMG. A loading manager system (LMS) module manages

the IMG power's demand and supplies to within certain defined goals. Typically, it will encourage power selling by consumers when it is conducive to do so with the goal of minimizing the IMG cost and peak-to-average ratio. This is achieved by applying various techniques [65]. The EMS is also dedicated to the overall managing and monitoring of energy flows (exchanges) among all the DGs and loads by way of timely scheduling. The IMG EMSs can be categorized in accordance with their architectural framework design and implementation layout. The centralized architecture though characterized by simplicity in implementation suffers from high computational and infrastructure costs, low reliability, and low flexibility. The decentralized architectural framework is often highly reliable, flexible as well as coupled with low computational and infrastructural implementation costs. Note however that its implementation is relatively complex since it might not attain a comparable optimal performance. Thus, the distributed scheme combines the best features of centralized and decentralized architectures. It is reliable, flexible and at the same time has a low computational burden [66], [67].

Overall, the IMG concept is geared towards integrating as many renewable sources as possible into the SG. It will interconnect a variety of distributed energy resources (DER) with different types of consumers in LV or MV distribution network. Most commercial DGs deployed at the distribution level, such as Solar PV and Wind are inherently stochastic. There is a need to manage these resources optimally to leverage the IMGs techno-economic benefits [68].

The EMS of the IMG incorporates several application services related to load/generation forecasting, SCADA, and Human Machine Interface to implement decision-making strategies. The whole process is carried out through the Microgrid Central Controller (MGCC), where DERs and controllable loads receive the optimal decision signals from the MGCC [69]. The MG EMS executes several functions such as exchange of power and market-related services at the utility level, optimal dispatch, and control of units at DER level and load level.

While most of the MG optimal scheduling strategies optimize the performance of DGs from the generation side, the steady rise in annual consumption is pushing the limits of grid capacity. One way to promote the locally generated DGs and influence the cluster of controllable loads is to employ DSM programs. Moreover, additional storage facilities investment will be reduced with proper management of consumer demands [70]. Several DSM strategies, such as load shifting, peak clipping, and flexible load shaping have been introduced to enable the interaction between IMG operators and consumers. Implementation of these strategies yields several benefits like OPEX cost

minimization, load curtailment, and energy efficiency enhancement [71]. The reported literature on the economic and technical aspects of EMS is diverse in objectives and proliferating in the field of research on MGs.

The application of DSM strategies in solving day-ahead optimal scheduling problems of IMGs is gradually gaining importance. These strategies will enable customers to change their energy consumption patterns thus assisting the IMG operator in reducing operational costs. The authors in [72] present a constraint-based DSM approach to minimize the operating costs and emission pollution and enrich customer satisfaction under high wind energy penetration. The coordination of shiftable loads with the volatile power output of wind energy is studied in this work. Direct Load Control is one of the popular DSM programs implemented for load shifting, peak clipping, etc. However, it offers limited freedom to consumers due to its intrinsic reliance on load shedding and its timing. The multi-energy DSM for a heterogeneous ESU is incorporated into an IMG EMS in [73]. The above research investigates the risk-averse model of both electrical and thermal storage in a residential MG to obtain flexibility in its operation. In [74], a Neuro-Fuzzy based flexible load priority list is developed to identify different curtailable load categories and reduce the energy import from the utility with high tariffs.

In [75], a multi-energy dispatch strategy is proposed to schedule power, heating, and cooling loads based on a day-ahead energy market. The non-linear models of combined heat power plants are linearized into mixed-integer linear programming to enhance the dispatch flexibility under grid-connected and islanded modes. In [76], the authors integrated weather-forecast data related to solar PV into the Markov decision framework and formulated the stochastic EMS problem. Naïve heuristic policies are proposed to quantify the 'feasible decision state-space to handle the supply-demand uncertainties using stochastic dynamic programming. A scenario-based stochastic model is presented in [67] to investigate the IMG's economic and security constraints. As opposed to stochastic programming, a new robustness factor is incorporated to enhance each generated scenario's robustness and accuracy. In most cases, the scenario generation approach is not feasible due to the heavy computational burden. The alternate approach to quantify the uncertain parameters is to identify the viable 'uncertain space'. The IMG dispatch is formulated as a two-stage adjustable robust optimization problem in [77]. The uncertainties factors are aggregated and 'polyhedral uncertainty space' is characterized to obtain dispatch solutions without over-conservativeness.

Apart from the intermittent energy sources, the uncertainty involved with scheduled load demand could also create a challenge to balance it with the supply. For example, EV random charging could

create stability concerns in an MG network. From this viewpoint, a separate EV charging station is modeled in [78] as a load and incorporated with EMS by employing Mixed Integer Distributed Ant Colony Optimization. A deep-learning-based forecasting algorithm is used in this case to forecast the PV power in a 10-minute timeframe. In [79], the stochastic loads and power flows are considered for energy management on a distributed framework. The authors have formulated the non-convex optimal power flow problem on a centralized layer and decomposed it to the distributed problem using the "predictor-corrector proximal multiplier" method.

Unlike the standard day-ahead scheduling problems with a time step of 1-hour, specific MG configurations will have a non-integer value in energy transit time. This intra-hour optimal dispatch model which is based on a centralized EMS framework is considered in [80]. However, these dispatch models with more elaborate time steps could result in a heavy computational burden, especially when multiple energy sources are involved. One such EMS strategy based on the Rolling Time Horizon technique is studied in [81] featuring high computational costs. In contrast to this technique, the Adaptive Neuro-Fuzzy Interface System-based EMS yields better results in computation. In this work, the authors have synthesized machine learning-based EMS models and proposed a graphic tool to analyze the MG energy flows. The effect of DSM and managing controllable loads is not considered. Multiple MGs are interlinked to form a 'networked microgrid' to enhance smart distribution networks' security, reliability, and resiliency.

Numerous studies have focused on the operation and planning of networked MGs in the presence of multiple intermittent sources. For instance, the probabilistic day-ahead scheduling problem is proposed in [82] to coordinate the local generators through a central controller. The impact of DR programs such as time-of-use and real-time pricing on optimal scheduling of networked MG is investigated in the above work. The probability distribution of uncertain parameters is obtained using Monte Carlo simulation. In a similar research work [83], the explicit effect of battery degradation costs on day-ahead optimal scheduling problems is investigated. A stochastic framework is designed to analyze the depth of battery charging and discharging capacity and solved using a Rainflow algorithm under different scenarios. In most of the previous works, the microgrid EMS problem aims to reduce the operating costs only. The assimilation of DSM tactics into the EMS problem is reported in very few research works. In contrast to these works, the flexible load shaping strategy is introduced in recent research work [84] to enhance utility and MG energy exchange costs. The overall operating cost of grid-connected MG is significantly reduced with DSM participation. However, the bid costs of DG units in the MG are considered convex with quadratic cost

coefficients. The throttling losses incurred in DG units are often neglected in the literature [85]. This phenomenon is addressed as the "valve-point loading effect" (VPE), and by considering the DGs with VPE, their cost function will become non-convex, non-smooth, and non-differentiable. A novel attempt is made to formulate the day-ahead dispatch problem of microgrids in DGs presence with a non-convex cost function to address the research gap discussed earlier. Further, the effect of load dynamics with DSM participation is also incorporated and is investigated. Most traditional optimization algorithms fail to solve the non-convex problem because the solution often gets trapped in the local optima [75]. Therefore, in this research work, a novel Quantum Particle Swarm Optimization (QPSO) algorithm is introduced to solve the EMS problem to optimize MG's day-ahead scheduling in DGs' presence with non-convex cost function and load dynamics.

### 2.2.2 IMG Model

A generic model of IMG comprising dispatchable and non-dispatchable DERs is adopted in this work. As shown in Figure. 2.5, three feeders namely residential, commercial, and industrial feeders in the MG are connected to the utility via the point-of-common coupling. Solar PV, Wind turbine (WT), Diesel Generator (DG), Micro-turbine (MT), and Fuel Cell (FC)are considered to provide energy to both curtailable and non-curtailable loads in MG. The MGCC will assign the power reference values to the local controllers for scheduling the required loads. The energy generation profile for the non-dispatchable sources like PV and WT units and load demand profile can be forecasted before 24 hours for day-ahead scheduling. The local controllers at each DER will receive the corresponding generation set points from the MGCC as per the optimal schedule. The system data related to generation and load forecasts, market prices, and DER bids, along with nonconvex cost coefficients are taken from [30].

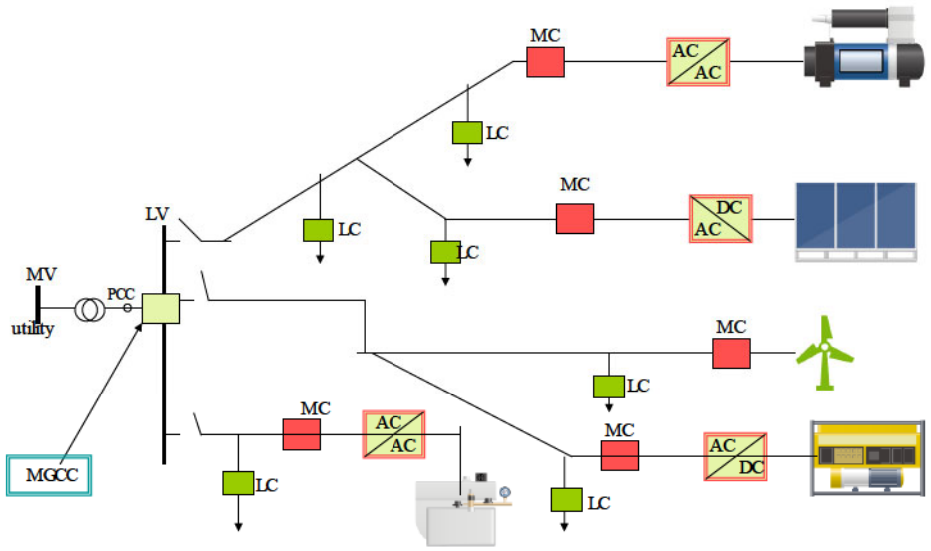


Figure 2-5: Generalised Model of an Islanded Microgrid

*A: Modeling of DG Units*

MGs with embedded distributed generation and ESS devices are expected to assume growing significance in future power systems. However, achieving efficient distributed economic dispatch in MGs is still a challenge in part due to stochastic phenomena and nonlinearity in DG units and loads.

*Solar PV*

Solar PV (photovoltaic) systems, generate dc power using an array of parallel-series interconnected photovoltaic modules. Primarily, the array absorbs sunlight and then consequently converts it to dc current which flows to a DC bus or through DC-AC conversion to an AC bus. PV generators are mainly characterized by three key factors i.e., solar irradiance ($w/m^2$), ambient temperature ($T_{amb}(^oC)$, as well as overall PV characteristics in determining their output power performance. Thus a PV generator output power ($P_{pv}$) is computed according to

$$P_{pv} = P_m \frac{1}{100}(1+\rho(T_{pvc}-25),\ watts \tag{2.1}$$

where; $P_m$ (watts) is the maximum power of the PV module generator under standard test conditions, $\rho(^oC^{-1})$ is its temperature coefficient, and $T_{pvc}$ is the PV cell temperature in degrees Celsius ($^oC$). $T_{pvc}$ is related to $T_{amb}(^oC)$ and the module's nominal temperature ($T_{NT}$) as follows:

$$T_{pvc} = T_{amb} + \frac{1}{800} * (T_{NT} - 20) \tag{2.2}$$

*Wind Turbine Generators*

Wind turbine (WT) generators rely on wind power to drive an electric motor-generator. Typically a WT generator structure comprises a tower, and rotor with three blades connected at the hub. When the wind passes over the blades, it exerts a turning (rotating) force, which in turn rotates an electrical motor. Ultimately electricity is generated. The power output of a WT generator (3) depends on the available wind speed $v(m/s)$ as well as the power generation characteristics of the WT generator unit itself.

$$P_{WT} = \begin{cases} 0, & v_{ct} < v \le v_{cn} \\ \frac{v^2 - v_{cn}^2}{v_n^2 - v_{ct}^2} \times P_{nWT}, & v_{cn} < v \le v_n \end{cases} \tag{2.3}$$

This is subject to;

$$P_n, v_n < v \le v_{ct} \tag{2.4}$$

where, $P_{nWT}$, $v_n$, $v_{cn}$, and $v_{ct}$ are the nominal WT generator power (watts), nominal speed ($m/s$), cut-in velocity ($m/s$), and cut-out-speed ($m/s$) respectively.

*Diesel Generators (DG)*

DG units comprise fossil fuel-based engines coupled to an electric synchronous generator to produce electrical energy. The DG operates based on compression and decompression diesel fuel. Air is blown into the generator until it is compressed. Under high pressure, it is directed towards the turbine's blades whence its kinetic energy causes a turning effect. The DG's fuel consumption $F_{DE}$ is normally characterized by its $kW$ power rating according to [75]. This quadratic cost function can be modified to a non-convex function of its valve–point loading effect (VPE) as follows:

$$F_{DE} = a_{DE}^2 + b_{DE}^2 + c + d \sin\left| eP_{DE} - eP_{DE}^{\min} \right| \tag{2.5}$$

Where, $a, b, c, d$ and $e$ are non–convex coefficients of the diesel generator, $P_{DE}^{\min}$ and $P_{DE}$ represent the minimum and nominal power outputs from the diesel generator respectively.

***Microturbine (MT) and Fuel Cell (FC)***

A fuel cell, via an electrochemical redox reaction, converts the chemical energy of a fuel, often hydrogen and an oxidizing agent, oxygen into electricity. Fuel cells require a continuous flow of fuel and oxygen (usually from air) to sustain the chemical reaction, whereas in a battery the chemical energy usually comes from metals and their ions or oxides that are commonly already present

in the battery, except in flow batteries. FCs can continuously produce electricity for as long as $H_2$ and $O_2$ are supplied. Like DG, the cost function of the *MT* is considered as non-convex to address the VPE; it can be expressed as follows:

$$F_{MT} = aP_{PM}^2 + bP_{MT} + c + d * \sin\left|eP_{MT} - eP_{MT}^{\min}\right| \tag{2.6}$$

Where, $P_{MT}, P_{FC}$ are the power outputs of $MT$ and $Fc$, $P_{MT}^{\min}$ is the minimum power output obtained from $MT$. The cost of power output from the fuel cell is usually calculated as per the bids:

$$B_{FC} = C_f \frac{P_{FC}}{\eta_{FC}} + C_{inv} \tag{2.7}$$

Where, $C_f$ is the cost of the fuel to operate $FC$, $\eta_{Fc}$ is the fuel cell efficiency, and $C_{inv}$ is its annual investment cost.

#### 2.2.3.1 Example IMG Problem Formulation

The traditional optimal scheduling problem consists of the standard convex quadratic cost function for DG units. As discussed earlier, with the involvement of VPE, the DG cost function will become non-convex [88]. Hence, our paper's main objective is to solve the *MG* optimal scheduling problem by considering a non-convex DG cost function. Further, the EMS will utilize the flexible load shaping DSM strategy to optimize the energy exchange between utility and MG subjected to dynamic load demand changes. The microgrid's total operating cost includes the fuel cost coefficients of DG units, start-up/shutdown costs, and the utility's market bid price as represented in (2.8). The mathematical representation of the MG-EMS problem is given as follows:

$$\text{Min E}(\alpha\alpha = \sum_{t=1}^{T} OC \sum_{t=1}^{T} \left\{ \sum_{i=1}^{NG} \left[ u_i^t B_{DG_i}^t P_{DG_i}^t + S_{DG_i} \left| u_i^t - u_i^{t-1} \right| \right] + p_u^t B_{grid}^t \right\} \tag{2.8}$$

where;

$$B_{DG_i}^t = \alpha_i p_{G_i}^2 + b_i p_{G_i} + c_i \tag{2.9}$$

$$P_{DG_i}^t = \alpha_i p_{G_i}^2 + b_i p_{G_i} + c_i + d_i \sin\left| e_i p_{G_i} - e_i p_{G_i}^{\min} \right| \tag{2.10}$$

$$\alpha = \left[ p_{G_1}^t, p_{G_2}^t, \ldots, p_{G_N}^t, p_{ut}^1, u_1^t, u_2^t, \ldots, u_i^t \right] \tag{2.11}$$

In general, the bid costs of DG units are represented in (2.9) with quadratic cost coefficients $a_i$, $b_i$, $c_i$. The VPE for DG units is modeled with additional cost coefficients $d_i$ and $e_i$ as shown in (2.10), and $\alpha$ represents the decision variables of the $i^{th}$ DG unit power output, utility power exchange, and the ON/OFF status of DG units respectively.

*Active Power Balance*

The active power generation from all DG units and utilities must supply the total load demand $P_i^t$ at any given hour $t$ for $NL$ load levels. This active power balance is considered as an equality constraint to optimize the total generation costs in the MG.

$$\sum_{i=1}^{NG} P_{G_i}^t + P_{ut}^t = \sum_{l=1}^{NL} P_l^t \tag{2.12}$$

*Active power generation limits*

The active power output from all DG units and utility are bounded to their maximum ranges $P_{G_{max}}^t$, $P_{u_{max}}^t$ and minimum ranges $P_{G_{min}}^t$, $P_{u_{min}}^t$ respectively. These limits are specified as shown in (2.13).

$$\begin{cases} P_{G_{min}}^t \le P_{G_i}^t \le P_{G_{max}}^t \\ P_{u_{min}}^t \le P_{ut}^t \le P_{u_{max}}^t \end{cases} \tag{2.13}$$

Out of all DG units considered in the proposed MG network, the non-convex cost coefficients are assigned to MT and diesel generator set to address the VPE.

Table 2.2: DG Power Limits with Non-Convex Cost Coefficients

| ***Type*** | $P_{G_{min}}^t$ | $P_{G_{max}}^t$ | $a_i$ | $b_i$ | $c_i$ | $d_i$ | $e_i$ |
|---|---|---|---|---|---|---|---|
| MT | 90 | 300 | 0.062 | 21.15 | 819 | 252.73 | 0.043 |
| FC | 30 | 300 | 0.006 | 1.62 | 2204 | 0 | 0 |
| DE | 0 | 80 | 0.049 | 18.16 | 869.7 | 335.45 | 0.034 |
| WT | 0.01 | 599 | 0.01 | 5.99 | 0.01 | 0 | 0 |
| PV | 0.01 | 249 | 0.01 | 44 | 0.01 | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| UTILITY | 1999 | 1999 | - | - | - | - |

The DGs bid information and minimum and maximum generation limits are shown in Table 2.2 [76] [78]. The load forecast data and utility market price information are shown in Figure 2.6.

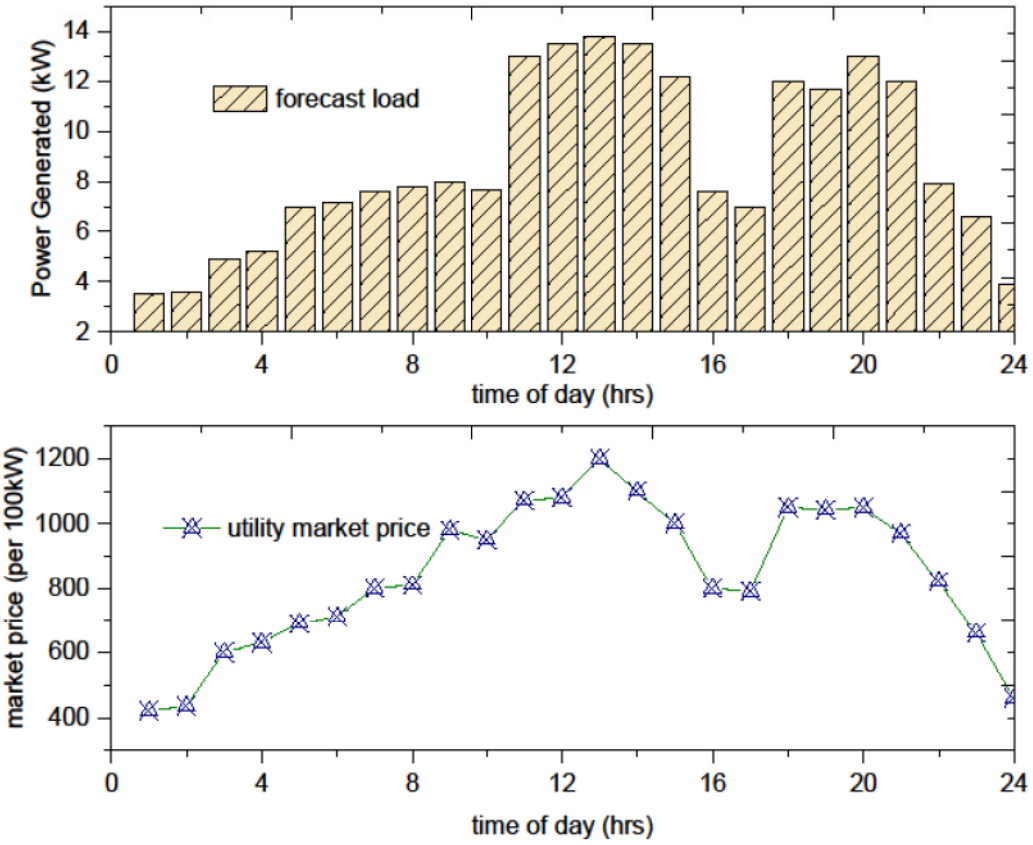


Figure 2-6: Forecasted Load and Utility Market Price

### 2.2.3.2 Methodology

This section deals with the modeling details for implementing a utility-induced DSM program and its incorporation into the EMS operational framework. A generalized framework for solving non-convex MG scheduling problems is presented in detail.

*Demand Side Integration*

The network operator enables consumers to participate in DSM programs to achieve financial goals and improve the system load demand profile. These strategies are broadly classified as utility-driven and customer-driven, as shown in Figure 4. The day-ahead optimal scheduling problem is incorporated with a flexible load shifting technique [65] with 10% and 20% DSM participation.

Initially, the DSM controller is fed with day-ahead load forecast data, and it implements necessary control actions to achieve the desired load profile. The controllable loads will receive the relevant control signals to either turn ON or schedule operation time via two-way digital communication technologies. Incorporating the DSM program into the proposed non-convex EMS problem is to bring the controllable load consumption profile like the desired load profile [65].

$$\text{minimize} \sum_{t=1}^{T} \left(TL(t) = DL(t)\right)^2 \tag{2.14}$$

$$TL(t) = \varphi(t) + \phi(t) - \Delta\phi(t) \tag{2.15}$$

The information related to targeted load $TL(t)$ is fed to the DSM controller to obtain the desired load profile $DL(t)$ at a given time interval $t$. Three factors influence the targeted load, namely predicted load $P_{pred.}(t)$, connected load $P_{con.}(t)$, and disconnected load $P_{dis.}(t)$.

$$P_{con.}(t) = \sum_{t=1}^{t-1} \sum_{i=1}^{N} N_{l,i,t} \circ P_{1,l} + \sum_{j=1}^{k-1} \sum_{i=1}^{t-1} \sum_{l=1}^{N} N_{l,i,(t-1)} \circ P_{(1+j)i} \tag{2.16}$$

The increment in connected load $P_{con}(t)$ is determined by shifting the number of $l$ type controllable devices to time $t$ and device connections scheduled before time $t$. Here, $N$ represents the number of $l$ type controllable devices that are transferred from time step 1 to $(1+j)$, and N is the total number of controllable device types. $P_{1,l}$ and $P_{(1+j),i}$ are denoted as the l type devices' load intake at time step 1 and (1+j), respectively, for a total duration of $k$.

$$P_{dis.}(t) = \sum_{q=t+1}^{t+m} \sum_{l=1}^{N} N_{l,i,q} \circ P_{1,l} + \sum_{j=1}^{k-1} \sum_{q=t+1}^{t+m} \sum_{l=1}^{N} N_{l,(t-1),q} \circ P_{(1+j)l} \tag{2.17}$$

Similarly, the disconnected load $P_{dis.}(t)$ is determined by a decrement in loads due to delay in connection times by shifting $l$ type controllable devices from time step $t$ to $q$ and delay in connection times of, $l$ type devices that are expected to be consumed before time $t$. The maximum permitted time delay is denoted by $m$.

$$\sum_{t=1}^{T} N_{l,i,t} \leq N(i) \tag{2.18}$$

$$P_{(1+j),l} = 0, \ \forall \ (1+j), l > T_D \tag{2.19}$$

$$N_{l,i,t} = 0, \ \forall \ (t-i) > m \tag{2.20}$$

Equation (2.20) represents the inequality constraint where the number of shifted devices at a given time $t$ cannot exceed the maximum available number of controllable devices $N(i)$ and the delayed characteristic of the DSM approach is shown in (2.17) and (2.18). [80],[81].

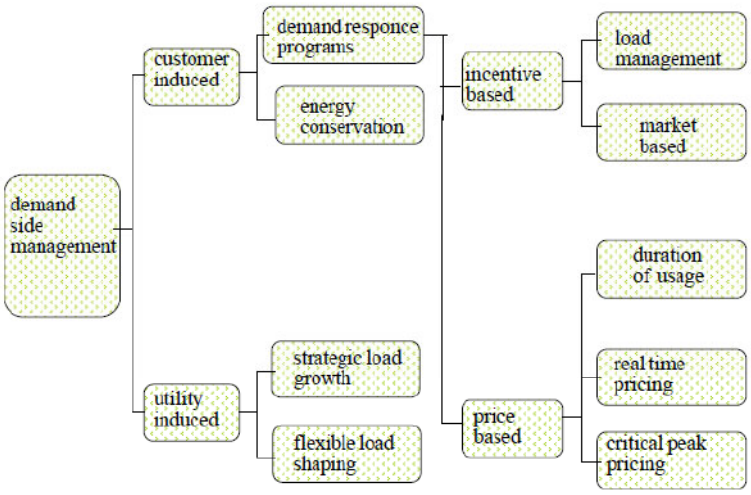


Figure 2-7: Classification of Demand Side Management Programs

*Proposed Framework*

The generalized framework to solve the proposed MG EMS problem is illustrated in Figure 2.8. Initially, the non-convex cost coefficients of the DG units are configured as per Table 2.2. Then, the MG system parameters related to the market price forecasted data of renewable generation, and loads are provided for day-ahead scheduling. The customers of industrial, commercial, and residential feeders will participate in DSM program and the modified load data are sent to the load controller for controlling non-critical loads. The impact of the proposed load shaping strategy on EMS is investigated by employing the QPSO algorithm.

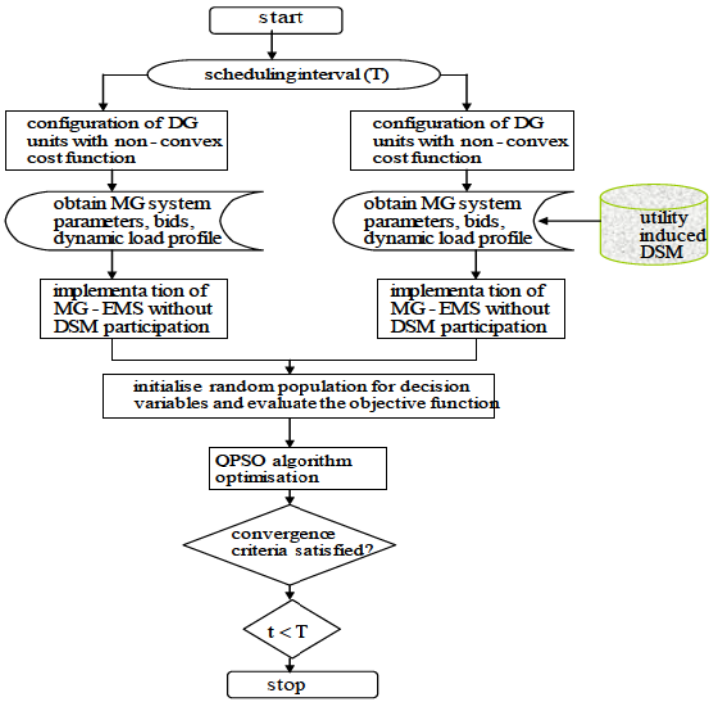


Figure 2-8: QPSO Flowchart for Solving Non-Convex EMS Problem

#### 2.2.3.3 Evaluation

*A) Simulation Evaluation*

The forecast data of renewable power generation, utility market price and loads are obtained from [89], and the values are tabulated in Table 2.3. The proposed EMS problem is solved in MATLAB environment using the QPSO algorithm with 30 trail runs. The simulation results are compared with its classical counterpart PSO to prove the efficacy of QPSO. The population size and the maximum iterations for both the algorithms are 50 and 200, respectively. The cognitive and social parameters for PSO are taken as 2; the maximum and minimum inertia weight constants are taken as 0.9 and 0.4, respectively. Several assumptions were made before implementing the algorithm as follows:

- The renewable power extracted from PV and WT is kept at maximum power point all the time.
- All the DG units in the MG will provide active power with power factor unity.
- Industrial, commercial, and residential loads are segregated into distinct load types and their dynamics are considered for DSM participation during peak hours.
- With these assumptions, four case studies related to the defined objectives are framed.

*Case- 1* deals with both convex and non-convex DG cost functions. The implementation of DSM program in the base case is neglected for the time being.

*Case- 2,* the DSM participation of 10% is evaluated with both convex and non-convex DG cost functions.

*Case- 3,* deals with the DSM participation of 20% with both convex and non-convex DG costs.

*Case- 4*, the dynamic loading for 15 minutes duration of 96-time intervals are considered and the results are evaluated with DSM participation of 15%.

A brief discussion of obtained simulation results for all case studies is given in the following sub-sections.

Table 2.3: Day-Ahead Forecast Data

| Time | PV(kW) | WT(kW) | Load(kW) | MP(Kwh) |
|---|---|---|---|---|
| 1 | 0 | 251.60 | 479 | 3.4 |
| 2 | 0 | 247.3 | 479 | 3.4 |
| 3 | 0 | 280.01 | 599 | 3.4 |
| 4 | 0 | 258.3 | 599 | 3.4 |

| | | | | |
|---|---|---|---|---|
| 5 | 25 | 290.55 | 719 | 6.9 |
| 6 | 55.35 | 297.01 | 719 | 6.9 |
| 7 | 65.33 | 245.91 | 839 | 6.9 |
| 8 | 112.55 | 256.95 | 839 | 6.9 |
| 9 | 160.22 | 214.98 | 959 | 6.9 |
| 10 | 165.5 | 229.99 | 959 | 6.9 |
| 11 | 187.33 | 246.33 | 1079 | 11.9 |

Table 2.4: Day-Ahead Forecast Data cont'

| Time | PV(kW) | WT(kW) | Load(kW) | MP(Kwh) |
|---|---|---|---|---|
| 12 | 195.51 | 297.1 | 1079 | 11.9 |
| 13 | 185.9 | 295.99 | 1199 | 11.9 |
| 14 | 189.302 | 314.01 | 839 | 11.9 |
| 15 | 140.01 | 289.91 | 839 | 11.9 |
| 16 | 138.9 | 280.1 | 960 | 6.9 |
| 17 | 60.59 | 289.1 | 1079 | 6.9 |
| 18 | 50.19 | 300.01 | 1097 | 6.9 |
| 19 | 36.98 | 3.31.92 | 959 | 11.99 |
| 20 | 18.05 | 300.93 | 839 | 11.99 |
| 21 | 11.76 | 291 | 719 | 6.9 |
| 22 | 0 | 280.1 | 599 | 6.8 |
| 23 | 0 | 280 | 719 | 6.9 |
| 24 | 0 | 279.99 | 619 | 3.4 |

*B) Simulation Results*

Case 1: Base Case

The obtained simulation results are shown in Figure 2.9, with convex DG cost function, the MT and FC supply with their maximum power limits and reduce power consumption from diesel generation most of the time. The MG's total operating cost with convex and non-convex DG cost function is 2,630 ZAR and 2,636 ZAR, respectively. The cost incurred in the base case is highest compared to cases 2 and 3 because the DSM participation is not considered.

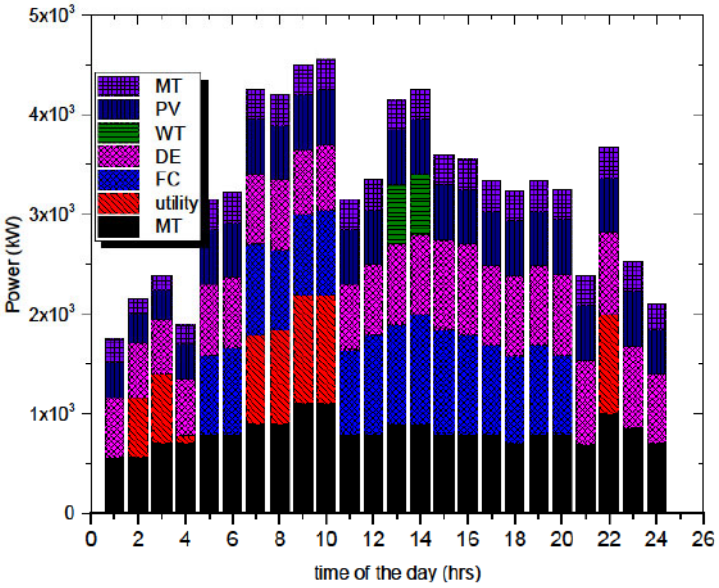


Figure 2-9: Non-Convex Cost

Case 2: Comparison of the convex and non-convex problem with 10 % DSM participation Figure 2.9 depicts the optimal generation schedule of DGs with a non-convex cost function. The total operating costs are minimized to 2582 ZAR with a reduction of 2.09 % in price in contrast to the case without DSM participation. Similarly, there is a 2.01% reduction in cost while considering convex cost function with 10% DSM participation. The flexible load shaping strategy helps the MG operator export more energy to the utility by reducing peak power, especially during the 11$^{th}$ -15$^{th}$ hrs.

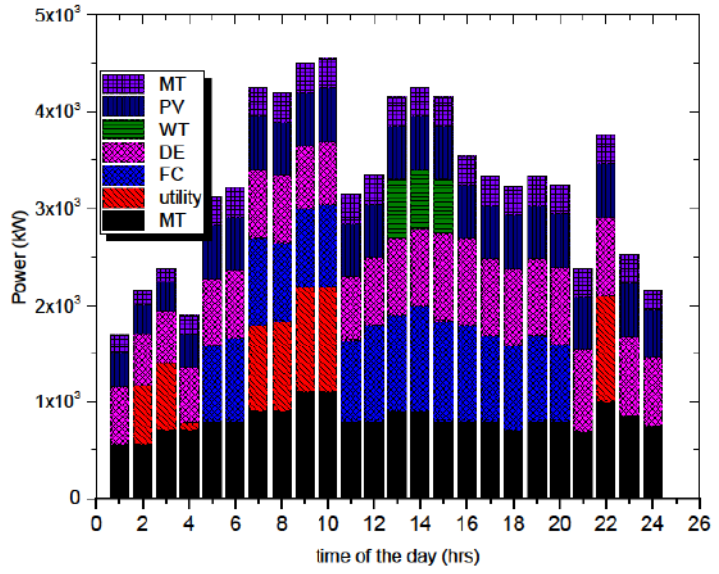


Figure 2-10: Case II, Non-Convex Cost

Case 3: Comparison of the convex and non-convex problem with 20 % DSM participation With 20% DSM participation, DGs' daily operating costs with Non-convex and convex cost functions are 2526 ZAR and 2522 ZAR respectively. In contrast with the case without DSM participation, there is a cost reduction of 4.354 % and 4.28% for non-convex and convex cost functions of DG units. The peak reduction and financial savings for this case are superior due to the highest DSM participation. Figure 2.10 shows that the utility's energy import is significantly reduced during 11$^{th}$ -21$^{st}$ hours with utility-induced flexible shaping.

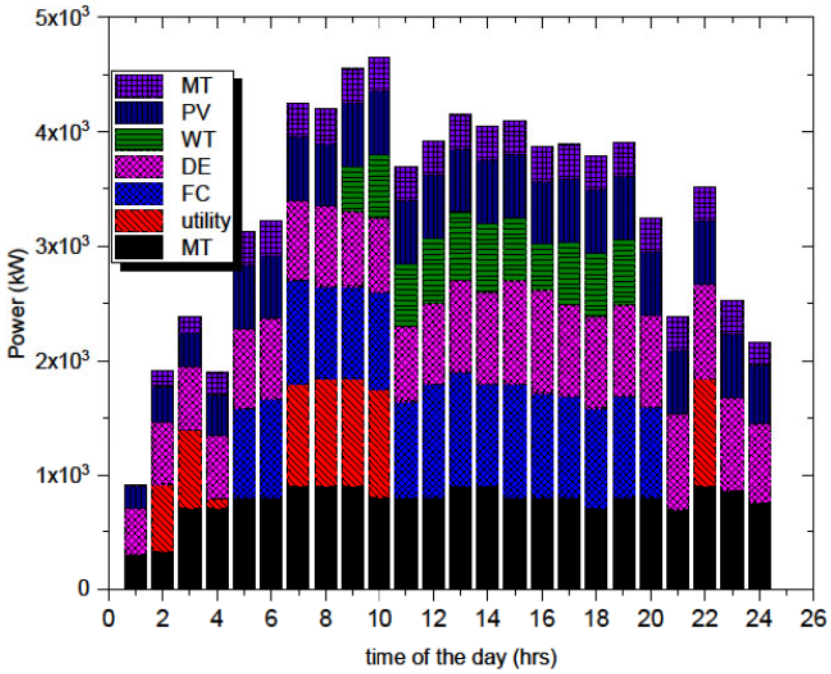


Figure 2-11: Case III, Non-Convex Cost

Case 4: Dynamic loads with 15 % DSM participation. The previous case studies attempt to solve the day-ahead MG scheduling problem on an hourly timeframe. However, the dynamic dispatch of loads with 15 minutes timeframe is considered in this case with 96-time intervals throughout the day. The curtailable loads from industrial, commercial, and residential feeders of MG will receive inputs from DSM controller either to turn ON the device or scheduled turn ON period in case of peak loads. This is shown in Figure 2.11.

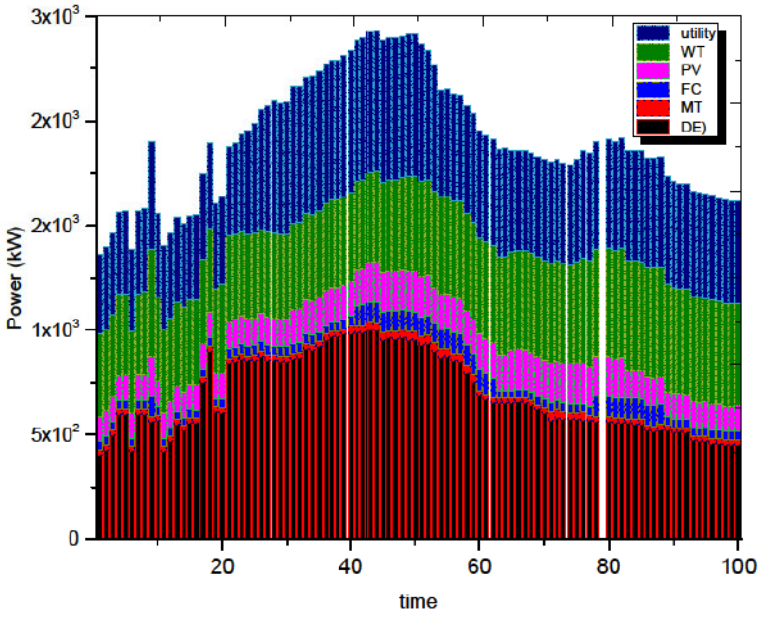


Figure 2-12: Simulated Results of Case 4

With this regard, the dynamic dispatch of loads with 15% DSM participation is evaluated in this case. The total operating cost for the scheduled 96 intervals is incurred as 3350 ZAR. Since the diesel generator set has the highest bid cost, its consumption is restricted to the minimum value. This is shown in Figure 2.12.

From the obtained simulation results, it is evident that the proposed QPSO optimization algorithms yield superior results while solving the non-convex EMS problem. A comparison of best, mean, and worst values of costs with the PSO algorithm is given in Table 2-5 to prove its efficacy.

Table 2.5: Performance of QPSO and PSO

| PSO | | | | |
|---|---|---|---|---|
| | best | worst | mean | Time(s) |
| convex | 2588.3 | 2590.1 | 2292.3 | 59.7 |
| Non-convex | 26 27.3 | 2629.1 | 2930.1 | 73.1 |
| QPSO | | | | |
| | 2589.1 | 2590.7 | 2592.1 | 49.7 |
| | 2629.1 | 2630.7 | 2632.1 | 51.2 |

The daily optimized costs for the proposed MG network in the presence of Non-Convex DGs are tabulated in Table 2-6.

Table 2.6: Optimized Costs in Rands with Different DSM Participation Levels

| | level | convex | Non-convex |
|---|---|---|---|
| Case I | - | 2589.1 | 2592.0 |
| Case II | 9% | 2595.2 | 2598.1 |
| Case III | 19% | 2561.7 | 2568.1 |
| Case IV | 16% | - | 3319.1 |

With different participation levels of DSM, it is observed that the flexible load shaping strategy effectively reduces the costs in all cases in contrast with the base case.

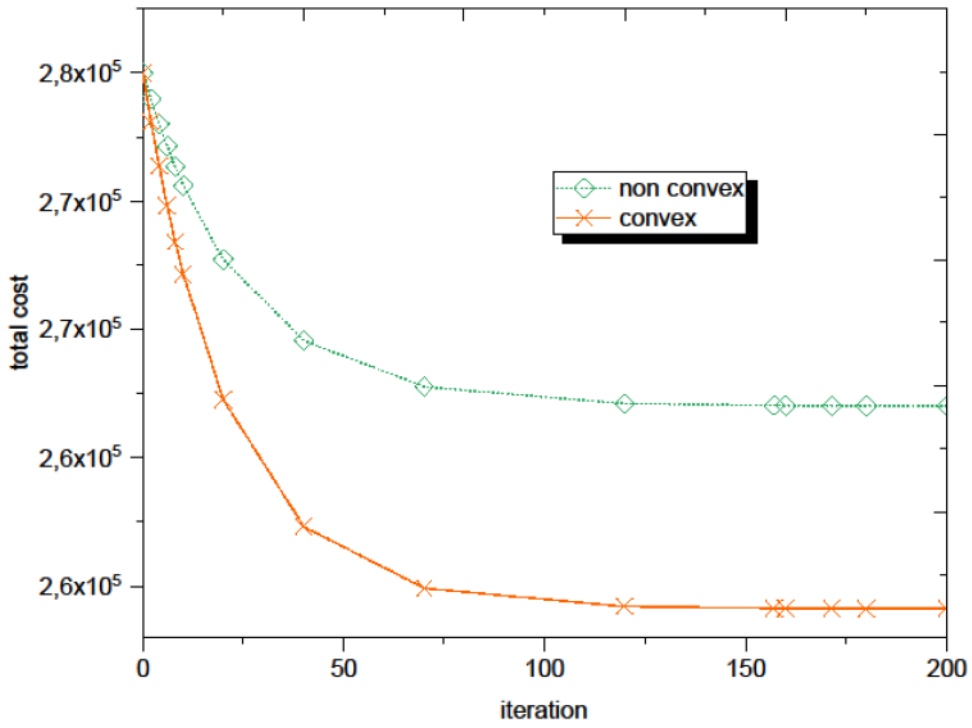


Figure 2-13: Convergence Characteristics for the Base Case

And further, due to the valve-point-effect characteristics of DG units, it is evident that the costs incurred for the Non-Convex DGs are more than the convex cost function of DG units.

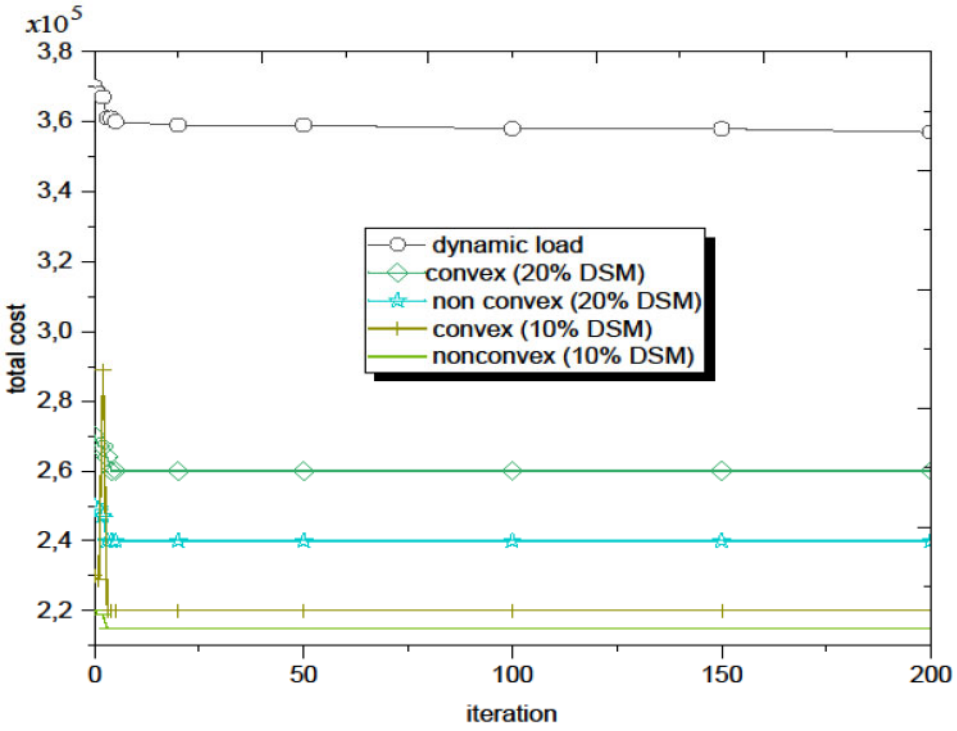


Figure 2-14: Convergence Characteristics of QPSO with DSM Participation

As discussed earlier, the QPSO outperforms its classical counterpart in terms of solution efficiency and computational time. Figures 2.13 and 2.14 represent the convergence characteristics of the proposed QPSO algorithm without and with DSM participation, respectively. It is observed that the proposed algorithm yields a robust solution within very few iterations.

## 2.3 Communication Subsystem and Technologies

The SG system is a result of blending ICT technologies to legacy and existing traditional power grids. In that way, it becomes relatively easier to integrate renewable as well as the new distributed generation system, Overall this will result in an efficient as well as a resilient power system. In a way, an SG is a power grid system that integrates the ICT subsystem and power management hardware devices to bring about seamless inter-operation abilities among different advanced components of the system for efficient utilization of the energy [90].

### 2.3.1 Architecture

The key architecture comprises three layers namely the communication, power, and applications layers [90].

- Power Layer: This includes the power generation and customer premises network systems. The layer integrates the traditional predicted generation systems with the less predictable renewable sources. It also has since replaced the normal simplex power flow with the duplex flow. In that way end, users can participate in both generation as well as trading of power. A notable effect of such an arrangement is that there are better capabilities of balancing demand and supply in the SG grid system.

- Application Layer: It encompasses several services and applications and facilitating interoperability among them. Typical such services and applications include advanced metering infra- structure, outages monitoring, faults monitoring, demand response management, asset management, fraud detection, and security.

- Communication Layer: It is the core ICT subsystem facilitating connectivity among the various entities constituting the SG grid.

- Note that legacy and traditional electrical grids suffer from drawbacks namely;

- Fragmentation of architectures
- Inadequacy of bandwidth for achieving duplex connections
- Incompatibles resulting in inter-operability difficulties between system components;
- Inabilities to handle increased volumes of data from smart-enabled devices.

It is also noted that the SG grid's supporting ICT subsystem can be private or public. The public infrastructure in this case would be the IoT public infrastructure. Relying on the public IoT infrastructure would result in increased security risk threats as such networks are shared. The private infrastructure will generally be dedicated and only accessible in-house. For that reason, it would have relatively fewer security risks threats. Performance-wise, it is also likely to render a more enhanced Qos than public network infrastructures.

The communication layer comprises three categories, namely a home-area network (HAN), a field-area network (FAN), and; a wide-area network (WAN).

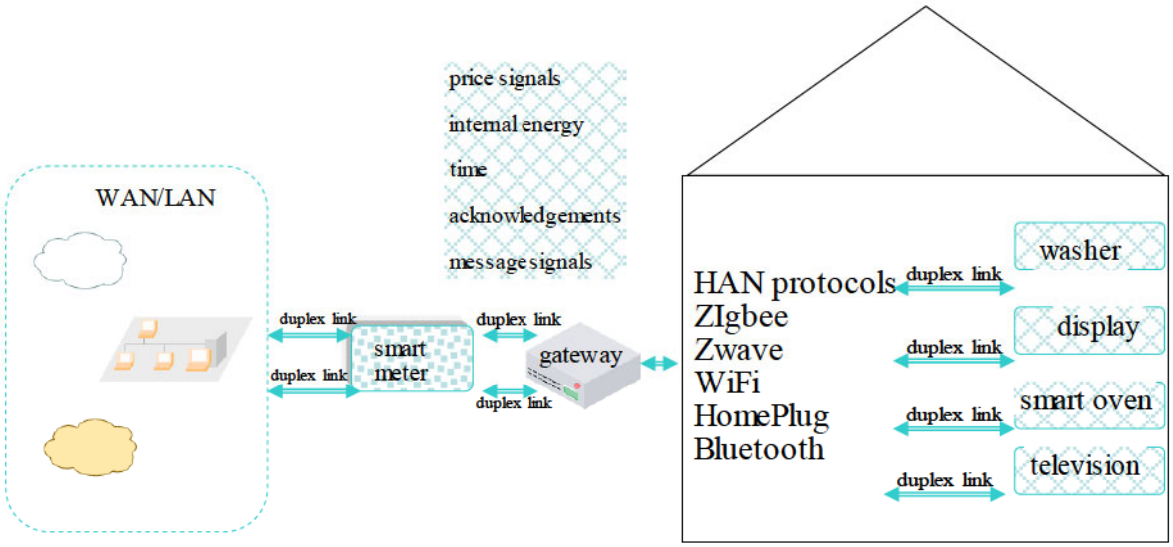


Figure 2-15: Energy Management Using Various Technologies in an SG

HANs, FANs and WANs are interconnected via access points, back haul, and core networks. The communication links between the three key entities (HANs, FANs and WANS) is facilitated using various media such as wireless, wired, or optical [90]. The choice of a medium will depend on the volumes of data to be exchanged. That is, in sections where there are large volumes of data, we certainly would go for an optical medium as it provisions much greater bandwidth, typically in the order of Terahertz ranges. A brief account of the various categories of transmission is as follows:

**WAN**:

A WAN generally spans vast distances, typically between substations and power utilities. It should be able to provide connectivity among all key entities of a vastly spread SG. Normally its links should be able to provide high bandwidths capabilities hence coaxial and, optical cables will be candidate media to facilitate such high bandwidth provisioning. The links normally employ more complex multiplexing techniques such as Dense wavelength division multiplexing (DWDM) or other forms of spatial multiplexing.

A WAN employing both DWDM and optical burst switching is illustrated in Figure 2.16.

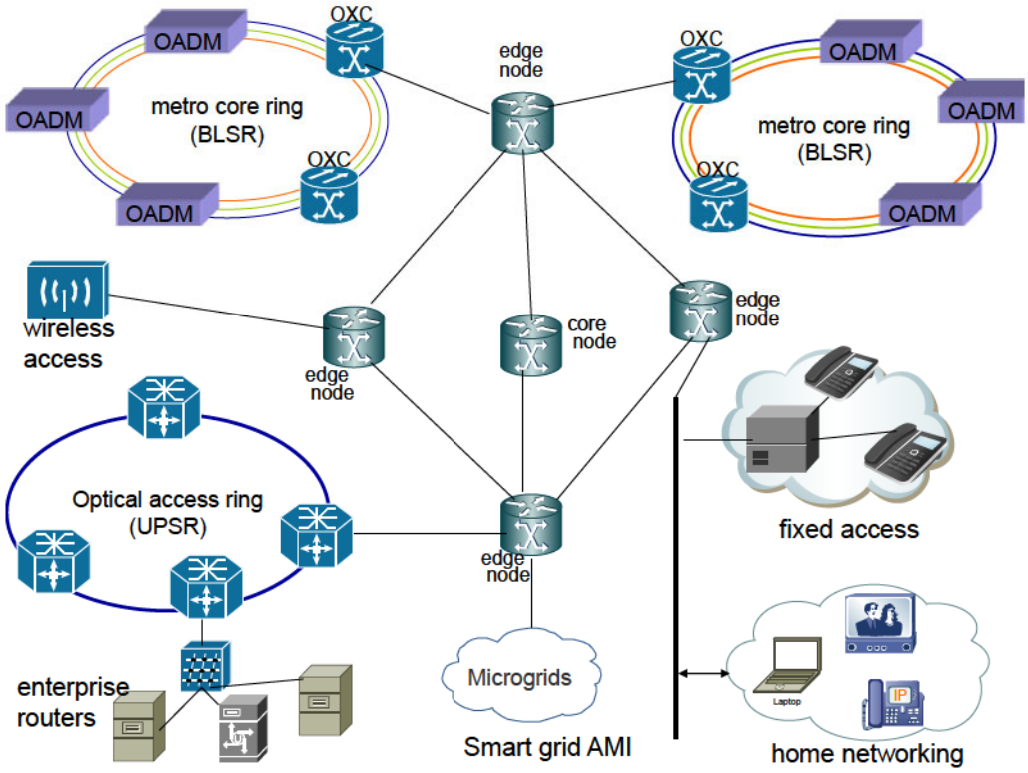


*Figure 2-16:* Generalized Communications Network Infrastructure

The WAN will generally accommodate both duplex and simplex communications typically needed for automation, coordination, and monitoring purposes in an SG domain. Sockets are typically employed for each SG application running on a WAN, thus each communication will be able to specify its QoS requirements. The introduction of IP version 6 in IoT makes this relatively easy. E.g., this networking protocol can differentiate QoS handling among individual communication stream

**FAN**

This is mostly provisioned for facilitating communications between end-user networks and substations. They also provide linkage between users and data concentrators. They typically spread over urban-suburban and countryside. FAN communication media will depend on the running SG applications. The use of optical cabling is not uncommon since this medium provides excellent bandwidth and thus high QoS capabilities (e.g., low latencies, and data losses). Wireless access technologies such as WiMAX are also incorporated in this category. The existing GSM infrastructure can also be utilized. Of late, there is much preference for the usage of IEC 61850 as it facilitates improved device-to-device (D2D) communication.

**HAN**

This is conveniently located in homes to provide the necessary regulation of power usage in the form of monitoring and control over its usage. SMs directly connect to it. In that way end-users can monitor their power usage and at the same time, the SG utility can remotely acquire power usage, i.e., AMR. The utility is also able to regulate power usage by home appliances to save power especially when demand is quite high. This section of the network may use wireless or PLC communications. The Association of Home Appliance Manufacturers (AHAM) recommends the use of link technologies such as ZigBee, Wi-Fi, Home Plug, Z-wave, and M-Bus. E.g., ZigBee can operate in a mesh configuration with added advantages, such as sleep mode. Note that the sleep mode operation of appliances has the distinct advantage of conserving energy. Z-wave is immune to RF interference and hence ideal for remote controlling of appliances [92], [93].

### 2.3.2 Operation and Services

The SG paradigm requires an enabling ICT communication infrastructure to provide both simplex and full-duplex connectivity among key entities thus sustaining energy exchanges among intelligent components and processing of data derived from the various applications and services. The services and applications play a vital role including innovations. Typical examples include, but are not limited to innovative approaches to power demand-side management, strategizing in grid energy storage, timed discharging of ESSs for load balancing, smoothing of power flows due to the intermittent generating nature of renewable sources, preventing power outages, integration of EVs, power factor corrections, and matching the generation and load balances. All this is summarized in Figure 2.17.

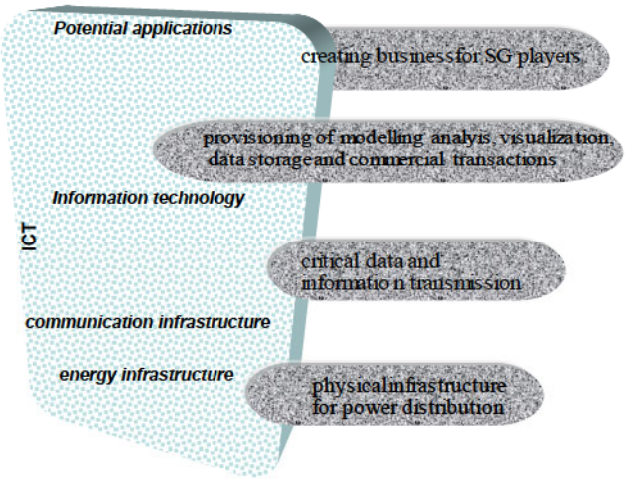


Figure 2-17: Integrated Energy Infrastructure Representative of a Typical SG

Thus, as far as the core function of power generation, transmission, and distribution is concerned, the ICT subsystem is facilitating the key exchange of information among entities throughout the SG. It also provides a platform for analysis and visualization. It is also pivotal in the control, monitoring, and maintenance of the entire system in an efficient manner. Before spelling out the various existing and would-be services and applications, we first need to discuss their communications requirements.

### 2.3.3 Applications and Communications Requirements

There is diversity in applications and services, and so are the requirements. E.g., individual services and applications have varying QoS demands. It is therefore imperative that the communication capability of the SG should be fail-safe (reliable) n order to make the operations of the SG grid successful. Typical communication requirements include the following:

- End-to-end delay: End-to-end delay refers to the time lapse between transferring data from sender to intended recipient. It is also referred to as latency. This characteristic is key in the normal operation of critical mission services and applications, e.g., outages and physical security attacks. However, some applications such as AMI can be tolerant to end-to-end delays (latency).

- Reliability: Reliability is the degree of consistency of a measure. In this case, it is a measure of the ICT communication subsystem's ability to relay/ transmit data according to design specification(s). Reliability can also spread to individual devices and components, i.e., a sensor's reliability to only read out correct data from its internal memory.

- Resilience: The ability of a system to operate fail-safe. Typically, since the ICT subsystem can be vulnerable to security threats, such as total denial of service, however, measures must be put in place that zero transmission can never be experienced.

- Frequency Ranges: The power grid was designed for relatively low frequencies, and if PLC is the platform for transmitting data, then the applications should operate at low to moderate frequencies to be accommodated. Similarly, if wireless relaying is opted for over long distances, then higher frequencies would be ideal.

- Data Rate: Data rate is directly mapped to bandwidth capability. The higher the bandwidth of a link, then the higher is the data rates it can support (Shannon's Theorem). Multimedia

or video applications will require higher bit rates for an acceptable GoS at the receiver end. However, AMI will require very small data rates

- Security: Some applications will need to be encrypted so to preserve complete privacy and security. Most critical mission services and applications will require high levels of security end to end.
- Throughput: This measure is also related to the blocking probability of a link. The higher the blocking in a network, the lower the throughput. Many applications are likely to require a minimum threshold throughput level to operate.

### 2.3.4 Example SG Services and Applications

A few services and applications are listed in this subsection.

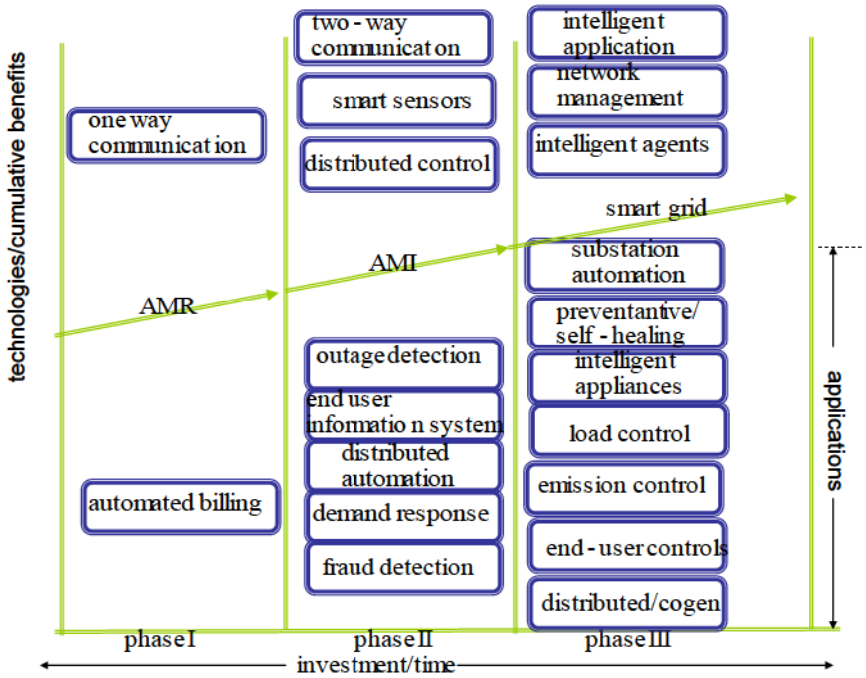


Figure 2-18: SG Applications Roadmap

*A. Substation Automation*

This is the facilitating of the monitoring, controlling as well as physical protection of substations throughout the SG through implementing substation automation systems (SASs). Such a service requires a reliable, scalable, secure, low latency network.

*B. Transmission Line Monitoring*

Transmission Line monitoring is used on live medium and high transmission lines of the high voltage network. This is to monitor any situations of overnight icing, overheating, and lighting strikes,

which endanger humans. Early warning sensors are deployed to monitor and detect these situations. Such a service requires reliable, secure, effective, and real-time communication to respond to emergencies quickly.

*C. Home Energy Management (HEM)*

A home energy management system is an application that allows customers to monitor and control energy usage within a household. The control can be done via low bandwidth links.

D. Advanced Metering Infrastructure (AMI)

AMI establishes a duplex communication network to transmit data between end customers and utilities. SMs are utilized within an AMI to gather meter data or event information.

MDMS, Consumer Awareness Systems (CAS), Interactive Services for Energy Demand Regulation (ISER) Systems to help with the prevention of energy-associated fraud, and precise billing are some of the characteristics and capabilities of the AMI. For the SGs we have looked at, there's a lot of effort on AMI and AMR applications, as well as standards like ANSI C12.19-2008. The diagram depicts a logical depiction of the infrastructure for automated metering. Figure 3-5 depicts SG AMR Application [93], [94].

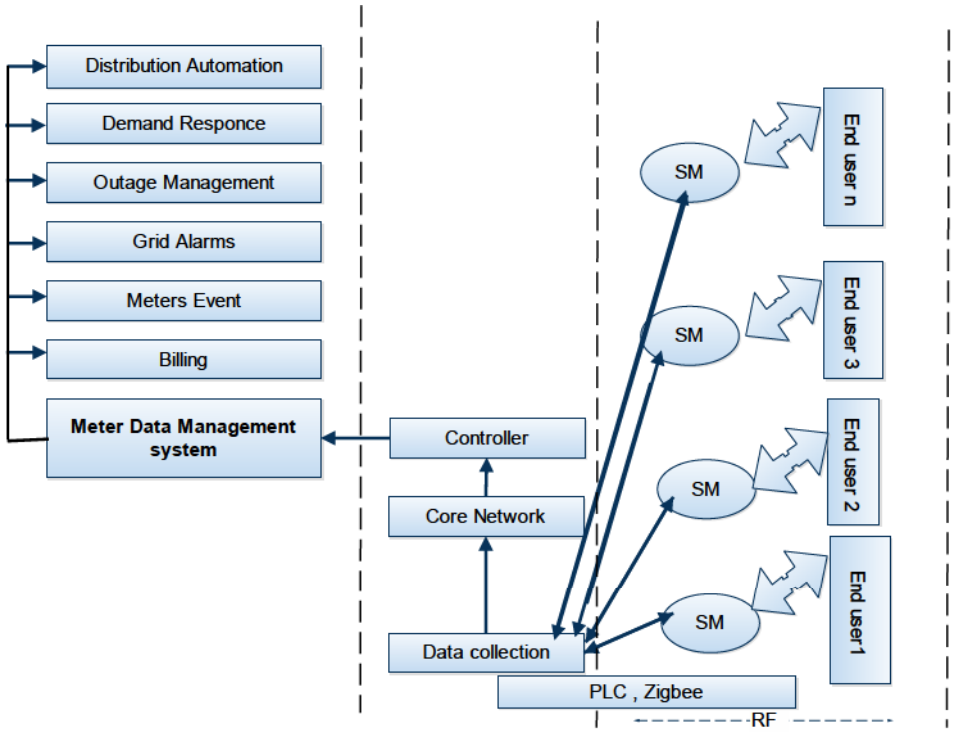


Figure 2-19: SG AMR Application

SMs operate as aggregators, sending data to the data collection unit, which is then sent to the MDMS via a system controller. The MDMS analyzes received raw data to create usable statistics and gives clients with power usage data. The SM which communicates meter readings to the MDMS regularly is the most fundamental element of an AMI scheme.

*E. Wide-Area Situational Awareness (WASA) Systems*

By definition, SG wide-area situational awareness (WASA) systems-based applications and services provide utility operators and designers critical information in real-time for efficient operation and analysis of the SG grid. In a way, it is live monitoring of the performance of the grid. The latency prerequisite for real-time monitoring and control is quite stringent and normally within 20miliseconds to 200-millisecond bounds [95].

*F: Demand Response Management*

In SGs, demand response management (DRM) involves the continuous monitoring of power demand. In that way, enhanced utilization of the available energy is achieved, and at the same time, the SG grid becomes more fail-safe (reliable).

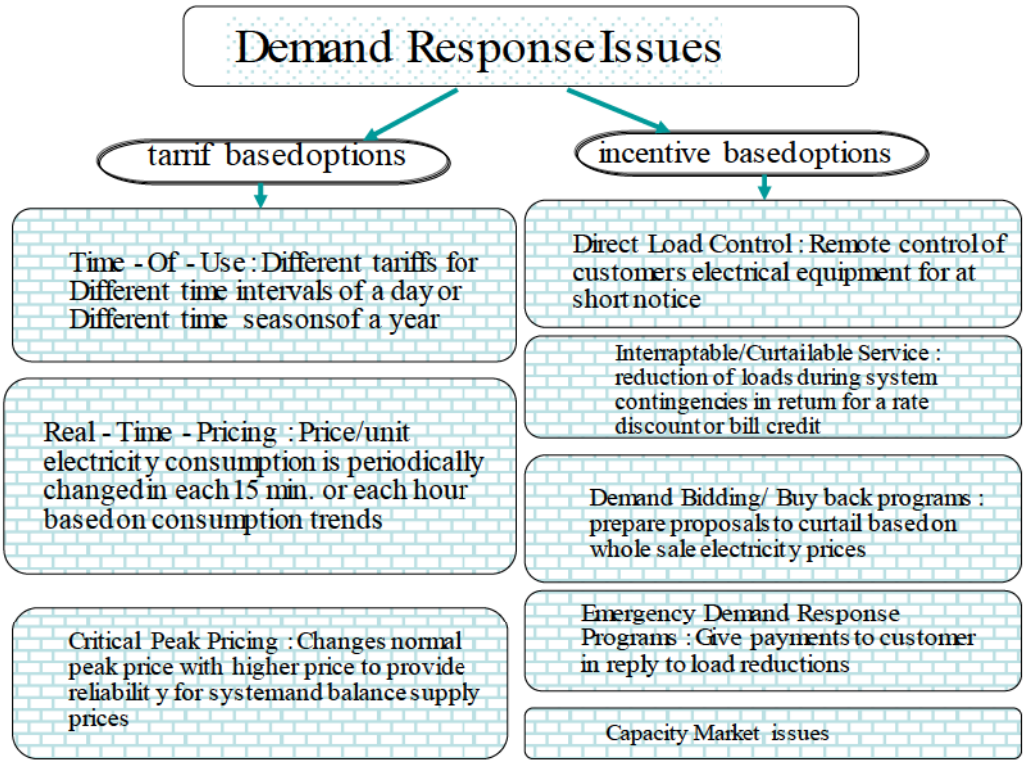


Figure 2-20: Demand Response Options

DRM is a technique for reducing peak power production demand by involving consumers and optimizing or regulating their power usage or demand load. DR can provide users efficient, dependable, and affordable electricity by effectively balancing energy demand and generation, either through automated billing or by employing different load management strategies. End-users participate in the energy industry through DR programs by shifting their energy consumption behavior to adjustable power pricing units instead of a fixed amount, resulting in revenues for both utilities and consumers.

DRs occur in a variety of types, depending on how they're implemented and how long they last. Consumers are given a price signal to help them save energy during peak hours. To distinguish between weekdays and weekends, for example, variable pricing might be utilized. Seasonal pricing may be factored into the Time of Use (ToU) for the DR program's implementation. The customer's overall demand load during Critical Peak Pricing (CPP) hours is computed by comparing it to the basic demand load during the same hours on a typical day. The client may be eligible for a reimbursement based on the amount of demand decrease.

Participants receive credits from Direct load Control (DLC) if they reduce their load during these occasions. If a person fails to shed a burden that is part of a DLC program, penalties may be applied. Load management from afar Remote Load Control (RLC) is a more advanced DR software that uses an advanced algorithm to remotely manage residential appliances to reduce demand load. Price signals and an M2M communication infrastructure are utilized. There is no stringent communication requirement for this service, save only for acceptable latency bounds and moderate bandwidth supports

*G. Outage Management*

Ann outage management system (OMS) in SG would be a service or application relied upon by the utility to assist in detecting as well as restoring power outages. Major functions in an OMS. With regards, to communication requirements, such a service is generally integrated with other services and will generally require low latencies as well as moderate bandwidth. The latency bound should be no worse than 2 seconds, whereas a bandwidth supporting a minimum data rate of 56-kbps would suffice.

*H. Distribution Automation (DA)*

The DA service results from automation which is relied upon in the design and maintenance of the SG's power distribution system, including interactions with the transmission system, As this service is categorized as mission-critical, it is necessary to maintain latencies of no worse than 15 ms coupled with a data rate of between 9.6- and 100-Kbps.

*I. Distribution Management*

This is a service associated with the process of monitoring the movement of assets from suppliers to delivery. Relating this to the SG, the assets would be the cabling, relay switches, and other components that connect the utility substation to the end-users. IEC 62357, IEC 61970 and IEC 61968 standards guide interoperability issues among these various components. In particular, IEC 61850 standard gives guidance on improving the interoperability issues in the SG. Constraints of minimum bandwidth to support 9.6–100-kbps data rates and latencies of 100 ms to 2 s would suffice.

*J. Asset Management (AM)*

By definition, AM implies the managing financial assets of the SG to balance the costs (CAPEX) and capitalize on investment opportunities. Asset Management Systems (AMS) are pivotal to realizing and maintaining a reliable and resilient SG system. E.g periodic monitoring and diagnosis of the power transformers is a key function of such a service. Hence routine tests are carried out on them for the early detection of incipient faults. A 56 Kbps data rate would sufficiently support such a service in a modern SG.

*K. Meter Data Management*

A meter data management (MDM) service is a collection of software-based efforts that performs long-term data storage and management. Such a system enables the storing, management, and further analysis. A data rate of 56 Kbps, and latencies no worse than 2 seconds would support such a service.

*L. Renewable Distributed Energy Resources (DER) and Storage*

This is a service catering to the management of renewable energy units or systems that are normally situated in homes or businesses to provide extra power to the SG. The bandwidth requirement for such a service is about 9.6 to 56 Kbps (bit rate) and latency of no worse than 2 seconds. However, such services are expected to be reliable, i.e. a reliability factor of 99% or better.

*M. Electric Vehicles*

The integration of electric cars and Plug-in Hybrid Electric Vehicles (PHEV) into the SG system is a necessary component. During peak hours, V2G power uses electric-drive cars to supply electricity back to the grid. Vehicle batteries are used to store energy in automobiles [96]. The V2G idea is divided into three distinct variants.

- A hybrid car,
- A battery-powered vehicle,
- A solar powered car.

All the above three require on-board batteries. Figure 2.12 shows the relationships between automobiles and the utility grid. The Vehicle storage is connected to feed back to the grid.

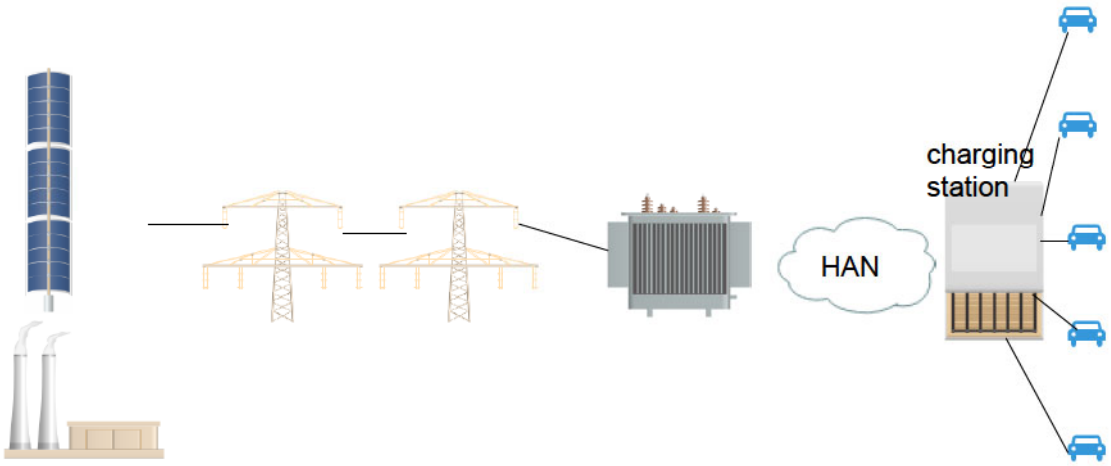


Figure 2-21: Vehicle to Grid

The PHEV significantly decreased local air pollution.

Numerous research has been done to define the purpose and duties of this framework, also known as an aggregator because it looks to be the most promising. Its role might be to act as a go-between for each PEV owner and the system operator, aggregating a particular number of PEVs, coordinating their price, and offering profitable services.

The advantages of V2G are:

- Load levelling at the apex.
- Power backup options

The communication needs for the service is typically are 5–10 kbps data rate and the data latencies of up to 2 seconds.

*N. Electrical Vehicles (EVs) Charging*

This caters to and manages the charging of EVs at designated charging stations. Currently, a specification of three standard charging levels is used to charge electric cars. For management and standardization purposes, various standards are available [97].

## 2.4 Security Issues

In this section, we discuss security issues in SG environments.

### 2.4.1 Overview

Both industrial and social advancements have led to increased demands for power and hence the surging of SGs which as defined earlier are a result of the blending of legacy power grids with modern ICT subsystem technologies. The latter integrates the various generation sources by way of facilitating an interactive infrastructure. This infrastructure established new management capabilities, such as demand response and AMI. The ICT subsystem can be privately owned by the SG (utility operator) or the public. Either way, there is a potential for security vulnerabilities and threats. Unless addressed and prevented, security breaches may lead to dire consequences such as Grid outages, customer billing information leakages as well as the destruction of infrastructures. It is thus an objective of this work (dissertation) to address cyber security issues in SGs. In particular, our focus is on providing an overview of potential cyber security threats, and reviewing current solutions as well as challenges. Key issues to be addressed in this section include:

- Key security objectives and requirements.
- Possible cyber security threats in SGs.
- Mitigating security attack prevention.
- Overview of network protocols and architectures.

### 2.4.2 Key Security Objectives and Requirements in SGs

Addressing both privacy and security is quite a key issue in regards to safeguarding normal operations of key services and applications in an SG. Some of the devices and elements in an SG are resource-constrained in terms of computing capabilities and thus traditional security and privacy

protocols may not be applied directly as they tend to be intensive resource demanding. The overall aim is to ensure identity privacy, as well as security for the data, are not compromised.

Guidelines on SG security typically emphasize availability, integrity as well as confidentiality key to satisfying the objectives.

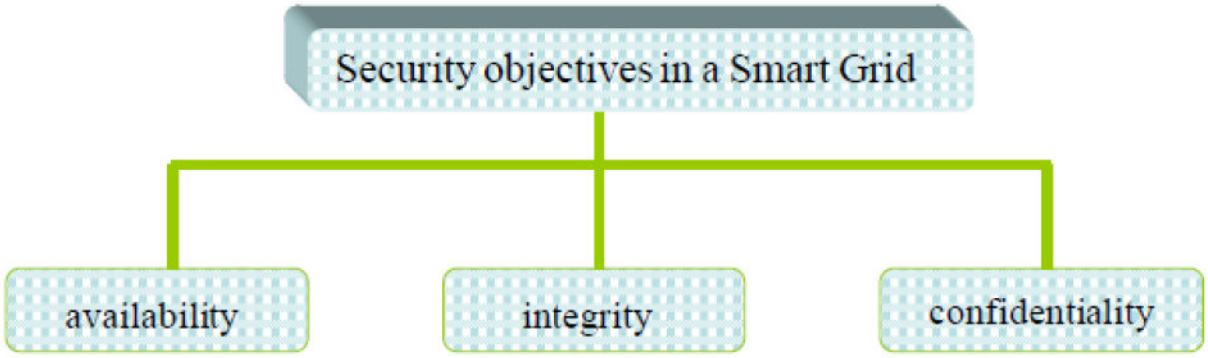


Figure 2-22: Security Objectives for an SG

- Availability in reference to SGs is simply the ability of customers to access resources or data at specified locations and in the correct presentation format. This reliable and timely access to data if violated may lead to disruption in the normal operations of the overall SG.
- Likewise, integrity is safeguarding against unauthorized data altering or deleting. Thus it is necessary to preserve data non-repudiation and authenticity in the SG, otherwise, loss of integrity may result in the inducement of improper decisions concerning overall grid power management.
- Confidentiality deals with putting in place measures that preserve authorized restrictions on data access and disclosure. The aim is to maintain and preserve personal privacy.

Availability, integrity, as well as confidentiality, are thus key security objectives that will ensure the SG's stability as well as reliability. However, it is also important to note that, there are no definite or rather single collection security requirements that address each of the SG interfaces. As such, the requirements and solutions tend to be implementation-specific, driven by the actual applications, configurations, and the constantly changing requirements for the security of all of the functions in the system.

Key cyber security requirements can be listed as follows:

- Attack detection and resilience operations. This necessitates routine profiling, testing, and comparisons of network data as a means of early detecting any anomalies due to attacks. Designing the ICT subsystem such that it has self-healing capabilities would enable resilience to such attacks as the network operations will still proceed normally and thus the SG's availability will not be compromised.

- Identification, authentication, and access control. All devices, elements, and entities in the SG must be pre-screened before being granted access. Each device's identity must be robustly identified. Each SG entity that can receive, generate or process data must be able to perform basic data ciphering and deciphering functions, to perform data encryption and authentication.

- Secure and efficient communication protocols. To ensure privacy as well as security in the grid, message exchanges must be performed within constrained time frames. The time criticality, however, can contradict security (semantic). To ensure the security of the data requires that it be robustly and reliably encrypted. The encryption and decryption processes require time especially if the encryption algorithms are robust enough. That will affect time criticality in delivering the messages between entities. Thus a tradeoff and balances are necessary between the two.

Table 2.7: Comparison of Security Requirements: SG versus IoT

| Security Functions | Smart Grid Communicat ion Network | The Internet (IoT) |
|---|---|---|
| Authentication and access control | Strictly enforced for all communication flows throughout the system | Mostly free end-to-end without access control |
| Attack detection an counter measures | Essential and widely-deployed everywhere | Mainly for critical routers everywhere |
| Every node | Basic cryptographic functions | No specification |
| Security for network protocols | From MAC-layer to application-layer security | From network-layer to application layer security |

Table 2-7 provides a comparative summary of key cyber security requirements for SGs versus those on the internet (IoT).

### 2.4.3 Network Security Threats in the Smart Grid

In this subsection, we explore examples of security threats and vulnerabilities in the SG. Most of these threats do occur during data exchanges. However, there are other threats in other spheres of

the SG's operations as well [97]. The following risks to data exchanges in the SG be broadly classified:

- Denial-of-Service (DoS) – This refers to deliberate or induced temporary network interruptions which affect data transfer to the point of bringing the network to a halt.
- Threat- Due to a lack of adequate ciphering and deciphering of transmitted data, it can easily be intercepted and modified.
- Customer Data Leakage Threats- the confidentiality and identity of end customers can easily be breached or compromised.

The next figure exemplifies the potential susceptibility of every entity in the SG to attacks.

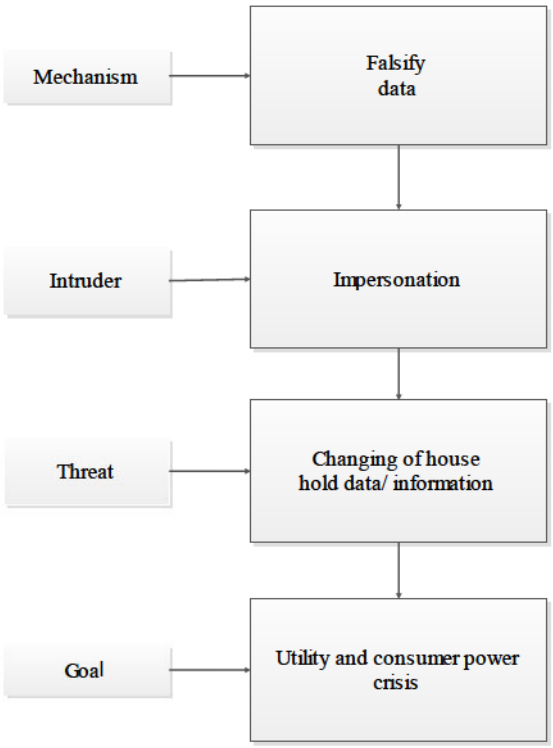


Figure 2-23: Potential Attacks

Typical example actions are as follows:

- By repeatedly transmitting unauthorized data, an intruder may obstruct the targeted recipient, thus causing it to malfunction or shut down completely.

- An attacker can modify the synchronization speeds in the SG, effectively causing elements such as SMs to go out of synchronization. As a result, the collected data becomes incorrectly time-stamped and consequently rejected by intended recipients such as processing servers at billing centers.
- Attackers can intentionally power off targeted devices.
- Attackers can intentionally unleash large volumes of traffic data on specified links or paths thus slowing down overall network throughput. This will result in increased delays and many applications and services may simply time out.

**Denial-of-Service Attacks**

DoS attacks will lead to SG's unavailability. Existing DOS attacks can be inflicted at several communication sub-layers [97].

Table 2.8: Denial of Service Attacks in SGs

| Communication layer | Attacks in SG systems |
|---|---|
| Application layer | |
| Network/ Transport Layers | Traffuc flooding<br>bufffer flooding |
| MAC layer | ARP spoofing |
| Physical layer | Jamming in substations |

At the Physical layer, jamming would be more pronounced. At the multiple access control (MAC) layer (also referred to as the link layer in OSI terms), attackers may modify the physical (Mac) address and hence the data will be delivered to an incorrect physical destination. They can also compromise reliable transfer by disturbing the smooth running of flow and error control mechanisms in this layer. Note that attacks at this layer can cause both availability and integrity issues concerning the normal operations of the SG.

The Network layer ensures global addressing and hence, tempering with addressing at this layer will lead to the data being delivered to a wrong destination altogether. The transport layer rather relies on the services of the network layer to ensure a reliable process to process delivery. If attacks succeed on this layer, then data may be delivered on the wrong ports and applications at the desktop ends.

Attacks at the Applications layer may lead to the overwhelming of the host's already limited computing resources. Normally attackers would simply flood the targeted terminal (entity) with

### Attacks Targeting Integrity and Confidentiality

Attacks targeting Integrity and confidentiality-specific attacks are normally directed and executed at the Applications layer. This is a vulnerable point for unauthorized acquisition, manipulation, or tampering of data.

*Table 2.9:* False Data Injection Attacks in SGs

| TargetedSystems | Impact |
|---|---|
| DC SCADA | Invalid stateestimation |
| AC SCADA | Invalid stateestimation |
| Electric market | Potential financial losses |

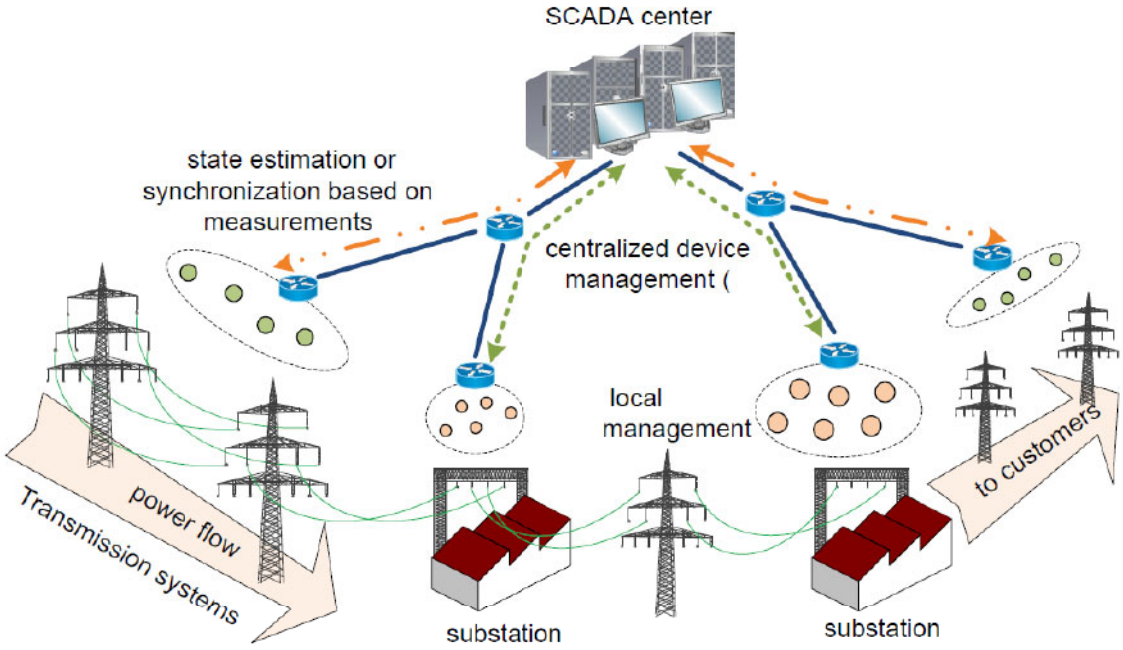


Figure 2-24: Key use Cases in Distribution and Transmission Systems in an SG

*Table 2.10: Key usage Cases with Critical Security Requirements in Distribution/Transmission system*

| No | Network | Information Delivery | Brief Description |
|---|---|---|---|
| 1 | Power substation networks | Single hop, peer to peer | Local monitoring control and protection of power equipment and devices in substations. |
| 2 | SCADA and wide area power systems | Multi-hop hierachical | Cetralised monitoring and control of power equipment at the SCADA center |
| 3 | SCADA and wide area power systems | Multi-hop hierachical | State estimation or synchronization base on measuementsfrom raw datasamples(e.g. from PMUs) |
| 4 | AMI and home area networks | Multi-hop hierachical | Information exchange between customers and the utility and the centers (e.g., meter reading service) |
| 5 | Demand responce home area network | Multi-hop hierachical | Interection between customers and the market (e.g., customers respond to real-time electicity price) |

**AMI Security Threats**

We define security and privacy criteria for the AMR framework based on the AMR functional requirements, threat analysis, and metering details. Below are the requirements:

***Authentication:*** A system should be able to verify that it is communicating with the person it appears to be. To prevent impersonation attacks, this provision should be implemented.

***Authenticity:*** A message's receiver should be confident that it has not been tampered with in route, that it is current, and that it came from the claimed source. This clause should be strictly enforced to prevent tampering.

***Confidentiality:*** Users' metering data should not be shared with unauthorized third parties to prevent eavesdropping attacks.

***Authorization:*** Only approved SG agencies can have access to their users' metering data.

Privacy security for consumers includes the following:

- That no SG agency should have access to individual user metering data.
- That only the user should have access to their metering data.
- *Verifiability:* Utilities should be able to verify that the metering data they receive from their customers is accurate.

- *Availability:* AMR protocols should be designed to be resistant to DoS attacks.

### 2.4.4 Tampering with Metering Data

Tampering can take place in several ways such as altering, blocking, deleting, and replaying genuine metering information or injecting unauthorized information into the network. Since data is used for a variety of reasons, including handling energy and planning potential network expansions, interfering with valid metering data may cause monetary losses. To disrupt the grid's regular activity, attackers could tamper with the metering data obtained. Because data is used for grid matching and forecasting potential energy demands, the altered data may distort power demand forecasts, leading to a rise in grid imbalance. A spike in disparity would not only raise operating costs but could also result in a blackout. Internal agencies may also tamper with legal metering data to increase revenue or cut costs. Utilities can try to rig metering data to maximize their prices. To lower their bills, some unethical consumers can try to tamper with their metering results [98].

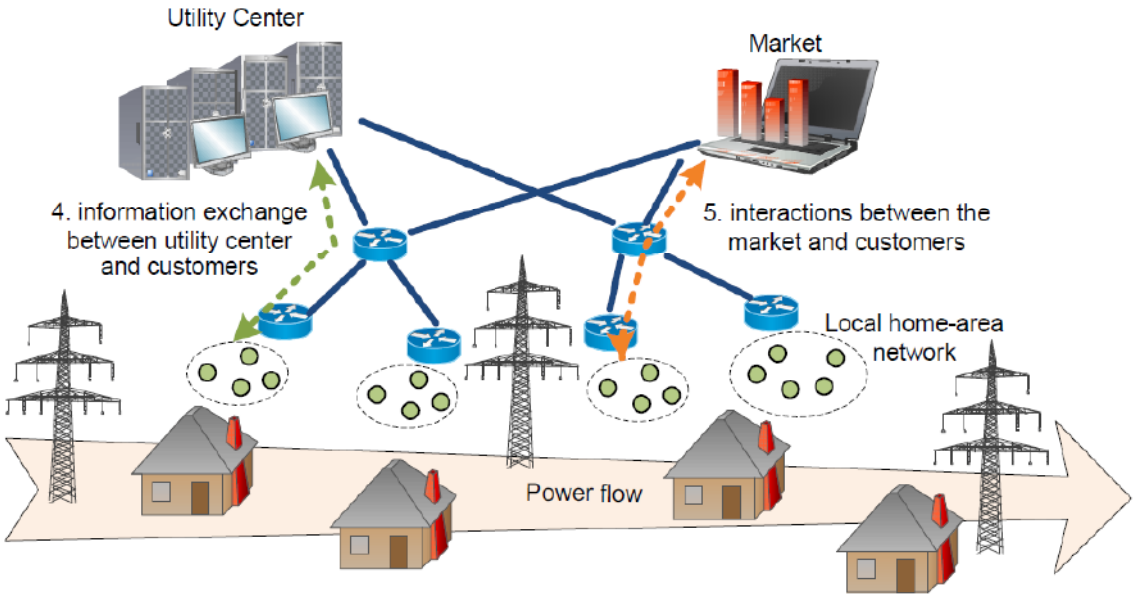


Figure 2-25: Key use Cases in the AMI and HANs

*Table 2.11:* Comparison Between the Distribution/Transmission System and the AMI Networks

| System | Communication Methods | Timing Requirements | Security Objectives |
|---|---|---|---|
| Power distribution and transmission | Single-/multi-hop communications, peer-to-peer | Milliseconds to seconds | Critical availability and integrity |
| Advanced metering infrastructure | Multi-hop, hierarchical networking | Minutes to hours | Critical intergrity and confidetiality |

## 2.5 Attack Detection for Power Networks

Because the SG incorporates an information network (ICT subsystem), it must be able to identify, detect and shut out potential security threats DoS attacks that may be launched anywhere in communication networks [99]. The attacks can be categorized as illustrated in Figure 2.26.

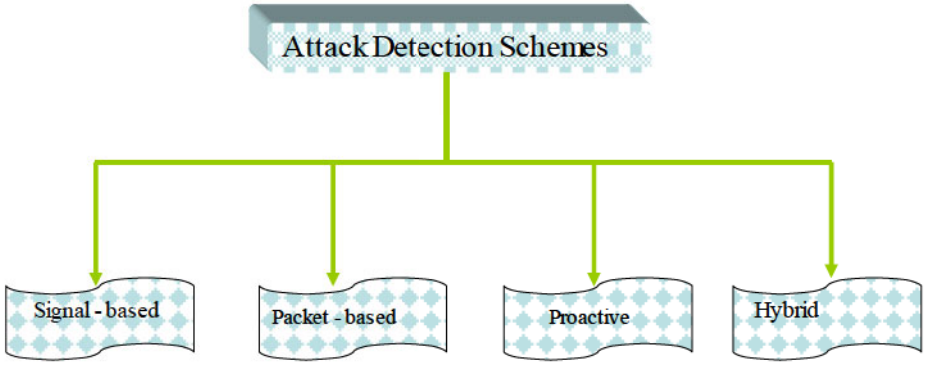


Figure 2-26: Classification of DoS Attack Detection Schemes

Signal-based detection approaches rely on measuring a received signal's strength to detect the levels of stray (jamming) signals. When measured above a certain threshold, then it is concluded that the channel (link) is under Dos attack(s)

Packet-based detection. This relies on packet blocking probability levels as signaling potential DoS attacks. E.g., a sudden increase in packet blocking signals ongoing DoS attacks. In this case network performance degrades significantly.

Proactive method. In this case, probing packets are sent in the network, or suspected section, to measure the status of potential attackers.

Hybrid method. This combines two or more of the measures already defined to try and improve attack detection accuracies.

Table 2.12: Potential Uses and Applications of Existing Attack Detection Methods for the Smart Grid

| Scheme | Potential Use | Existing Application |
|---|---|---|
| Packet based | Wide applications | Substations |
| Signal based | Wireless applications | --- |
| Proactive | Limited | --- |

## 2.6. The IoT and Security Features.

In this section, we overview IoT's security features. This is because as earlier cited SGs may elect to rely on public ICT infrastructures such as the IoT as their pillar ICT subsystem [100].

A consensus is slowly being reached towards an IoT-enabled works standardized architecture. The consensus among the various alliances and study groups seems to advocate for the following layers:

- *Physical (perception) layer:* The layer comprising the various objects and devices. Mostly the devices are involved in data acquisitions.

- *Network layer:* This is the key layer to facilitating communication between peers within the IoT.
- *Transport layer:* The layer ensures safe data delivery between sender and destination.
- *Application layer:* This is the end-user interface for accessing various applications and services.
- *Processing layer*. Process data derived from the transport layer.
- *Enterprise /Business layer:* For the regulation of the entire IoT operations and this may include business, profit, and security models.

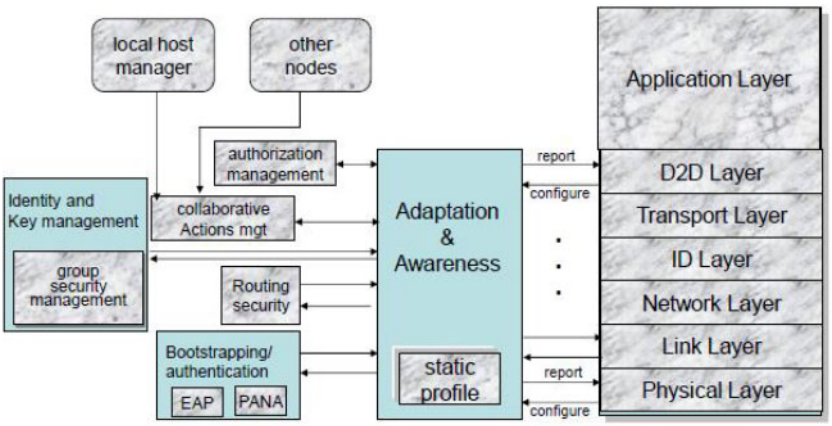


Figure 2-27: Generalized Secured Communications Architecture

Shown in Figure 2.27 is an example of security architecture. On the right is the architectural layers, whilst the security layers are on the left side. As can be noted a D2D communication service layer is added after the user (applications) layer. Its role is to enable linkages between dissimilar network devices thus solving interoperability issues experienced with current M2M and equivalent technologies [101].

- **Transport Layer's** functions are QoS, dependent, but retain the fundamental role of ensuring the process-to-process delivery of data.

- **The Identification (ID)** layer's main function is to identify the required resources. It can facilitate privacy and authentication by way of utilizing the node ID. The Host Identity Protocol (HIP) can be relied upon by this layer
- **The Network (NET)** layer is the equivalent of the IP layer and takes care of logical addressing. And general end-to-end packet routing.
- **The MAC** layer regulates the utilization of channel resources. It will allocate access such that channel contentions are minimized [14].
- **Physical Layer (PHY) regulates** electrical specifications of the data associated symbols. This includes appropriate line encoding for the various media

### 2.6.1 Privacy

To preserve privacy on the original data or to hide the sensitive parts, data perturbation techniques are used [101]. During transmission and receiving of data, noise is always an issue, to minimize these issues, anonymous techniques are used. There are noise addition techniques that are used to add noise to the original information for the message to not be readable to hackers. Data sampling, noise random, data swapping and differential privacy are the four groups of this technique implemented to add noise to the message to be make it unreadable. To hide the data owner's identity by removing any unambiguous identifier making data unclear is the other technique used called anonymous protection. K-anonymity, I diversity, and T-closeness are the methods for privacy-preserving. The data restriction technique encrypts the inputs and blocks access to limit data usage. This method controls access to data and uses cryptography-based techniques.

The technique that is effective in ensuring data sharing is called access control. The data owners have the privilege to choose who can get access to see their data and how others manipulate their shared data. Cryptographic protection techniques are used mostly when preserving the privacy of the shared data, the secure multiparty computation, a cryptographic method that uses keys to encrypt and decrypt data are asymmetric/symmetric encryption, public key infrastructure.

## 2.7 Summary Chapter

Security and privacy in an SG is of importance, and as such, this chapter devotes to reviewing requirements in this regard, the chapter devotes itself to reviewing SG infrastructures in regard to

key issues such as AMI and its incorporation with the general power supply and distribution systems; key requirements of cyber security for SG communications, and appropriate regulations and standards for both general power generation and supply infrastructure and security of the Smart Grid. It is generally concluded that:

- It is key that SG general and cyber security infrastructural standards ought to be properly defined.
- This set of standards will assist in easily enabling cost-effective SG services and applications related to energy (power) distribution, fault diagnostics and rectifications, energy management and smart charging and recharging of EVs.

The overall key finding in this chapter includes the need to adequately address both security and privacy issues. Hence in the next two chapters, these two important aspects of next-generation SG developments, namely privacy and security are addressed.

# 3. Privacy Preservation in Smart Grids

## 3.1 Introduction

The incorporation of ICT technologies enables two-way communication, i.e., end-users can interact with the utility operator and vice-versa. In that way, both parties interact and consequently, this leads to improved operations and management of the SG.

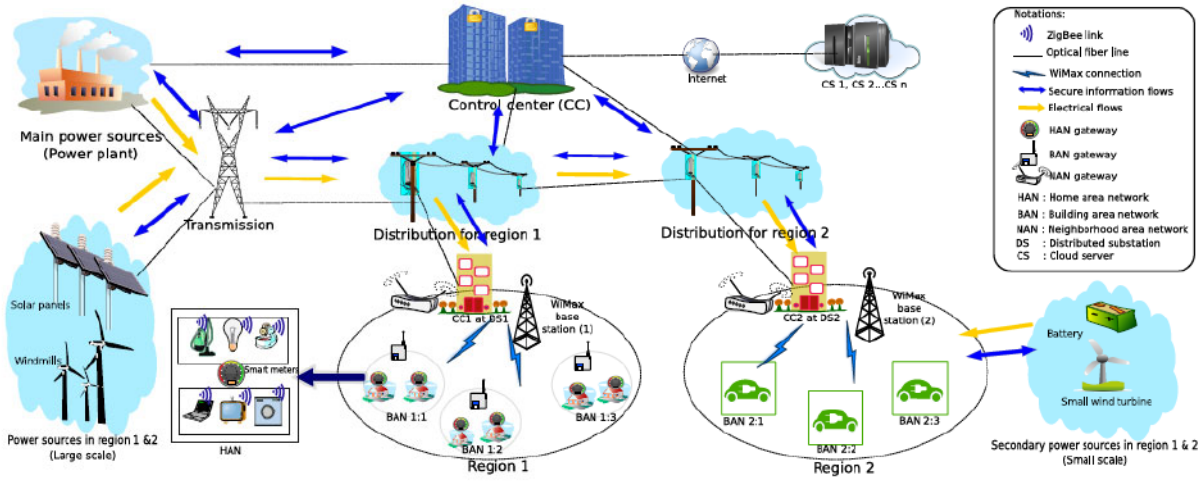


Figure 3-1: Smart Grid

This is because there is more effective real-time monitoring as well as control of electricity generation, distribution, and consumption in the system. The overall focused objectives are:

- To integrate renewable generation by individual households and private entities into the main power grid.
- Real-time power consumption monitoring, effective billing, and measurements.
- Achieving optimal balancing of demand and power energy consumption by end-users (customers).
- Effective interaction between utility versus end customers (facilitated by the ICT subsystem).
- Guarding and enforcing measures against malicious attacks and other security threats.
- Degree of autonomy in management to enhance reliability.
- Maximize efficiency in terms of assets used in the SG.

The duplex communication facilitation means that the utility can use SMs to remotely acquire users' energy consumption data. This however violates end users' privacy in terms of habits. Several

studies have been carried out in mitigating such issues. Hence in this chapter, we focus on SG privacy, as well as privacy preservation frameworks. We thus will first need privacy in the SG, then followed by the schemes themselves.

## 3.2 Privacy and Smart Grids

There are various kinds and forms of Privacy attacks in the SG. These include key-, data, impersonation, and physical-based attacks. Thus, in this subsection we define each of them.

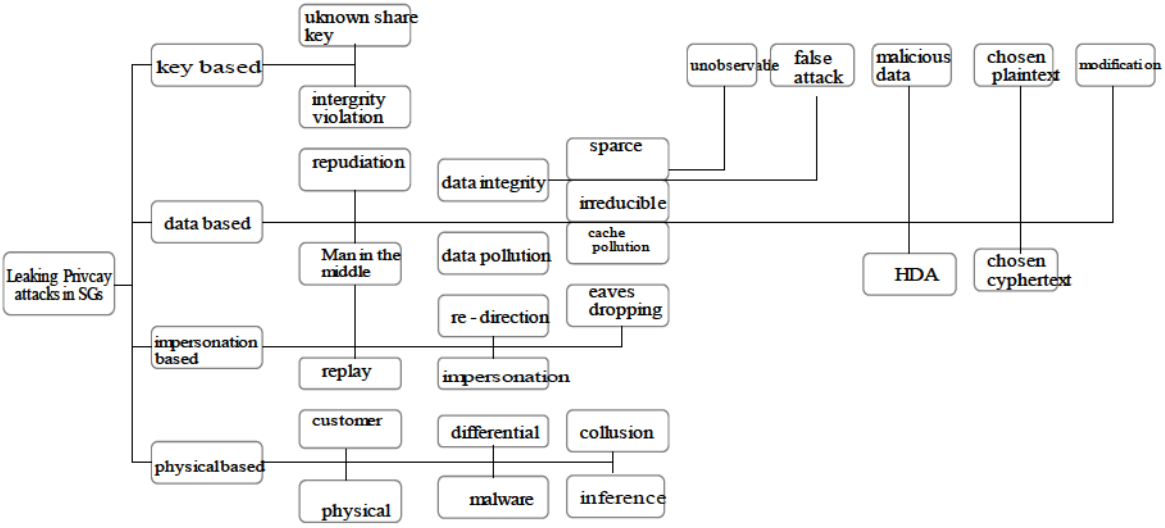


Figure 3-2: Classification of Attacks

### 3.2.1 Key-based attacks

To preserve privacy, key-based privacy schemes are generally relied upon. Before the commencement of a session between two entities within the SG, two parties will agree on a secret key. This is normally accomplished at the "registration phase" in which a secret key or certificate is agreed upon. The key/certificate will be used throughout for mutual authentications. However, during authentication phases, adversaries can easily trick either party into disclosing the key/certificate. From then onwards the adversaries would have successfully infiltrated the SG space.

### 3.2.2 Data-based attacks

Such attacks are directed to power consumption-related data by individual households Adversaries, in this case, capitalize on the fact that data consumption trends e.g., may peak at specific times of the day, on certain days of the week, or particular seasons of the year. They can therefore direct attacks on the power consumption data at those times to try and modify the exact data semantics and in the process, the data integrity will be violated as well.

### 3.2.3 Impersonation Related Attacks

This broadly refers to the actions of adversaries directed to the SG in a bid to intercept or rather capture SM data whilst being relayed to billing centers. A typical example of such attacks is the man-in-the-middle attack which is illustrated in Figure 3.3.

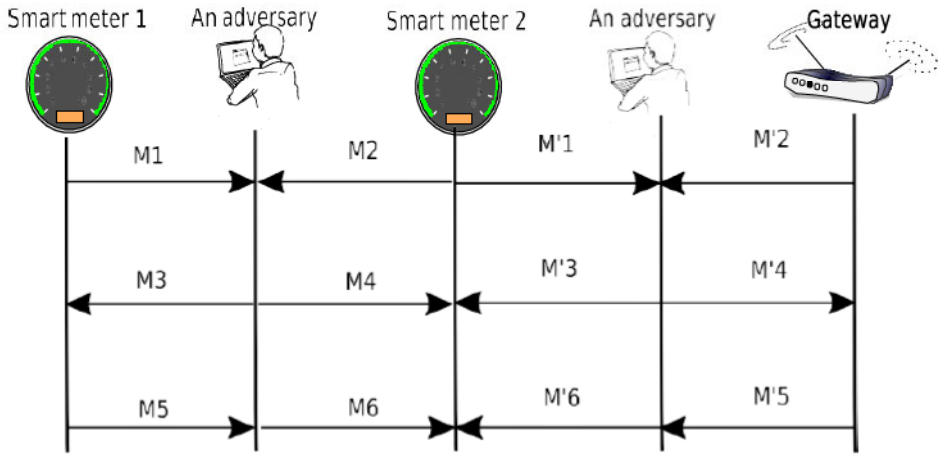


Figure 3-3: MITM Attack Illustration

Before sending data SMs must authenticate with the associate gateway or with those who will relay the data on their behalf. They exchange initially exchange public keys as part of initializing a session. In this case, the public keys are ($M1$, $M2$, $M'1$ and $M'2$). The adversary manages to intercept the public keys and redirects them to $M3$, $M4$, $M'3$ and $M''4$. It is now possible that SM1 and Gateway will both use the adversary's public key instead to encrypt data before relaying it to other parties such as SM2a (The action is represented by messages M5 and M'5). The attackers will eventually intercept the encrypted messages and decipher them using the now known private key.

### 3.2.4 Physical Based Attacks

They are directed towards physical hardware. This can be in the form of targeting an end user's SM unit, a data concentrator (aggregator) etc. In all cases, the attackers may either completely deactivate the unit (system) or tap stored data which they can later decipher and use for launching further attacks.

### 3.2.5 Impersonation Related Attacks

Overall, to counter all these threats the following security requirements are necessary:

Initial Authentication: Before any two entities in the SG can enter into a data exchange session, they must first perform identification and subsequently authenticate. Usually, the identification is by way of using encrypted pseudonyms. The authentication phase then follows in which the parties furnish proof of identity.

Integrity: The messages received by either party must be checked for integrity.

Non-repudiation: Measures should be taken in the SG to ensure that any device indulging in a particular action, should not repudiate it.

Access control: IT would be necessary to enforce some form of access restrictions in which access to any resource is privileged and that prior security checks must be performed. Privacy: In this case knowledge of details about the originator of data (such as real identity and location) must be restricted only to authorized parties.

### 3.2.6 Solution Approaches

One possible solution to solving privacy threats in the SG is to implement privacy preservation measures that mostly involve cryptographic methods. Various studies have explored such methods and in general tend to categorize them as public-key primitives, symmetric-key primitives, and unkeyed primitives.

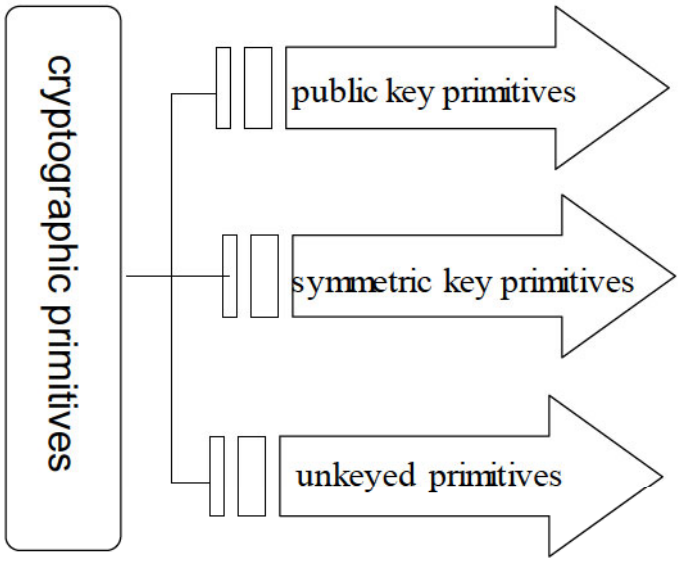


Figure 3-4: Taxonomy of Cryptographic Primitives

Under the category of Public-key primitives, we have asymmetric cryptography, which is a cryptographic system that employs public keys (known to all entities) and private keys (known to owners only). Specialized one-way function cryptographic algorithms are relied upon in generating

both keys. Privacy of the private key must be maintained, whilst the public key is distributed via secure channels.

The first kind of primitives is the symmetric key primitives, which are also called private key primitives. And here the same key is going to be used by both the sender as well as the receiver. That is why the name symmetric key primitives or private key cryptography. Symmetric because it is symmetric in nature.

Unkeyed primitives rely on hash functions and random sequences

We thus in the next subsection review privacy preservation cryptographic approaches

## 3.3 Privacy Preservation/ Cryptographic Approaches

Data aggregation, anonymization, and perturbation are techniques widely implemented to preserve privacy in SGs. To adhere to total privacy preservation as well as satisfying security requirements, the techniques are further augmented with multiparty computation (MPC) or homomorphic ciphering/ deciphering.

Note that the ciphering part (MPC) is based on allowing individual entities (parties) to collaboratively generate using the individually owned data, but not sharing its content with the rest of the entities (parties) involved. Thus, the advantage of homomorphic encryption-based techniques is that it permits cryptographic mathematical operations on ciphered text. Nevertheless, this feature does allow entities to perform the computations but without knowledge of the data contents.

With anonymization, pseudonyms are instead used rather than the true entity's name. In that way it becomes difficult to map an individual's real name to the energy consumption-related data. In addition to hybrid approaches, two or more primary techniques are blended thus resulting in an even more robust technique concerning privacy preservation. In this category, we have time perturbation techniques and others. Lots of research has already been done regarding privacy-preserving schemes in SG environments and we thus henceforth review them in detail.

### 3.3.1 Aggregation Based Schemes

With regards to aggregation-based privacy preservation schemes, the authors in [112] lightweight privacy-preserving data aggregation (LPDA) that utilizes the bilinear pairing technique as well as a one-time masking method to conceal an entity's identity, whilst at the same time maintaining a lightweight aggregation. Generally, the parties are involved: several HANs within the same BAN, BAN-Gateway and the CC. Its three-phase operations are as follows:

1. At the starting phase, the CC computes the mandatory bilinear together with two hash functions. It retains one key designated as the master, private, and the other is made public. Both HANs and BAN–gateway register with the CC and in the process are granted private keys, which will be used for establishing static keys for communication purposes between them.

2. The aggregation request phase is next. The authenticated HANs receive time-stamped aggregation request messages (regarding energy consumption) from the BAN Gateway.

3. During the aggregation response phase, individual HANs in the vicinity responds by collating the energy consumption message, before sending it to the BAN gateway. Note that it masks the message using its assigned static key as well as a once-off mask. Upon receiving this message, the BAN performs the necessary verifications and authentications before relaying the same message securely to the CC. The CC will also in turn verify and authenticate the received message. The scheme overall was proved effective in preventing security vulnerabilities. However, its drawback is that of key management complexities as well as high computational loads. Especially now that hop-to-hop communication is involved.

In [113] a homomorphic encryption-based privacy scheme is proposed. In this case, a spanning tree is formed to acquire customer consumption data. The collector, in this case, is designated as the root and all messages exchanged between nodes are encrypted. Implementation details are as follows: In the first instance, an aggregation route connecting all SMs in the targeted area is constructed. Energy consumption data is aggregated upwardly on the tree. An individual parent SM requests and acquires data messages from its child SMs and merges them with its own. This proposed approach was proved to ensure complete confidentiality since intermediary SMs cannot read the message's content. However, forgery of data is possible as there is no proper auditing of messages.

Similarly, in [114] privacy-preserving aggregation (EPPA) scheme is proposed. It uses primitives such as homomorphic Paillier cryptosystems, bilinear pairing, and a dynamic increasing sequence. The scheme involves three entities: SMs, residential area gateway (GW), and the utility operator.

Reference [115] proposes an efficient privacy-preserving demand response (EPPDR) Scheme. It uses similar cryptographic approaches as schemes already reviewed. In particular, its initialization phase is similar to that of the EPPA scheme. Both the utility operator and GW make use of identity-based signatures in generating private and session keys, which will then be shared non-interactively between the entitles involved.

However, this scheme generates new session keys after each time-out period, within the same session.

Relatively similar schemes are discussed in [116], [117], [118], [119], [120], [121], [122]. Other categories of aggregation schemes include:

- Multiparty Computation Based Schemes [123], [124].
- Anonymity Based Schemes [125], [126], [127], [128], [129].
- Hybrid Based Schemes [130], [131].
- Identity and Attributes Based Schemes [132], [133], [134], [135], [136], [137], [138], and [139], [140].
- Ciphertext-Policy ABE (CP ABE) [141,[142], [143], [144], [145], [146], [147].

## 3.4 Lightweight P rivacy Preserving Scheme for SG HANs

### 3.4. 1 Introduction

Based on the literature survey, we carried out in the preceding sections, in this section we propose and analyse lightweight-based data aggregation that ensures privacy as well as confidentiality. It is centered on forecasting power consumption demands for a particular neighborhood, and overall, because most attacks occur, during the transmission of data across the ICT subsystem, it thus seeks to limit that. It does so by first forecasting its demands, and only links with the utility operator (CC) when adjustments have become necessary. It is a desirable goal that the scheme satisfies all desirable privacy objectives, is robust, as well as being lightweight. Furthermore, we also aim at the objective of minimizing both communication and computational overheads.

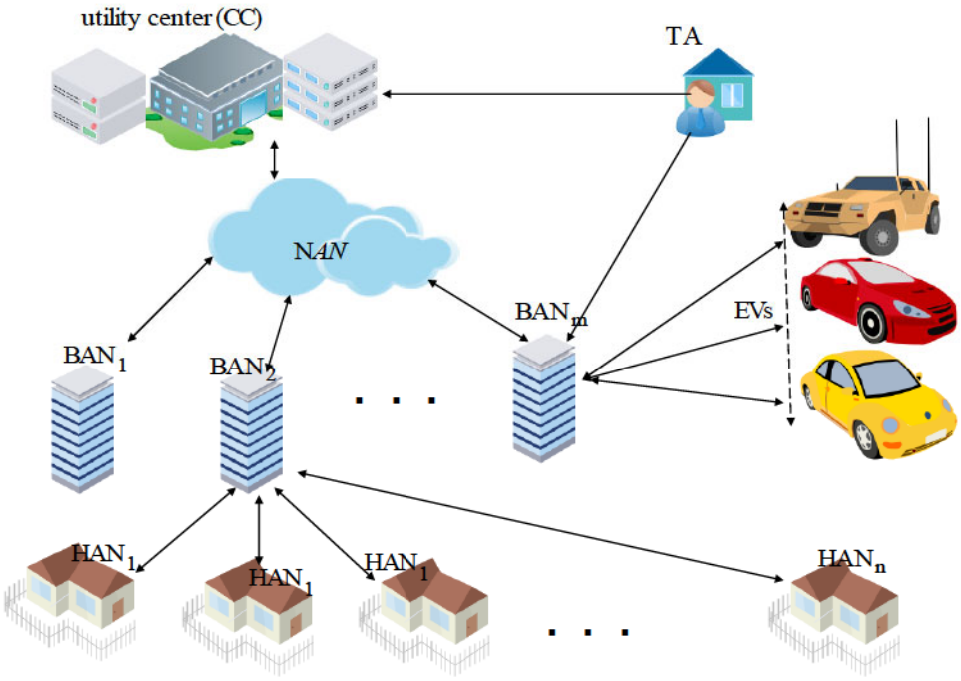


Figure 3-5: Scheme's Model Illustration

As illustrated by Figure 3.5, the scheme *BANs* connect to *CC* via the available *NAN* targets a particular residential area, within an SG and has several $BANs = \{BAN_1, BAN_2, \ldots BAN_m\}$. In other words, *BANs* do not connect directly to the *CC*, but via an available *NAN* network coverage (which is facilitated by the ICT subsystem of the SG. The *NAN* merely relays messages to *BANs* and *CCs*. All *BANs* are assumed to be non-computational resources constrained. It also interconnects several *HANs*,

$$HANs = \{HAN_1, HAN_2, \ldots HAN_n\}. \tag{3.1}$$

Note that a typical *HAN* represents a standalone household and hence will comprise several household electrical appliances.

A trusted authority ($_{TA}$) assigns *IDs* to each *SM*.

### 3.4.2 Model Requirements and Design Objectives

It is assumed that both *CCs* and *BANs* cannot temper maliciously with any data received from *HANs*. Note, however, that attackers may try to intercept the data as it is exchanged between the trusted parties.

Thus to safeguard from situations in which attackers (adversaries) may extend their actions:

- End user‘s privacy: the end customers’ personal information cannot be indulged to unauthorized users. Neither can their energy consumption data or trends be divulged to unauthorized parties. To further consolidate the end user’s privacy, the scheme will not divulge the actual IDs to the CC. In other words, this knowledge of these details will only be confined to $BANs$.
- Messages Integrity and Confidentiality: The end customer’s power usage details, trends, and associated billing must be protected from any attackers. Total integrity must be ensured. In short, any attempts or acts of malicious actions must be detected in real-time.
- Availability: All key entities such as the $BAN$ servers must be available and accessible throughout. This implies that the system should be completely shielded from DoS attacks.

**Design Goals**

The proposed scheme has the following desirable objectives:

- Minimization of computational loads.
- The communications overheads must be kept at a minimum or be avoided altogether
- The scheme aims to preserve the consumers' privacy.

We will rely on the NTRU, which is an open-source public-key ciphering and deciphering system that utilizes lattice-based cryptography to encrypt and decrypt session data [148]. NTRU comprises two algorithms namely: NTRUEncrypt and NTRUSign [148], [149]

NTRUEncrypt, primarily encrypts. Its public-key cryptosystem, or encryption algorithm, is a lattice-based i.e., on the shortest vector problem in a lattice. It is quite dependent on the presumed difficulty of factoring certain polynomials in a truncated polynomial ring into a quotient of two polynomials having very small coefficients

The NTRU cryptosystem can be summarized as follows:

If $n$ is a power of $2$; and $\Phi$ has $n$ liner factors $\Phi = m+1$, $R = Z[x]/\Phi$, $q(q = 1 \bmod 2n)$:

$$\Phi = \Pi_{i<n}\Phi_i = \Pi_{i<n}(x-\Phi_i) \bmod q \tag{3.2}$$

$$R_q = \frac{R}{qR} = Z[r]_q/\Phi \tag{3.3}$$

where $R_q^x \in R_q$ .

In the above two equations, $q$ is a prime number.

**Key Generation**

The key generation procedure would be as follows:

For $_n, q \in Z, p \in R_q^x$ , $\sigma \in R$ .; if we sample the value $f'$ from a discrete Gaussian function $D_{Z^n,\sigma}$, where $\sigma > Poly(n) * q^{0.5+\varepsilon}$, for any value of $\varepsilon > 0$, we have:

$$(sk, pk) \cup R \times R_q^x \tag{3.4}$$

A secret key can be generated as follows:

$$f = p * f' + 1 \tag{3.5}$$

In the above equation $(f \mod q) \in R_q^x$, and $f = 1 \mod p$. The secret value will range from $g$ to $D_{Z^n,\sigma}$, subject to $(g \mod q) \in R_q^x$.

We can finally recover the secret key $sk = f$ and public key $pk = h$

where;

$$h = pg / f \in R_q^x \tag{3.6}$$

**Encryption**

Given a message $M$, a sender $S$ generates;

$$\text{rand}.s, \varepsilon \leftarrow \overline{Y_\varepsilon} \tag{3.7}$$

and ciphertext as:

$$C = hs + p\varepsilon + M \in R_q \tag{3.8}$$

**Decryption**

Upon receiving $C$ the receiver $R$ will decode the message using the private key $f$ as follows:

$$C' = f.C \in R_q \tag{3.9}$$

$$M = C' \mod p \tag{3.10}$$

The NTRUSign , also referred to as NTRU Signature Algorithm, is public-key cryptography digital signature based and utilizes the GGH signature scheme. It operation is mainly centered on mapping a message to a random point in a $2N$-dimensional space, where $N$ is defined as one of the NTRU-Sign parameters, and solving the closest vector problem in a lattice closely related to the NTRUEncrypt lattice.

Given $N$ , $q$ , $d$ , and $NB$ being a prime dimension, a modulus, a key size and verification bound perimeter respectively.

Also given the existence of two polynomials $f, g$ which are both invertible modulo $q$ , such that their coefficients $d+1$ equal $1, d$ , $-1$ and the remaining $0$ , we then have;

$$h = f^{-1} * g(\text{mod q}) \tag{3.11}$$

They compute polynomials ( $F, G$) such that;

$$f * G - g * F = q \tag{3.12}$$

**Key Generation**

For an arbitrary user $i$ we select a random polynomial $r_i \in R_q$ such that;

$$f_i = f * r_i,\ g_i = g * r_i \tag{3.13}$$

$$F_i = F * r_i^{-1} \tag{3.14}$$

$$G_i = G * r_i^{-1} \tag{3.15}$$

Ultimately the output is;

$$Sk_i = (f_i, g_i, F_i G_i) \tag{3.16}$$

Signing In Process

Upon $S$ hashing a message $M$ , such to create a random vector $(m_1, m_2)$ (mod q) , and substituting (writing) $m_1$ , $m_2$ in the following:

$$G_i * m_1 - F_i \circ m_2 = A_i + q * B_i \tag{3.17}$$

$$-g_i \cdot m_1 + f_i * m_2 = a_i + q * b_i \tag{3.18}$$

The signature on the message $M$ is;

$$s_i = f_i * B_i + F_i b_i (\text{mod } q) \tag{3.19}$$

**Signature Verification**

The verifying entity $V$ also hashes the received message $M$ to create $(m_1, m_2)$ then calculates:

$$t_i = s_i * h(\text{mod } q) \tag{3.20}$$

Subject to the following:

$$\|s_i = m_1\|^2 + \|t_i - m_2\|^2 \le NB \tag{3.21}$$

### 3.4.3 Proposed Scheme

This is a two-phase scheme, the first of which accomplishes initialization (i.e ensuring connectivity among the different entities involved in the energy supply). The second phase addresses message exchanges within a $BAN$ 's domain

**Phase I**

The key steps are summarized as follows:

*A) Key generation*

The designated $_{TA}$ will encryption and signing in keys for both $CC$ and $BAN$ as follows:

For the $CC$ 's secret key $f_{cc}$ we have;

$$f_{cc} = p * f'_{cc} + 1 \quad , f_{cc} \bmod q \in R_q^x \tag{3.22}$$

$$f_{cc} = 1 \bmod p \tag{3.23}$$

The $_{TA}$ also samples $g_{cc}$ from the function $D_{Z^n,\sigma}$ such to satisfy;

$$g_{cc} \bmod q \in R_q^x \tag{3.24}$$

After which it calculates:

$$h_{cc} p g_{cc} / f_{cc} \in R_q^x \tag{3.25}$$

Thus $h_{cc}$ is the $CC$ á public key whereas $f_{cc}$ is the private key.

Similarly, for the $BAN$ gateway its keys are computed as follows:

$$f_{bam} = p * f'_{ban} + 1 \tag{3.26}$$

Once again $f_{cc} \bmod q \in R_q^x$ and $f_{ban} = 1 \bmod p$

The $_{TA}$ also samples $g_{ban}$ from the function $D_{Z^n,\sigma}$ such to satisfy;

$$g_{ban} \bmod q \in R_q^x \tag{3.27}$$

After which it calculates:

$$h_{ban} pg_{ban} / f_{ban} \in R_q^x \tag{3.28}$$

Thus $h_{ban}$ is the $CC$ á public key whereas $f_{ban}$ is the private key.

**Signing keys**

Once again, the $_{TA}$ a pair of polynomials $f, g$ invertible module $q$. Both satisfy $d+1$ of their roots equal $1$, $d$ roots equal $_{-1}$ and the remainder equal $0$. The public key for all end users is calculated according to:

$$h = f^{-1} * g (\text{mod}\, q) \tag{3.29}$$

It then computes $(F, G)$, in which;

$$f * G - g * F = q \tag{3.30}$$

In order to generate the signing key for $CC$, it selects $r_{cc} \in R_q$ and setting;

$$f_{ccs} = f * r_{cc}, \quad g_{ccs} = g * r_{cc} \tag{3.31}$$

It then further computes;

$$F_{cc} = F * r_{cc}^{-1}, \; G_{cc} = G * r_{cc}^{-1} \tag{3.32}$$

Thus the $CC$ 's signing keys will be;

$$Sk_{cc} = (f_{cc}, g_{ccs}, F_{cc}, G_{cc}) \tag{3.33}$$

Correspondingly, the signing key for the $BAN$ gateway is computed by first selecting $r_{ban} \in R_q$ :

This is followed by;

$$f_{bans} = f * r_{ban}, \quad g_{bans} = g * r_{ban} \tag{3.34}$$

and then,

$$F_{ban} = F * r_{ban}^{-1}, \; G_{ban} = G * r_{ban}^{-1} \tag{3.35}$$

Thus the $BAN$ 's signing keys will be;

$$Sk_{ban} = (f_{ban}, g_{bans}, F_{ban}, G_{ban}) \quad (3.36)$$

**Generation of IDs**

Each $SM$ is assigned an d $ID$, $ID_1, ID_2, \ldots ID_n$. At regular intervals corresponding pseudo IDs are generated according to;

$$ID_{new} = h(ID_{old}) \quad (3.37)$$

where $h$ is a hash function.

**Electricity Demand Forecast**

This is gone according to a forecasting function $g(\ )$ and for each $HAN$, the forecasted demand is;

$$x_i = g(HAN_i) \quad (3.38)$$

Thus for each cluster, the $BAN$ aggregates the forecasted demands as follows

$$x = \sum(x_1, x_2, \ldots, x_n) + \varepsilon \quad (3.40)$$

Where $\varepsilon$ denotes a backup. Note that the backup is mainly derived from $EVs$;

$$C_{EV} = \sum C_i \ , 1 \le i \le N_{EV-\text{expected}} \quad (3.41)$$

Thus we have;

$$\varepsilon = r * C_{EV} \quad (3.42)$$

subject to $0 < r < 1$ a scaling factor

Note that at initialization phase, an optimal number of $EVs$ required to work as energy buffers is determined by the $BAN$ according to:

$$\min \ N_{EV}(m) \quad (3.43)$$

Subject to:

$$\varepsilon(m) \le \sum_i C_i(m), \ i \in \{1, \ldots, N_{current}(m)\} \quad (3.44)$$

$$N_{EV}(m) \le N_{current}(m), \quad N_{current}(m) \in \{1, \ldots, N_{\max}(m)\} \quad (3.45)$$

$m \in \{1,...,100\}$

**Power Consumption Agreement**

Note that $x$ is considered as the aggregated demand per $BAN$ by the $CC$. It is never aware of each individual $HAN$'s requirements in this regard.

**The Agreement Request Message**

This is an agreement between the $BAN$ and $CC$. The $BAN$ initially send an agreement request message $m_a$ to $CC$. This involves sending the requested (forecasted) amount $x$ in encrypted form i.e. $x$ is hashed to yield $(x_1, x_2) \pmod q$.

$$G_{ban} * S_1 - F_{ban} * S_2 = A_{ban3} + qB_{ban3} \tag{3.46}$$

$$-g_{bans} * S_1 + f_{bans} * S_2 = a_{ban3} + q * b_{ban3} \tag{3.47}$$

Thus the signature is;

$$S = s_{ban3} = f_{bans} * B_{ban3} + F_{ban} * b_{ban3} \pmod q \tag{3.48}$$

This will yield $S$ and $s_{ban3}$. Consequently the $BAN$ computes;

$$m_5 = S \| s_{ban3} \| T_{s_5} \| k_5 \tag{3.49}$$

After encrypting $m_5$ the $BAN$ sets $s_5, \varsigma \leftarrow \overline{\gamma_\alpha}$ and also uses $h_{cc}$ to generate:

$$m_b = h_{cc} s_5 + p\varsigma_5 + m_5 \in R_q \tag{3.50}$$

At the $CC$, $f_{cc}$ is used to decrypt $m_b$. $_{ban3}$ s is also verified, so is the validity of the time stamp.

If the need arises, the $BAN$ can adjust the requested power according to the following algorithm:

1. BAN Electricity Share Adjustment Procedure
2. $x$ : The xed demand for BAN
3. $y$ : The current actual demand for BAN
4. $z$ : The EV remaining capacity
5. $\beta : \beta = \|x - y\|$ : The dierence between x and y
6. **If** $(x > y \,\&\, \beta < z)$ then;
7. $\beta \leftarrow EV_{battery}$
8. else if $(x < y\beta\hat{} > z)$ then
9. $B - z \leftarrow CC$
10. else if $(x < y \,\&\, \beta > z)$ then
11. $\phi - z \rightarrow CC$
12. end if

Figure 3-6: Algorithm

### 3.4.4 Protocol Evaluation

The analysis of this scheme is in two parts, security analysis, and evaluation. The security analysis is done using a set of Java-based scripts of the NTRU public-key cryptosystem, comprising the signature NTRUSign and encryption NTRUEncrypt schemes [150].

#### 3.4.4.1 Security Analysis

As emphasized in the introductory stages of the subsection, the goal of the proposed scheme is to ensure privacy for the end-users, associated data (mostly billing) as well as entities. In addition, it should be able to provide sufficient confidentiality, integrity, availability, authenticity, and accountability guarantees. We thus analyse all these aspects in relation to the scheme's capabilities.

*Individual End-User's Privacy Preservation.* With respect to an individual's private information, the scheme thrives by all means to maintain privacy. This includes the concealment of the end-users ID, location, and power-consuming patterns. Whereas it is possible that the $CC$ can be a point of launching attacks by adversaries, however, note that the scheme, ($CC$) does not have details of the end user's details. Only the $BAN$ has the information. Neither is it able to extract finer details of individual power consumption bills, since the $BAN$ delvers such information in aggre-

gated form (i.e., for all the customers connected to it). In any case, all these messages are in encrypted form e.g., messages from $BAN$ to $CC$ are delivered in encrypted form. The use of both private and public keys means that only the $CC$ can decrypt the messages, as it has a corresponding deciphering key. Messages relayed from $HANs$ to the $BAN$ are also in encrypted form.

*Messages' Confidentiality is Guaranteed*. The agreement between parties such as the $CCs$ and $BANs$ are concluded and exchanged using public keys. As such confidentiality is maintained between these entities. The same applies to messages between the $HANs$ and $BAN$ gateways. As was earlier cited, the $TA$ assigns identities to $SMs$ and for this reason, MiTM attacks will not succeed. In short, the $SM$ 's ID s real identity is concealed. The use of signing signatures makes it further difficult to intercept and decrypt any messages, as an only authority with the correct signatures can do so.

*Integrity of Messages Exchanged*. Concerning the integrity of exchanged messages between $CC$ and $BAN$, note that they must be hashed and signed (using a private key). The $SMs$ also combine energy consumption-related messages together with their IDs, prior hashing them and relaying to $BANs$. The $SM$ details can only be validated by the $BAN$ since it has this information stored in its database Likewise, the database information is secured since stored data is encrypted by a private key disclosed only to the $TA$.

*Authenticity Guarantees*: Public keys are used to authenticate entities such as $CC$ and $BAN$. In that way, their messages are also authenticated as it is them who encrypt, formulate and encrypt the messages.

*Resources Availability:* $BAN$ gateways are secured from DoS attacks. The number of $HANs$ to a given $BAN$ is strictly limited and any extras (i.e., attackers) will immediately be detected

*Accountability:* Individuals are at liberty to validate as well as verify their bills at the local $BAN$. This is because the latter has information related to price changes. Moreover, there is a relatively low expected volume of message exchanges between the customer end and $BANs$. In that way adversaries may find it hard to intercept messages. The NTRU cryptosystem also prevents adversaries from obtaining any knowledge from any intercepted data. In summary, the scheme preserves customers' privacy.

#### 3.4.4.2 Performance Evaluation

We will look at the efficacies of the scheme in the following subsections. In this regard, we only carry out an analytical evaluation.

#### 3.4.4.2.1 Communication Overheads

In designing protocols and schemes some of whose operational aspects involve communication, it is important to evaluate the levels of communication overheads. Communication overhead refers to the extra data bits in the headers and message trailer flags. Such extra data does assist in proper addressing, flow, and error control as well as delineation at the receiver end.

Relatively, low volumes of messages are exchanged between the various parties in the proposed protocol scheme. This is partly because most of them are first aggregated, then dispatched as a multiparty message.

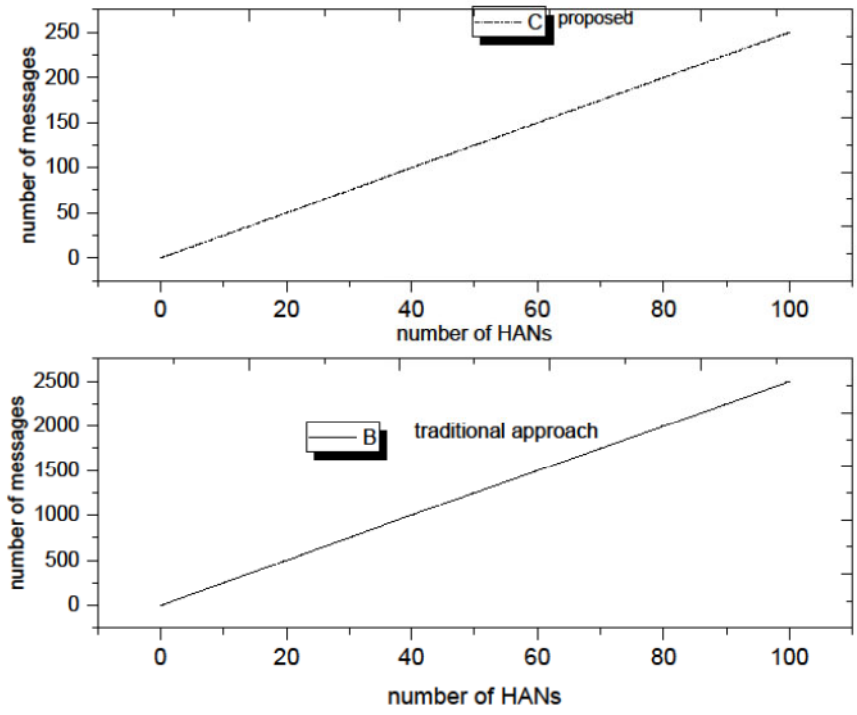


Figure 3-7: Comparisons of Communication Overheads (c) Proposed (b) Traditional

E.g., *BANs* do not participate in the initialization phase. However, only two messages each are exchanged by both CC and BAN when negotiating the power-share agreement, In the second phase *HANs* restrict themselves to sending demand messages provided this has been necessitated by a sudden change in demand or power tariffs. Figure 3.7 plots the communication overheads. The same Figure plots overhead levels for traditional approaches for comparison purposes. In this case, the number of *HANs* connections per *BAN* is varied gradually. It is clearly shown that the proposed scheme does lower the number of messages exchanged (and consequently communication overhead) in comparison with traditional approaches.

We subsequently explore the communication overhead loads for varying numbers of demand messages. i.e., the following five cases are considered:

- Case I: a fraction of the total number of *HANs* send a single power demand message over a 24-hour period (day), whilst the rest do not send any requests at all.
- Case II: Each *HAN* send a single power demand message per 24-hour period (day).
- Case III: Some *HANs* send two power demand messages each, others send a single message, and the rest do not send at all over a 24-hour period (day).
- Case IV: Each *HAN* send a couple of power demand messages per 24-hour period (day).

Case V: Each *HAN* dispatches three power demand messages every day.

Figure 3.8 plots the variation in communication overhead for the proposed taking into regard the five scenarios explained earlier. As can be observed from the graph, the number of messages to about 350 domain clusters has 120 *HANs*.

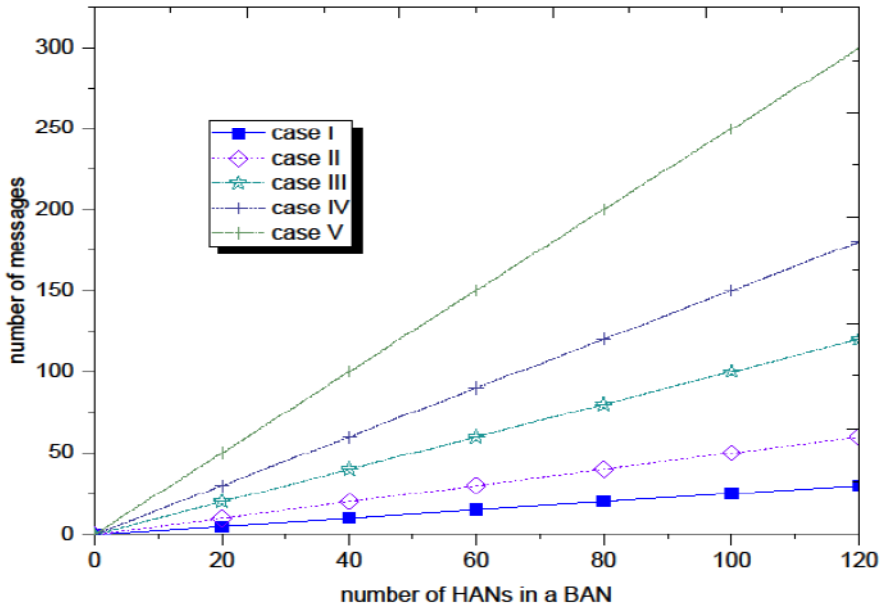


Figure 3-8: Communication Overhead Considering for Various Scenario Cases

#### 3.4.4.2.2 Computation Complexity

In the context of this work, computational overhead (loading) would be a combination of excess or indirect computation time, memory, bandwidth, or related resources that are required for the proposed scheme to perform the desired tasks (focused design objectives).

In this case, the computational times for signing ($T_S$), verification operations ($T_V$), encryption () $T_E$ and decryption ($T_D$) are taken into consideration.

Note that during the initialization phase, $CC$ and $BAN$ each performs a single cyphering operation, single decryption, as well as a once-off signing/verification. This equates to a computational time of:

$$C_I = 2\times[T_E + T_D + T_S + T_V] \tag{3.51}$$

For the next phase (phase II) a $HAN$ is likely to be involved in message exchanges in the form of demanding extra power allocations. In this case, it performs a single encryption operation which will be decrypted by the associated $BAN$. This equates to $T_E + T_D$ per data message. The likelihood that tariffs might change and hence necessitates communication between $CC$ and $BAN$, thus the computation time is $2\times[T_S] + T_V$. If the number of $HANs$ is $m$, the total computational time becomes;

$$m(T_E + T_D) + (2T_S + (m+1)T_V) \tag{3.52}$$

In the next phase, i.e. billing, the message is sent to $CC$ from $BAN$ this necessitating one encryption, one decryption, one sign and one verification process. Following the method used in [150], to approximate, the aggregate computational times, we have;

$$C_{proposed} = 90\times[T_E + T_D + T_S + T_V] \tag{3.53}$$

$$C_{traditioal} = 810\times[T_E + T_D + T_S + T_V] \tag{3.54}$$

Figure 3.9 plots, the aggregate computational times of our proposed scheme.

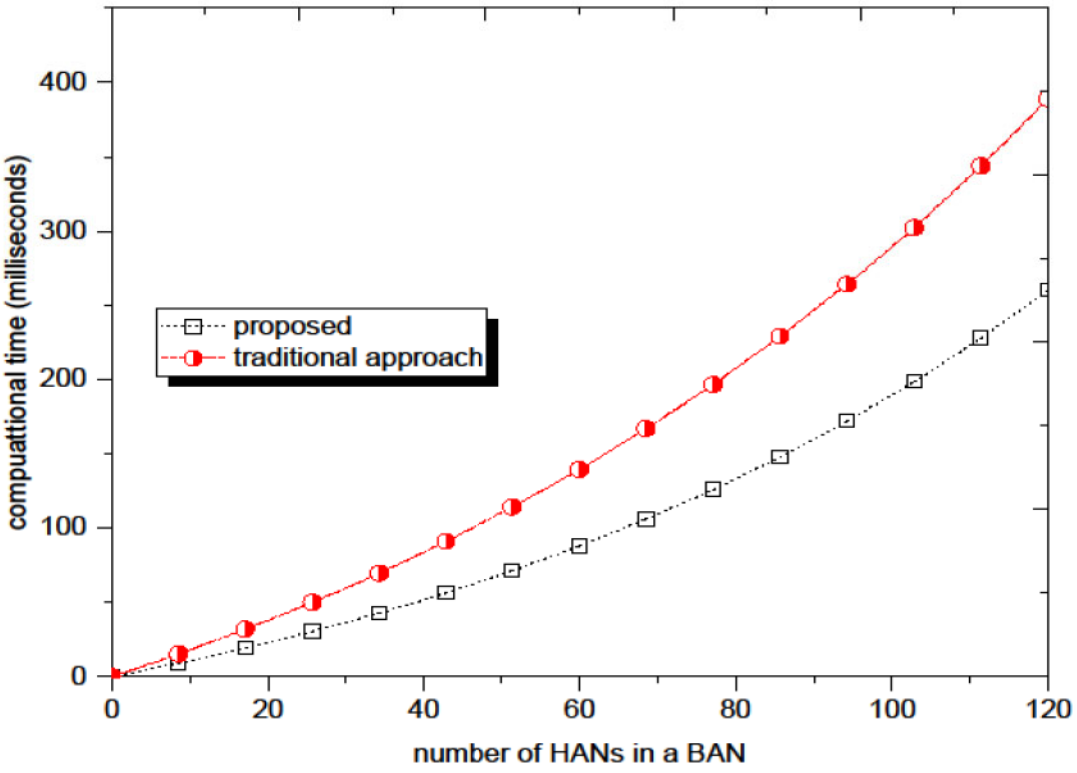


Figure 3-9: Computation Overhead Traditional vs. Proposed Scheme.

From the plotted graph, it is observed that an increase in the number of *HANs* results in computational time increases. However, by comparison, the increases are much lower for the proposed scheme. Thus overall, our scheme manages to execute fast, despite the limited computational resources. The computational time fit within the expected time frame scales of a fully fletched SG network.

We now evaluate a worst-case scenario, in which all *HANs* in a cluster domain send the maximum possible dumber of power demand messages.

Figure 3.10 provides a plot of the computational times in this worst-case scenario.

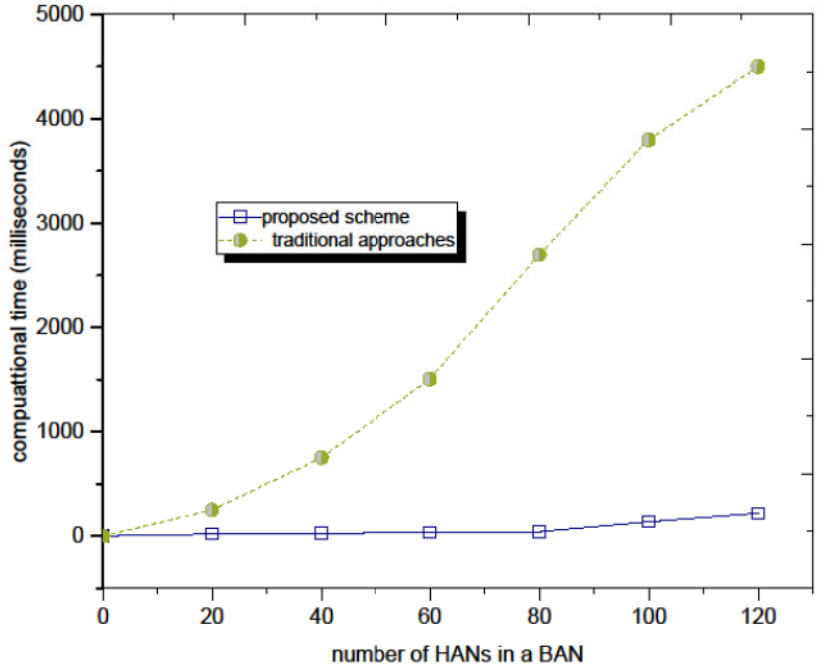


Figure 3-10: Computation Overhead Traditional vs. Proposed Scheme.

Once again, the aggregated computational times for the proposed versus traditional approach schemes are plotted and compared. The proposed scheme has a much reduced computational overhead hence the computational times are comparably less.

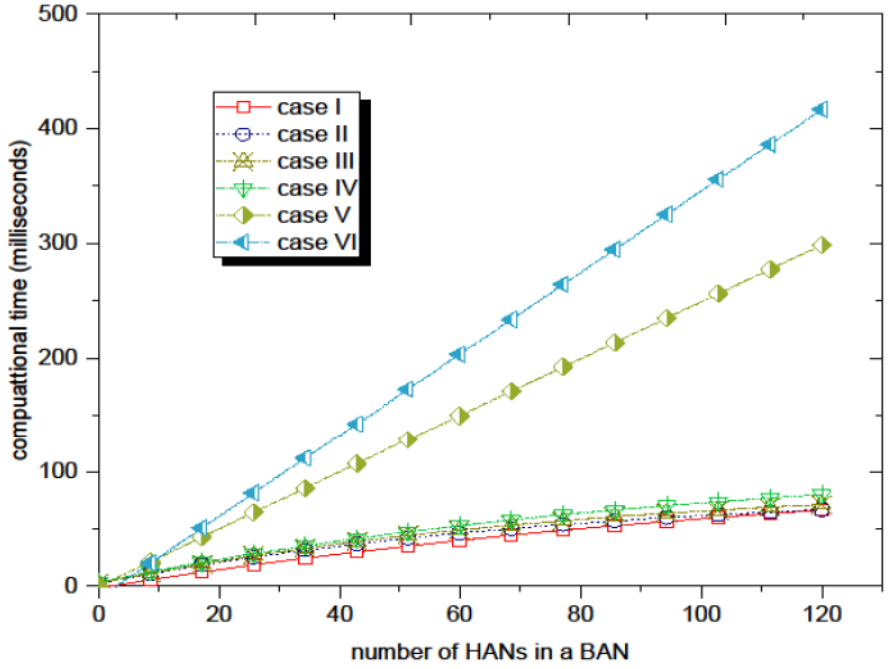


Figure 3-11: Computation Overheads Comparisons.

The five case scenarios (repeated) plus an additional sixth case, are once again considered as we explore aggregated computational times.

- Case I: a fraction of the total number of *HANs* send a single power demand message over a 24-hour period (day), whilst the rest do not send any requests at all.
- Case II: Each *HAN* send a single power demand message per 24-hour period (day).
- Case III: Some *HANs* send two power demand messages each, others send a single message, and the rest do not send at all over a 24-hour period (day).
- Case IV: Each *HAN* send a couple of power demand messages per 24-hour period (day).
- Case VI: Each HAN sends a maximum possible number of power demand messages per 24-hour period (day).

As can be observed from the same graph, the computational complexity relatively rises with increases in power demand messages. We thus can conclude that the proposed scheme guarantees privacy and at the same time it minimizes computational and communication overhead levels.

## 3.5 Chapter Summary

The chapter has reviewed privacy issues in SGs. Several attack options geared towards compromising privacy for end-users and entities are outlined. Key requirements for privacy are also discussed. Based on the literature survey, we carried out a lightweight based data aggregation that ensures privacy, as well as confidentiality, is proposed. It is centered on forecasting power consumption demands for a particular neighbourhood, and overall, because most attacks occur, during the transmission of data across the ICT subsystem, it thus focuses on limiting that. It does so by first forecasting its demands, and only links with the utility operator (CC) when adjustments have become necessary. It is a desirable goal that the scheme satisfies all desirable privacy objectives, is robust, as well as is lightweight. Furthermore, the scheme has the objective of minimizing both communication and computational overheads.

# 4. Physical Security Considerations in Smart Grids

## 4.1 Introduction

To ensure service reliability, and efficiency in the operation of next-generation SGs, adequate security measures must be put in place. It is necessary that addressing and deploying key security measures must be rolled out alongside the planning and deployment of the rest of the SG infrastructures.

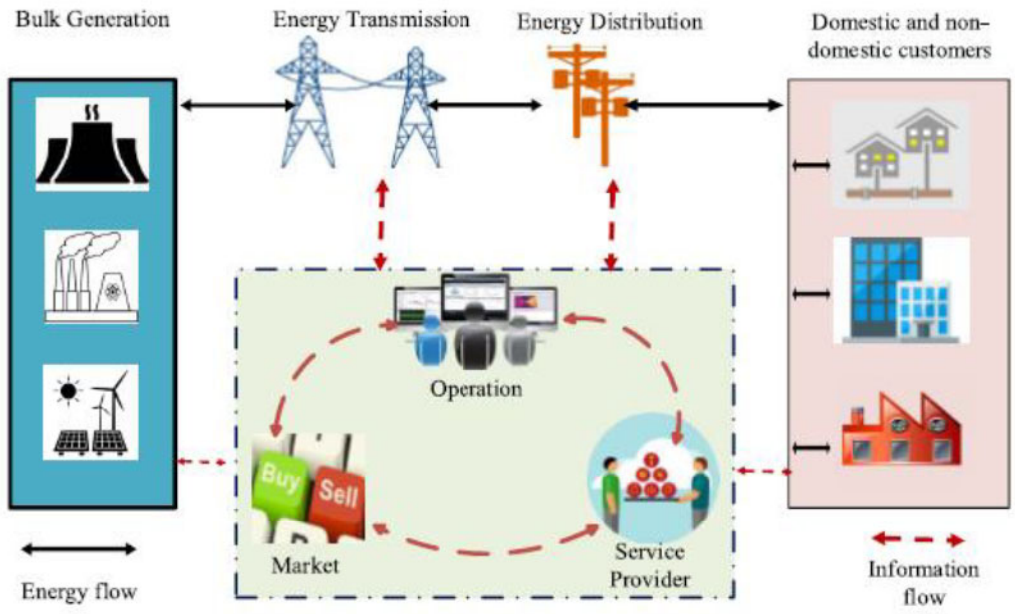


Figure 4-1: An Architectural and Service Level of the SG

In short, the bulk generation, transmission, distribution, and end-user infrastructures must be planned concurrently with the required security. Notably, the objectives of modern SGs are to minimize power energy losses through theft or physical dissipation. It becomes more feasible and practical to maintain a reasonable balance between generation and consumption for prolonged periods, and thus this brings stability to the grid. Furthermore, the grid's operations become efficient as well as reliable. Key measuring elements such as smart meters (SMs), frequency meters (FMs), as well as phasor measurement units (PMUs) are incorporated to achieve the grid's efficiency objective. Their security must be ensured at all times. Additionally, these same three key units will be able to provide periodic updates of key information and data to the SG central control and management center. As an example, SMs are located at end-user side networks to aggregate the power usage for each user and relay it to billing centers.

## 4.2. Literature Survey on Security in SGs

Security: In [151], the authors analyzed general security challenges in various parts of SGS. Case studies are carried out herein with reference to the key components such as renewable generation, low and high-frequency transmission of power, distribution as well as billing in the customer side networks. Also discussed herein are cryptographic-based countermeasures that include, authentication, key distribution, and management in different sections of an SG.

Likewise, in [151] the authors focus on SG and smart home security, and in particular the interactions between the SG and HANs. After categorizing various security threats, they also evaluate theoretical impacts. Furthermore, key security countermeasures are suggested. These include authentication and general physical security. However, the work did not provide any critical comparative analysis of the then existing schemes.

Security in respect of data-driven approaches is discussed in [152]. The data-driven approaches include, data acquisition, data storage, data generation, and data processing security. Various security analytics techniques, such as data mining statistical methods, and visualization are discussed. Whereas the work sounded quite extensive, it however fell short of further evaluating adverse implications and other complexities in terms of deployment in existing SG. SMs and data intelligence techniques for future energy systems are discussed in [153]. Intelligence tools such as support vector machines, and fuzzy logic are explored. The whole idea was to elevate intelligence in SMs such to detect any abnormalities in real time. Typical examples explored herein included end user profiling and load forecasting. However, the authors fall short of relating the detection of abnormalities, end user profiling and load forecasting to the enhancement of security.

Cyber-physical attacks are discussed in [154],[155]. In particular attack scenarios on various sections and entities of SGs are exemplified. Counter measures such as protection, detection and mitigation are mitigated upon. However no comparative analysis of the various counter measures is carried out hence extending this work would be a key step.

The authors in [155] discuss cyber-attacks in IoT enabled networks and environments. They exemplify as well as model a threat vector that can be utilized by adversaries in attacking various IoT devices and elements. In this same work, the authors point out at hidden IoT enabled attack paths. The works however falls short of providing an in-depth mitigation of would-be feasible counter measures.

## 4.3 Security Goals in SG Metering Networks

In this subsection, we provide a list of tamperings that can take place in several ways such as altering, blocking, deleting, and replaying genuine metering information, or by injecting unauthorized information into the network. Since data is used for a variety of reasons, including handling energy and planning potential network expansions, interfering with valid metering data may cause monetary losses. To disrupt the grid's regular activity, attackers could tamper with the metering data obtained. Because data is used for grid matching and forecasting potential energy demands, the altered data may distort power demand forecasts, leading to a rise in grid imbalance. A spike in disparity would not only raise operating costs but could also result in a blackout. Internal agencies may also tamper with legal metering data in order to increase revenue or cut costs. Utilities can try to rig metering data to maximize their prices. In order to lower their bills, some unethical consumers can try to tamper with their own metering results.

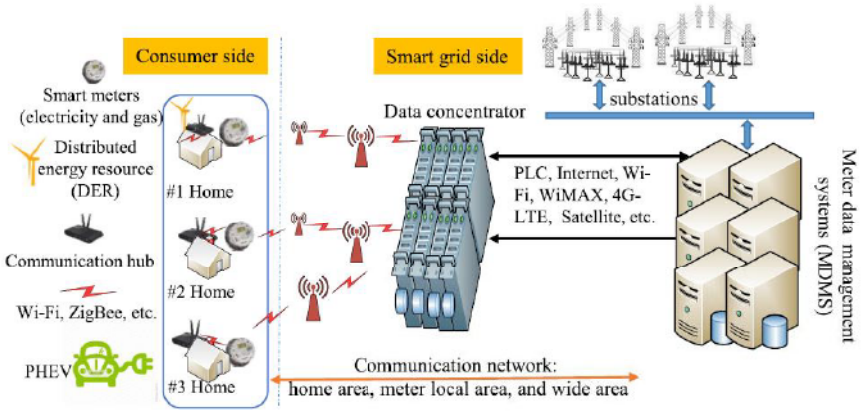


*Figure 4-2:* SG's AMI

The AMI network considered to have stringent time frames as far as its operations are concerned. Typical time scales are provided in Table 4.1

Table 4.1: Latency Requirements for Services

| Time Latency | Services/Applications |
|---|---|
| ≤3.5ms | protectiverelaying todetectmulfunctioning units |
| Subseconds | moniting a unit sttaein a WAN |
| Seconds | substationcontroland feeder management |
| Minutes | peridoc checking of uncritical devices and pricing |
| Hours | energy usageunit and wholesale - market pricing |
| Days | long term monitoring |

We define security and privacy criteria for the AMR framework based on the AMR functional requirements, threat analysis, and metering details. The requirements are:

***Authentication:*** A system should be able to verify that it is communicating with the person it appears to be. To prevent impersonation attacks, this provision should be implemented.

***Authenticity:*** A message's receiver should be confident that it has not been tampered with in route, that it is current, and that it came from the claimed source. This clause should be strictly enforced to prevent tampering.

***Confidentiality:*** Users' metering data should not be shared with unauthorized third parties to prevent eavesdropping attacks.

***Authorization:*** Only approved SG agencies can have access to their users' metering data.

Privacy security for consumers:

- No SG agency should have access to individual user metering data.
- Only the user should have access to their metering data.

***Verifiability:*** Utilities should be able to verify that the metering data they receive from their customers is accurate.

***Availability:*** AMR protocols should be designed to be resistant to DoS attacks.

**Non-repudiation**: It is key that non-repudiation must be guaranteed or prevented. By this it implies an individual or entity completely denying his/her previous actions.

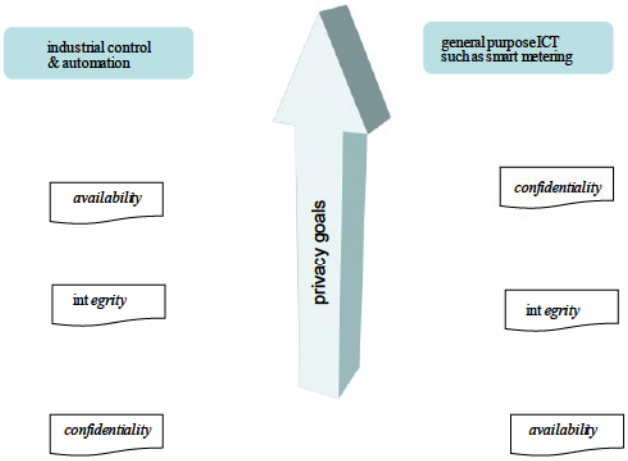


Figure 4-3: Summary of Security Goals

**Access control:** Some degree of access control must be enforced so that only authorized parties may have access to data. This is because the common sharing of data and databases is quite prevalent in SGs. A typical example is shared usage, control, and management data. It is mandatory that each entity requiring access to such data must be authorized first.

**Accountability and auditing:** It is necessary to enforce measures that ensure regularised as well as periodic accountability and auditing to further validate the security mechanisms for the SG metering network systems.

## 4.4 SG Metering Network and System Level Threats

### 4.4.1 SG Metering Network

As already known, an SG metering network facilitates a two-way communication for data exchanges data between end customers and utilities. Constituting the entire system, is sensors, SMs, monitoring systems e.tc. SMs are the direct interfaces (units) for the acquisition of end user power usage data. In addition, we have units such as Consumer Awareness Systems (CAS), Interactive Services for Energy Demand Regulation (ISER) Systems to help with the prevention of energy-associated fraud, and precise billing respectively. The figure next, conceptualizes the SG metering network system.

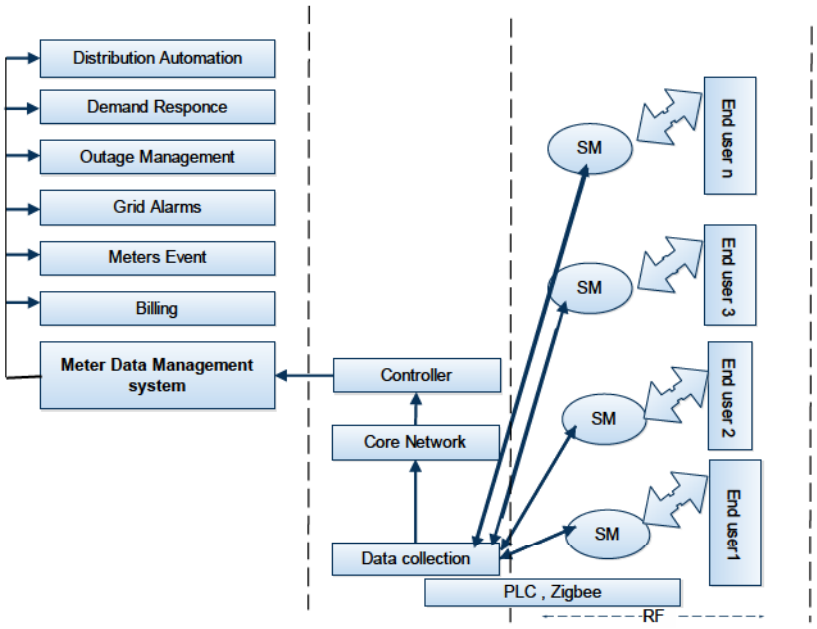


Figure 4-4: SG Metering System Conceptualization

Often SMs operate as aggregators, sending data to collection units, which in turn relay it to MDMSes. The MDMS analyzes received raw data to create usable statistics and gives clients with power

use data. Outage extent evaluation, outage recovery verification, and invoicing applications, are all possible forms of information extractable from SM read data. Sending the message within the delay bounds is particularly challenging since all SMs power constrained devices. As a result, for high numbers of SMs, it is necessary to establish network connectivity over short durations.

### 4.4.2 SG Metering Network Security

The SG metering network systems (also referred to as AMI) is prone to security threats and these can generally exemplified as follows [154]:

*Radio Subversion or Takeover:*

The reliance on radio communications makes the system vulnerable to attacks, in that the RF channels can easily be intercepted or jammed. Once accomplished, it becomes possible to disrupt all SMs and their communication with BANs in the affected areas.

C*redential Compromise*

Use of weak authentication (including public and private keys) makes an entire system vulnerable to credentials capture. In this case, the adversaries only need to capture an adequate number of credential sets before using them to halt the SG systems.

*Availability Compromises at Back Office*

Adversaries can always attack vulnerable units such as processing servers and install malware such as (Black energy ). The malware will then be launched to ground the entire systems. In particular malware such as KillDisk can also be used corrupt or overwrite MBRs in servers.

*Network Barge-In by Unknown*

The multi-hop nature of SG communications means that certain sections of the links/ paths may be prone to attacks. As an example, an SM located at the end user network side has to relay its data to higher levels via multiple hops. In the process relay nodes are relied upon to get the data to the intended destinations. As such most of the intermediary relays are often unguarded and vulnerable thereof. Typical attacks that may be launched include M-iTM attacks. The result is that the communication modules may end up malfunctioning.

*Denial of Service*

This is a threat mostly focused on degrading operational performances. Often, depending on the severity of such attacks sections or the entire SG may grind to a halt. There are various ways of achieving DoS attacks. These include:

- Radio frequency (RF) spectrum jamming in which the operational frequency spectrum is blocked or deliberately garbaged with excessive noise levels.
- Targeted end user devices can also be prevented from receiving data from key sender.
- Routing attacks are also quite commonly used to achieve DoS. Typically, endless loops can be imitated in one or more sections of a network, with the result that traffic loads in the affected sections become to excessive.
- Jabbering is also another popular method used. In this case a single remote device is caused to send excessive levels of data, hence ending up dominating the receiver end. In this case all other devices can no longer communicate with the targeted receiver.
- Stack smashing is mainly application layer level based.

### 4.4.3 Security Threats Via AMI

Most of these attacks will be via the SMs themselves. Such attacks are generalised in the next figure [155].

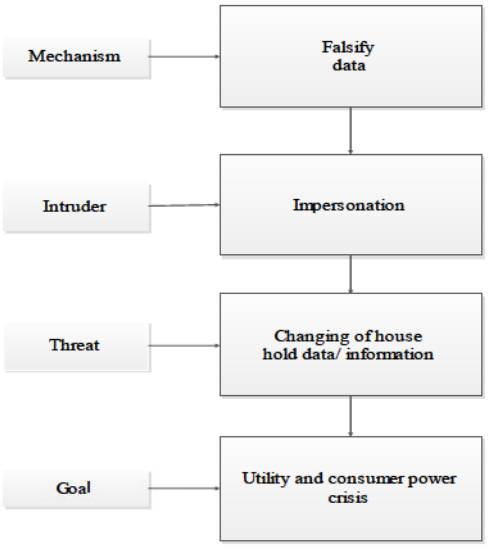


Figure 4-5: Potential Attacks

The attacks can come in various forms e.g.

- By repeatedly transmitting unauthorized data, an intruder may obstruct the data transmission line as earlier cited. This places both the sender and receiver under a lot of stress and can cause them to shut down completely.
- By altering the synchronisation speed, thus making network's SMs to be out of sync with the servers, the time-stamping on the collected data becomes invalid and data ultimately rejected.
- Attackers can simply power off equipment.
- Attacker may excessively stream messages across the network, and in the process slow down desired network responses.

We further list down examples as follows:

**Dictionary Attacks**

A dictionary attack is a means of breaking a cipher or authentication scheme by trying to figure out the decryption key in cryptanalysis. Trial and error with several key options, usually words in a dictionary are used in such methods in the hopes to match it with the decryption key. As a result, an attacker could finally be able to decode the records. When the combination is right, it means the intruder has succeeded [154].

After encrypting the usage data, the AMR device sends it to the utility collector. The suggested protection uses monitoring protocol, on the other hand, protects against the attack by using a random number. In reality, since the SM sends reports to the utility in such a short time and the ordinary consumers in households consume such a small volume of energy in such a short time, often a few kilowatts, an opponent is likely to be aware of the whole continuum of data that is being reported at all times [154].

**Packets Replay Attacks**

In this case, actual data is maliciously repeated or interrupted. By resending authenticated messages, this attack tries to get around the authentication process.

**Traffic Analysis**

Intercepting and analysing messages to evaluate the data patterns in a messaging medium constitutes traffic analysis which itself is a malicious act and as such a security threat. This method of

attacks aims at collecting all of nodes contact behaviours to generate activity patterns. An attacker cannot decode the messages contents, but instead will time when the AMR machine transfers data to the utility.

**Impersonation Attacks**

Theft of another entity's name is known as impersonation. An adversary may also set up a false SM on the AMR network, which can connect with a targeted victim's SM and analyse the packets, possibly compromising security as well as privacy [155].

**Eavesdropping Attacks**

Eavesdropping is a passive attack in which an adversary intercepts data packets between service collectors and SMs on the network. After that, an adversary attempts to inspect the packages in order to assess their data integrity

**Location Migration**

SMs are switched from high tariff zones to lower tariff ones. Another such attack would be to switch from high usage zones to low ones. In that way the SG will be deprived of potential revenues.

## 4.5 A Group Authentication and Data Security Scheme for Smart Metering In SGs

In this section, wwe propose a secure and scalable framework for ensuring privacy and security in the *SG* IoT compatible communication architecture that provides interconnectivity to multiple authorities, as well as devices and elements which are part of the *SG* system. Our framework emphasizes complete users' access control as well as privacy on their data.

### 4.5.1 D2D Communication Phases

The introduction of next generation power grid systems referred to as SGs has brought about improved operational efficiencies in terms of demand, supply and marketing. The incorporation of distributed control and management infrastructures has brought about new and innovative applications and services. However, this latter development has brought about various privacy as well as various security issues which need to be addressed adequately. Security threats such as semantic attacks, physical attacks as well as nature related disasters are prominent examples of threats with regard to SGs deployment which if not addressed can ultimately lead to a complete infrastructural collapse, increased revenue losses due to energy theft, power blackouts, SG user privacy breaches,

as well as safety compromise to of operating and maintenance personnel. It is therefore imperative that privacy and security issues in the SGs be critically addressed so as to minimize as well as avoid possible failures or threats.

Key to the successful operation of future generation SGs would be an enabling communication subsystem to interconnect the various distributed computing systems. Harnessing the already available IoT as the pillar communication subsystem for SGs has added advantages. The International Telecommunications Union (ITU) defines an IoT enabled network as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.

The diversity in terms of dimensions and the scopes of an IoT enabled network has prompted standardization in order to establish interoperability among interconnected things in SGs. In this regard, several standardization authorities are currently working or wrapping up relevant standards.

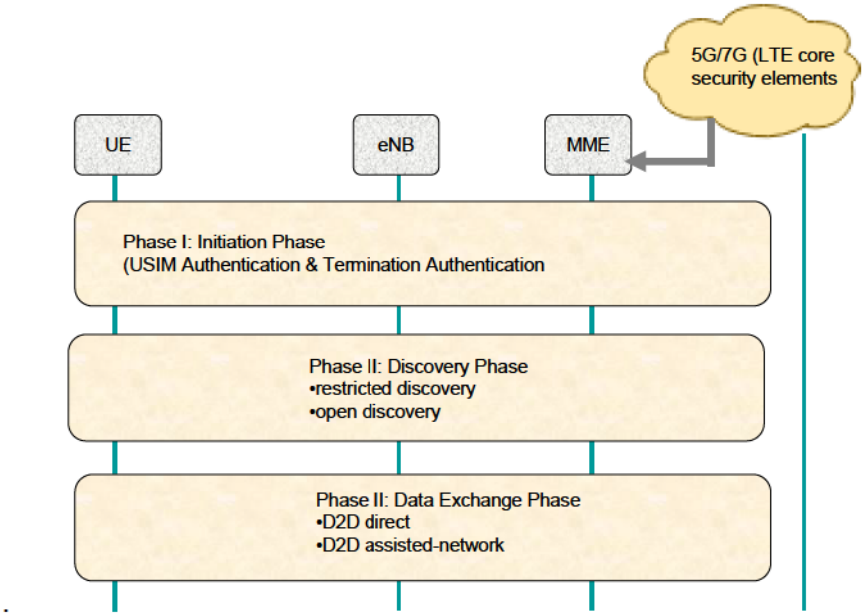


Figure 4-6: Summary IoT's D2D Communication Phases

To provide a common seamless SG communication subsystem platform for the envisaged multitudes of services and applications, a D2D group communication standard is being defined. Most individual applications or services in the SG involve the collaboration of devices constituting a group. Typical such examples would be multicasting targeted users for power usage regulation purposes or data acquisition from smart meters. In this regard D2D group communication has the potential to afford high data rates, minimal end to end latencies, as well as matured peer discovery mechanisms. A typical D2D communication is characterized by three distinct phases namely,

initialization, discovery and data exchanges as illustrated in Figure 4.6. Privacy and security issues are considered key milestones in such communications and thus the required authentication as well other security requirements for Phase I are provided by the core network itself whereas additional security requirements are needed for the other two phases. Typically, services and applications will involve the cooperation and interaction of devices within proximity forming a group. Thus, efficient device discovery mechanisms are required for detecting the proximity of such D2D communication-enabled devices. When initiating a service targeted device are expected to detect peers within proximity to potentially establish the required D2D communication session.

Third party companies may from time to time acquire various *SG* related data for varying purposes. E.g., a billing company (*BC*) will from time to time collect users' energy consumption data for billing purposes. Often this is done on a monthly basis. Frequent performance monitoring of certain key devices and elements within the *SG* infrastructure may be necessary in order to detect potential problems and rectify them before breakdown. Hence the need to ensure that the operations and maintenance acquired data is also reliably exchanged among authorized entities. Because an *SG* afford users the ability to generate and trade power, hence various companies may from time to time need user's energy consumption data for further analysis as well as for market related research purposes. In all cases users must be ensured of complete control over their own data in terms of its confidentiality as well as accessibility. Thus, security as well as privacy is of paramount importance.

In legacy power systems the utility's trust certificates were used as a security tool by SMs to decide on whether it can accept the acquisition of data from it or not. The same certificates would be relied upon to decide on whether to release requested data or not. This approach may not be practically feasible for the envisaged massive SG network's SMs to memorize all the identities. The use of X.509 protocol based public keys does not provide sufficient security guarantees as any slight breach may cause massive repercussions as well as possible disruption of the SG infrastructural network. Reference [153] suggests loading all data and related security information into specialized servers or repositories from where it can be tapped by various companies. In this case each data server/repository will be responsible for strict access control. Any security breach on the part of a single server/data repository will result in the revelation of all the data it maintains.

Recently the implementation of attribute-based encryption (ABE) in SGs has been suggested in order to address the underlying privacy and security challenges. With this encryption approach, all key SG devices and elements cipher their data on a set of attributes, which regulate the access to the data. Authorized parties that may otherwise have different identities will be able to decipher

the data independently provided they possess appropriate sets of required attributes. In this way data exchanges in the SG are exchanged between sources and recipients securely but without disclosing unnecessary details to either parties. In short ABE facilitates a secured multicasting of the user's data to multiple recipients , and at the same time the SMs do not need to furnish the recipient's detailed identity.

The authors in [157] proposed a version of ABE called, Ciphertext- Policy ABE (CP ABE), that guarantees a secure role-based access control as well as multicasting of data generated or stored in the SG's various components. For an example, even if the data stored in any of its repositories was to be compromised only the encrypted data is leaked and without knowledge of the related/ required attributes decrypting it would not be possible. Notably CP-ABE does not make prior checks on entities' privilege before deciding on whether access is granted or not as is the case with conventional software based systems.

### 4.5.2 Existing Group Authentication and Key Agreement Schemes

Quite a number of group privacy and security protocols specifically relating to groups AKA continue to be explored. Security requirements such as confidentiality, mutual authentication, privacy preservation, integrity and most importantly utilizing a common and single security (encryption) key during the communication sessions in the IoT network is preferred. Such protocols need to inherently achieve efficacy in maintaining the group key unlink ability as well as generate minimal overheads that otherwise may lead to network congestion. To alleviate signaling related congestion the authors in [158] proposed a congestion avoidance approach in which a group of devices delegate a leader to handle the communications on behalf of the rest of the group members. In this way the volumes of aggregated signaling overheads is significantly lowered and so is the congestion.

The same approach was revisited by the authors in [159] in which they propose a group AKA (G-AKA) protocol. In this case a single device from the group is authenticated by the AKA authority in the SG, after which the same device is now delegated to authenticate the remaining devices of the group. One disadvantage with such a protocol is that of the possibility of high levels of signaling overhead being generated should several devices wish to gain access to the SG network simultaneously. It has also been shown that the protocol is so secure in preventing to potential threats such, as DoS and redirection attacks.

A symmetric key based AKA (SE-AKA) protocol that enhances both data integrity and confidentiality was investigated in [160]. Whereas the protocol shows improvements in security, it however generates massive signaling overheads that ultimately lead to network signaling congestion.
In [161] an enhanced group AKA (EG-AKA) protocol is proposed to authenticate a targeted group of devices. The protocol is quite computationally intensive due to the use of asymmetric key operations. Other similar authentication schemes are explored in [162], [163].

### 4.5.3 IoT Communication Subsystem

In order to provide privacy as well as security in an AMI service secure authentication and key exchange among the D2D communication compliant smart meters (SMs) is necessary. A third-generation partnership project (3GPP) IoT enabled network architecture is assumed as illustrated in Figure 4.7.

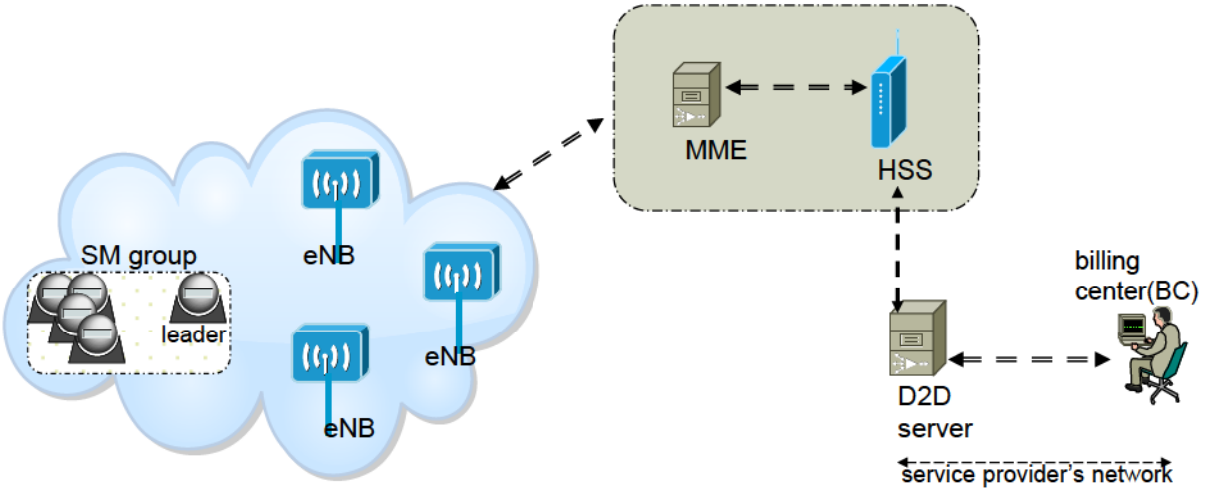


Figure 4-7: SG IoT Enabled Communication Subsystem Architecture.

Key security related blocks defining the SG communication subsystem include the D2D communication server, (D2D), home subscriber server (HSS) and mobility management entity (MME). The HSS retains attributes information of the SM devices and relies on the MME to verify the SMs by way of granting a set of authentication tokens. The billing entity (which is part of the service provider control authority) can be regarded as a D2D user and as such remains outside the core SG communication network domain. To facilitate SM data reading in a particular area the D2D server connects to both the BC as well as SMs. Upon successful authentication among the parties the data read from the SMs can now be furnished to the BC. The AMI service infrastructure abstractly comprises: the BC, neighborhood located data collectors (DCs) and the SMs.

The required communication link is provided by the available IoT enabled network. This is illustrated in Fig. 4.8.

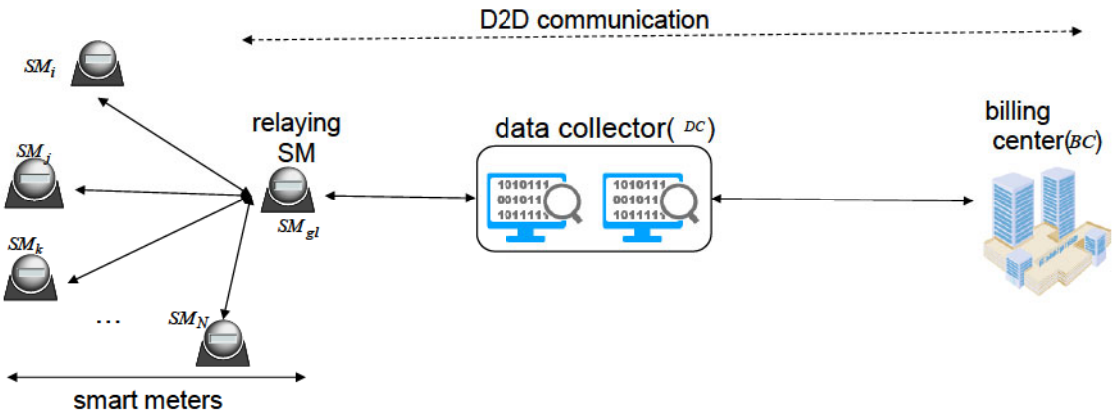


Figure 4-8: Abstracted AMI Service

The data exchanges between the various entities constituting the AMI traverse one or multiple collectors and possibly through other SMs acting as relay points. D2D communications is assumed between the BC and DCs. As such all SMs deployed in the SG are assumed to be D2D communication compliant and physically unclonable. Data load handling in SMs addressed by way of data aggregation in which data from various remote units is combined together before relaying across the network via a designated relaying $SM$ . The same relaying $SM$ becomes a group leader ( $SM_{gl}$ ). In that way both the bandwidth as well as links are utilized more efficiently.

### 4.5.4 Model and Group Authentication

In this section we briefly describe the security framework that we will refer to as the Smart Meter Group Authentication and Key agreement scheme (SM-AKA). We assume that each approved $SM$ is preloaded with a private ( $A^-$ ) as well as a public key ( $A^+$ ) on a long-term basis. Similarly, both the $DC$ and authorized billing center ( $BC$ ) are also preloaded with their own private/public key pairs on a long-term basis. For shared key establishment, $SMs$ , $DCs$ and $BC$ commonly make use of Diffie-Hellman ( $DH$ ) parameters $g$ and $p$ [160]. They all agree on the use of the following elementary cryptographic operations:

i. public encryption key on message;

$$M \rightarrow Public\_key(K,M) \tag{4.1}$$

ii. Symmetric key encryption on the same message using the key in step i;

$$i \rightarrow symmetric\_key(K,M) \tag{4.2}$$

iii. Signature of the message by $_A$ a derivative of ($A^-$);

$$signature)\_(A,M) \tag{4.3}$$

iv. Computing of the hash key of the message using the same key $hash\_(k,M)$.

v. We assume a centralized key generation center ($KGC$) and is available for use within the $SG$ by authorize parties.

Our security objective is to ensure that the data read from $SMs$ can only be read by an authorized $BC$ and thus it is necessary to efficiently encrypt the data exchanged between a designated $DC$ and $BC$. In practice the entire data collection procedure has a tree like formation. The $DC$ then collects the data from all the targeted $SM$ group members via the designated group's leader ($SM_{gl}$). The collected data is then forwarded to the $BC$ via the available network.

The detailed descriptions are as follows:

*Session Request and SM Group Registration*

A $BC$ is routinely requested to acquire data from $SMs$ within the $SG$ and as such registers for the AMI service with the service provider ($SP$).

As an authorized user with a real and valid identifier ($RID_i$) the $BC$ completes the necessary registration formalities with the local $HSS$. If access is granted the $HSS$ acknowledges by generating and issuing a pseudonym ID ($pseudo\_PID_i$) to the $BC$.

$$pseudo\_PID_i \overset{def}{=} (pseudoID, ExpiryTime) \tag{4.4}$$

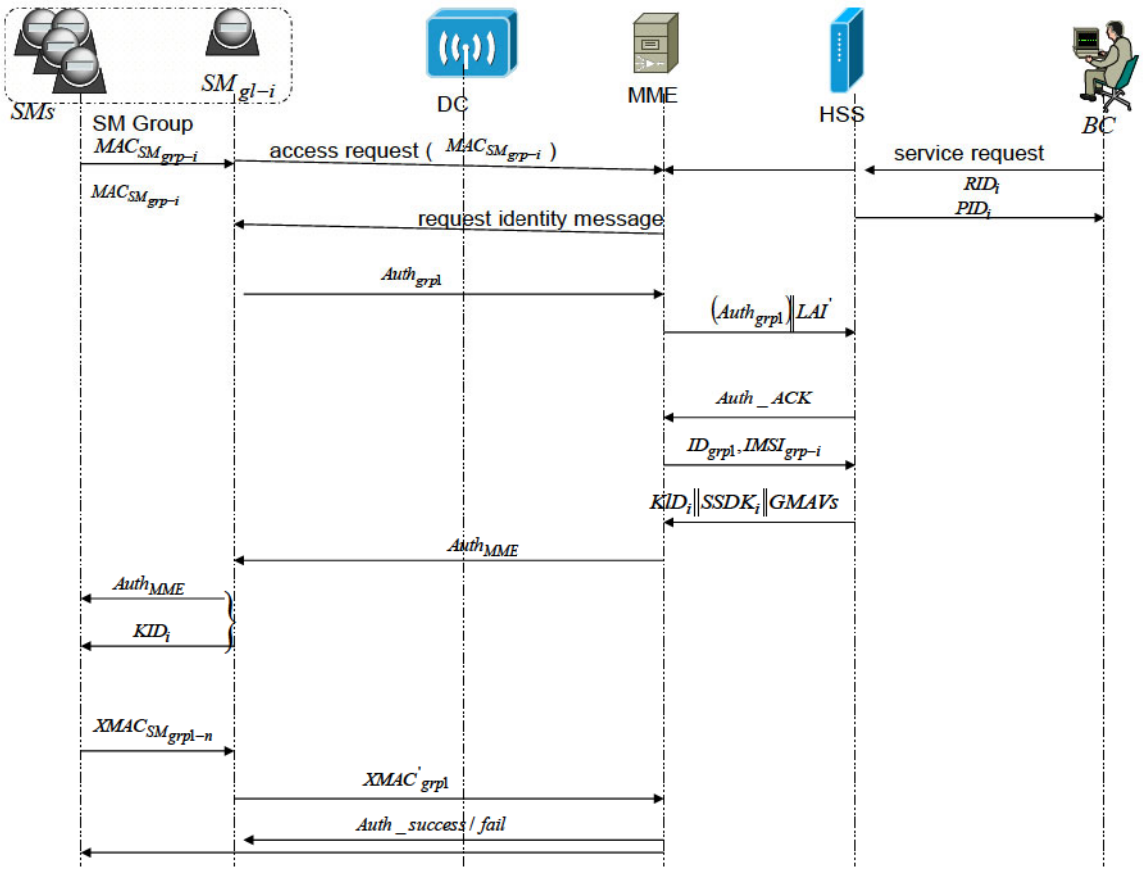


Figure 4-9: Sequence Events for the Proposed Framework

The already generated $RID_i$ will further be used in the $SM$ group discovery (formation) as well as the initialization process. All members of the $SM$ group ( $SM_{grp-i}$ ) must be authenticated as well by the $HSS$. In this regard the latter generates a set of random numbers $\mathbf{R_z} \in \mathbf{Z_p^*}(z = 1,2,...i)$ that will be used to compute a set of temporary identities $TID_{SM_{i-j}}$ to each $SM$ in that group:

$$TID_z = h_1(ID_{MTCD} \| \mathbf{R_z} * x) \tag{4.5}$$

where,

$h_1(.)$ is a secure hash function with parameters $_p$ and $_q$; $_x$ is $HSS$'s own secret authentication key. The $HSS$ further computes the newly formed group's authentication key as follows:

$$GK_i = h_3(\sec_{i-1} \oplus \sec_{i-2} \oplus ..., \oplus \sec_{i-j} \oplus g * x) \tag{4.6}$$

where $h_3(.)$ is a hash key and $g-$is a random integer.

*Group Authentication and Key Agreement*

In order to maintain group privacy as well as security individual $SMs$ in the group must mutually authenticate as belonging to the group, $SM_{grp-i}$. The $SP$ then assigns a key ($K_{grpi-j}$) to each group member, as well as generating a group key which will be used for mutual authentication as well as privacy protection between the group's members and $SP$. This is done mainly by the group's leader ($SM_{gl-i}$) and the $HSS$. This is carried out in sequence as follows:

1. Each group member shares a fresh temporary identifier ($TID_{SM_{i-j}}$) and associated token $f(TID_{SM_{i-j}})$ with the group's leader.

$$SM_{i-j} \rightarrow \left\lfloor TID_{SM_{i-j}}, f(TID_{SM_{i-j}}) \right\rfloor \Rightarrow SM_{gl} \tag{4.7}$$

2. This is followed by the group's leader calculating the Lagrange component (LC) vector for the group. For it to do so, it will first acquire $TID_{SM_{i-j}}$ and $f(TID_{SM_{i-j}})$ values from the $KGC$.

The general formula it uses for the LC computation is;

$$LC_{grp-i} = f(TID_{SM_{1-i}}) \prod_{q=1, q\neq j}^{\frac{n}{m}} \frac{-TID_{SM_{1-q}}}{TID_{SM_{i-j}} - TID_{SM_{i-q}}} \bmod p \tag{4.8}$$

This computed component is shared with all group members for mutual authentication purposes within the group. This step is necessary in order to ensure that unauthorized $SMs$ or other devices may not have access to the data being collected.

3. Upon successful completion of the previous step, the group leader further authenticates with the core network ($MME$) on behalf of the entire group. It does by furnishing both the group's $MAC_{grp-i}$ and $Auth_{grp-i}$ computed values.

$$MAC_{grp-i} = h_2(GK \| ID_{grp-i} \| LAI \| S') \tag{4.9}$$

$$Auth_{grp-i} = (TID_{grp-i} \| MAC_{grp-i}) \tag{4.10}$$

$$SM_{gl-i} \xrightarrow{Auth_{grp-i}, TID_{SM_{i-1}}, \ldots TID_{SM_{i-j}}} MME \tag{4.11}$$

4. $MME$ will then confirm the legitimacy of the group's existence with $HSS$.

$$MME \xrightarrow{Auth_{grp-i}, LAI} HSS \tag{4.12}$$

5. The $HSS$ authenticates the group by recalculating the group's $MAC_{grp-i}$ based on values furnished by the $MME$.

$$MAC'_{grp-i} = h_2(GK \| ID_{grp-i} \| LAI \| S) \tag{4.13}$$

If authentication is successful at this stage, $HSS$ generates a temporary group key ($TGK$) for the group as follows:

$$TGK_{grp-i} = h_3(GK \| r_{HSS}) \tag{4.14}$$

where, $r_{HSS}$ is a random integer.

6. $HSS$ confirms the successful authentication with the $MME$ in which case the latter further computes its own $LC$ ($LC_{MME}$) and corresponding $Auth_{MME}$ before sending them to the group's leader($SM_{gl-i}$). These are:

$$LC_{MME} = f(ID_{MME}) \prod_{q=1}^{\frac{n}{m}} \frac{-TID_{SM_{i-q}}}{ID_{MME} - TID_{SM_{i-q}}} \times \bmod p \tag{4.15}$$

$$Auth_{MME} = (LC_{MME} \| r_{MME} \oplus GTK \| r_{HSS} \| ID_{MME}) \tag{4.16}$$

Upon receiving $Auth_{MME}$, and encrypted $KID_i$ the group leader broadcasts them to the rest of the group members.

7. Once the group members receive the values in (4.15) and (4.16) above, each in turn updates its $LC$ accordingly;

$$LC\_new_{SM_{i-j}} = LC_{SM_{i-j}} * \frac{-ID_{MME}}{TID_{SM_{i-j}} - ID_{MME}} \tag{4.17}$$

Each $SM$ further calculates its own, integrity and cipher keys $TGK$ using the received $r_{HSS}$ as follows:

$$TGK_{grp_i} = h_3(GK \| r_{HSS}) \tag{4.18}$$

$$IK'_{grp_{i-j}} = h_4(ID_{grp_i} \| r_{HSS}) K_{grp_{i-j}} \tag{4.19}$$

$$CK'_{grp_{i-j}} = h_5(ID_{grp_i} \| r_{HSS}) K_{grp_{i-j}} \tag{4.20}$$

$$K_{asme}^{'MTCD_{grpi}} = KDF(GTK_{grp-i} \| IK'_{grp_{i-j}} \| CK'_{grp_{i-j}} \| ID_{grp-i} \| IMSI_{grp_{i-j}}) \tag{4.21}$$

Each member further computes its response using (15) to (18) before furnishing it to the group leader.

$$XMAC_{SM'_{grp_{i-j}}} = h_1(ID_{grp-i} \| r_{HSS} \| IMSI_{grp_{i-j}})_{GTK_{grp-i}} \quad (4.22)$$

The group leader finally computes the group response.

$$XMAC_{grp-i} = h_1(XMAC_{MTCD_{grp1}} \oplus XMAC_{MTCD_{grp1-2}} \oplus \oplus,....XMAC_{MTCD_{grpn}})_{GRPK_1} \quad (4.23)$$

The response is sent back to the *MME* for final authentication.

*Faulty SM Unit Replacement*

During normal operation of the SG, it is possible for an already authenticated SM and forming a group, to malfunction and thus this necessitating its immediate replacing. Such a scenario constitutes a joining/exiting event from the already authenticated and validated group. Because the SM still retains the group's secret S in its flash memory, the rest of the group needs to update its current key so as to exclude the exited member(s) from continuing to retain the secret S. The new SM must also be prevented from knowing previous secret values S. This is because, otherwise if it is an intruder, it should be completely prevented from discovering and exploiting previous secret values S. Hence when a new SM joins, a new group key is recomputed as:

$$GK_i^{'} = h_3(GK \oplus \sec_{i-j}) \quad (4.24)$$

where $\sec_{i-j}$ is the secret value of the node to which the new SM is located. Likewise *HSS* generates a new value for $s$ as follows:

$$S_{new} = S + \delta S \quad (4.25)$$

where $\delta S$ is a random value of $s$ generated each time a member joins or exits.

Similarly, when an SM exits the group, a new group key is generated as follows:

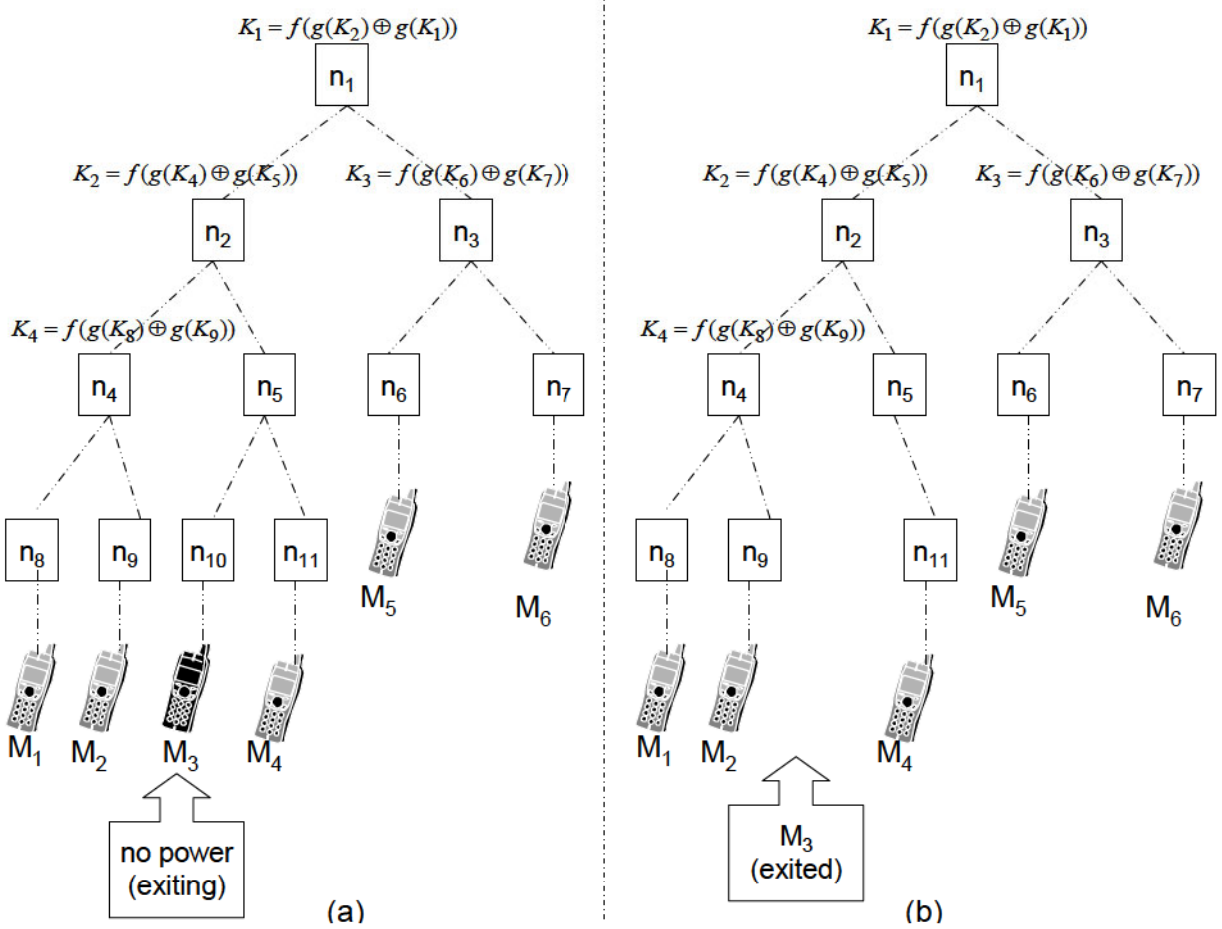


Figure 4-10: Units ( *SMs*) Joining or Exiting

$$GK_i^{''} = GK \oplus \sec_{i-j} \tag{4.26}$$

### 4.5.5 Data Access Control Using CP-ABE

Parties involved include HANs, BANs and data concentrators (DCs). As usual, HANs relay SM data to BANs.

A remote terminal unit (RTU) in turn sends the aggregated data to a gateway smart meter ( $GSM$ ) . This is illustrated in Figure 4.11.

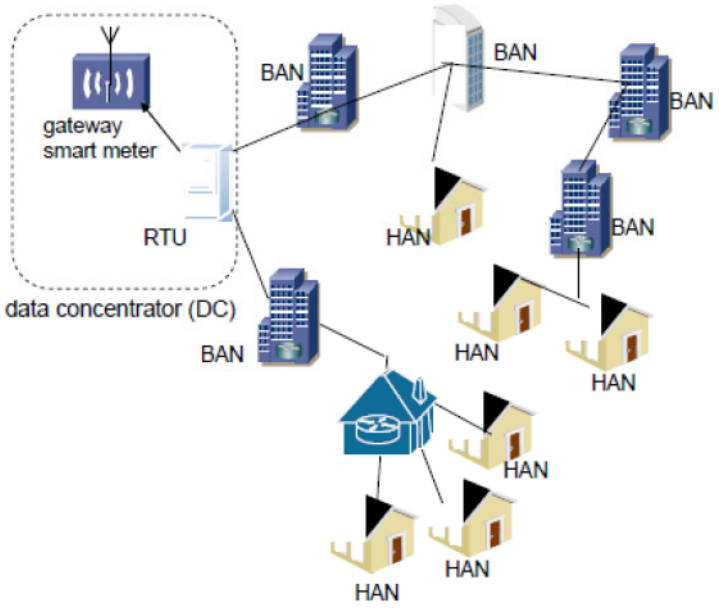


Figure 4-11: Data Aggregation

Further, illustrated is a distribution center (KDC) that distributes both private and public keys for encryption and decryption purposes [163], [164].

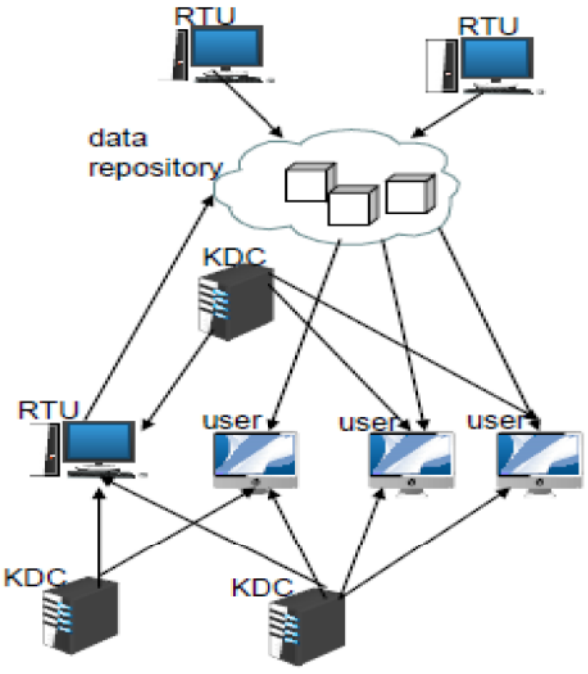


Figure 4-12: KDC Connected in a Distributed Fashion

A web of multiple interconnected KDCs is chosen since it enhances efficiency and reliability in the distribution of the keys is illustrated in Figure 4.12.

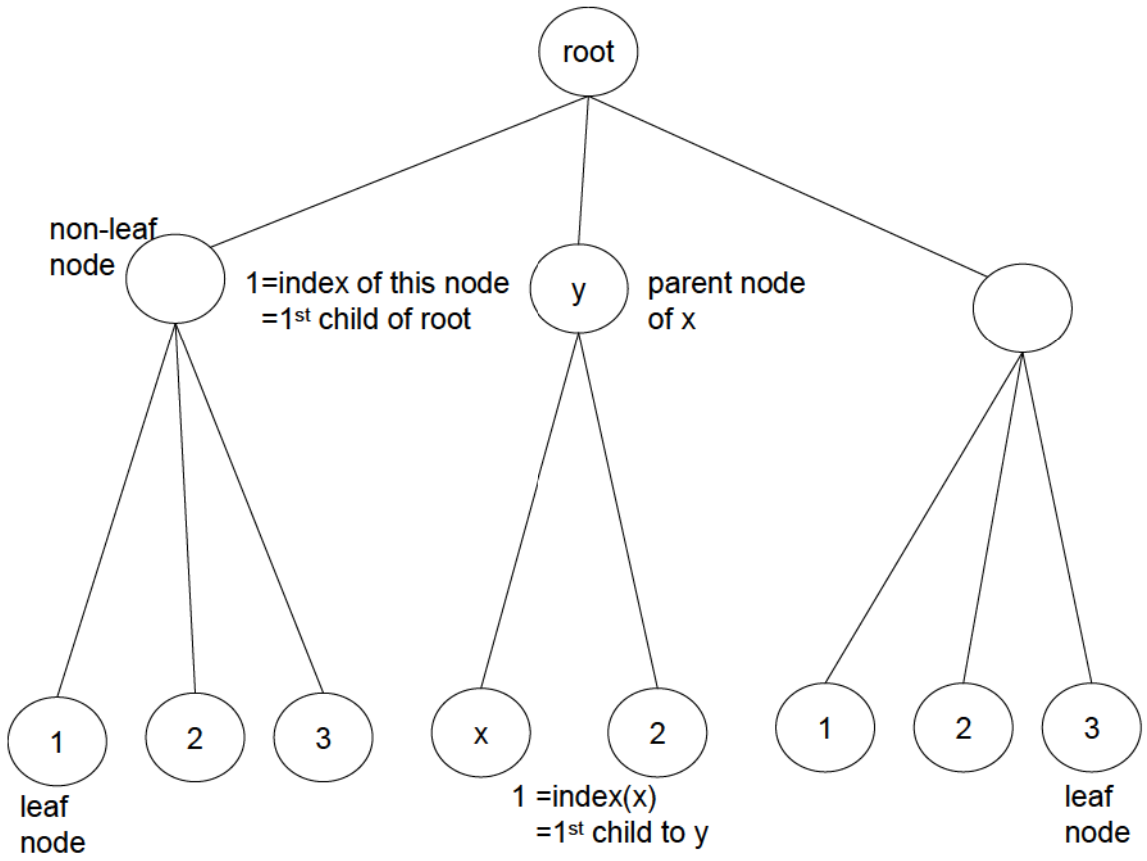


Figure 4-13: Tree Based Access Control Structure for CP-ABE.

With this scheme the ciphertext is encrypted using a set of attributes under a given access structure and thus a receiver will only be able to decrypt the information if it has a corresponding matching set of attributes. The approach relies on several *KDC* that are distributed throughout the *SG* in order to enhance its reliability. In short, the multi-KDC CP-ABE approach does not require trusted authority or any coordination between the KDCs. Furthermore it, generally will allow any type of monotonic access structure.

As such we assume that all the *SG* users (*SMs*) have some identifiable attributes. An example sample tree-based access structure for the considered CP-ABE targeted broadcast for an *SG* smart grid is shown in Figure 4.13. As illustrated, each non-leaf node represents a logic gate, and has a threshold. If its threshold equals one, it is an OR gate and alternatively if its threshold equals its children number, it is considered as an AND gate. On the other hand, each leaf node is considered as an attribute. All the nodes in the access tree are ordered by index numbers as demonstrated in the figure.

We first define a set of attributes as, $N:1,\ldots,n$ for some natural integer $n$. Next, we let $I$ represent the set of attributes that are needed for decryption. The scheme considers access structures that comprise a single AND logic gate whose inputs are literals, represented by $\wedge_{i\in I}\underline{i}$, where $\underline{i}$ is a literal (i.e. $i$ or $\neg i$).

*AUTHORITY SETUP & GENERATION*

- Select bilinear groups $G_1$ and $G_2$ of prime order $p$ with generator $g_1$ and $g_2$ respectively. A bilinear map $e: G_1 \times G_2 \to G_T$ is defined on them.
- Choose random exponents $y, t_1,\ldots t_{2n}$

The published key is:

$$PK = (e, g_1, g_2, Y, T_1, \ldots, T_{2n}) \tag{4.27}$$

Where;

$$Y = e(g_1, g_2)^y, \forall \in Z_{2n} : T_i = g_1^{t_i} \tag{4.28}$$

The master secret key is;

$$MK = (y, t_{1,\ldots,t_{2n}}) \tag{4.29}$$

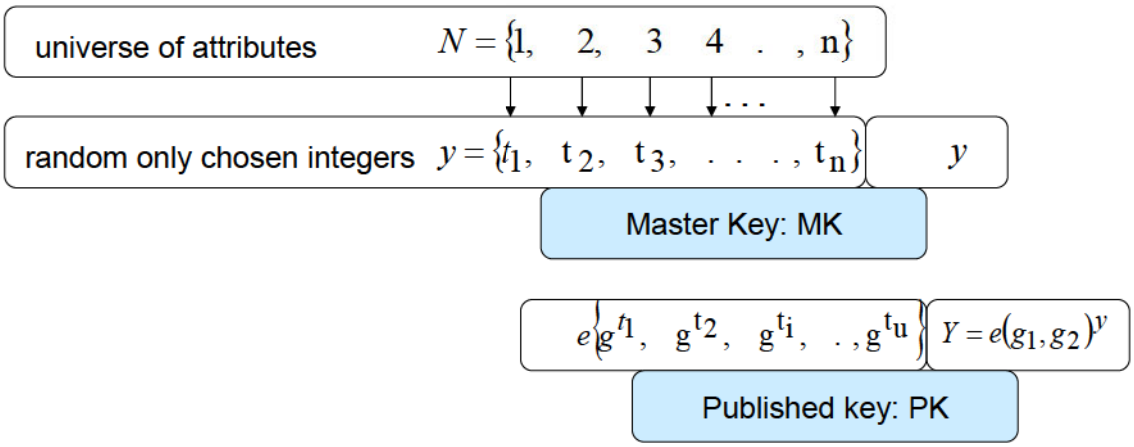


Figure 4-14: Master Key and Published Key Generation.

It is noted that at this phase the distributed KDCs are the sole attribute authority ($AA$) issuers of secret keys for attributes and are completely independent of each other. Consequently, recipients will be able to decipher the encrypted data from any given $SM$, provided they have obtained the necessary proper set of secret keys from the associated KDC (AA).

*ENCRYPTION*

Given a message $M \in G_T$ and an AND gate $W = \wedge_{i \in \underline{i}}$, the cyphertext is generated as;

$$CT = \left(\vec{C}, \bar{C}\{C_{i,0}, C_{i,1} | i \in N\}\right) \tag{4.30}$$

where,

$$\vec{C} = M.Y^S, \ \bar{C} = g^S \tag{4.31}$$

and $s$ is a random number in $Z_p$. Summarily for each $i \in I$, $C_{i,0}$ and $C_{i,1}$ are calculated as follows:

- If $\underline{i} = i, \ C_{i,0} = T_i^S, \ C_{i,1} = T_{n+i}^x$ (4.32)
- If $\underline{i} = -i, \ C_{i,0} = T_i^x, \ C_{i,1} = T_{n+i}^S$ (4.33)

In both cases $x$ is a random number in $Z_p$ and for each $i \notin I$, $C_{i,0} = T_i^S$, *and* $C_{i,1} = T_{n+i}^S$.

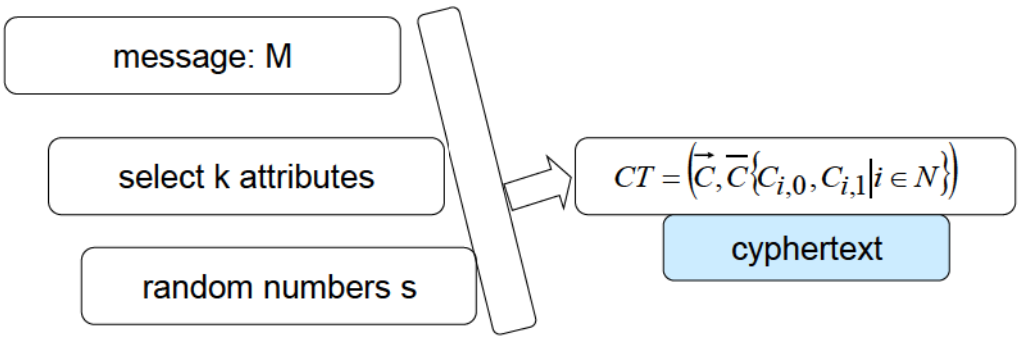


Figure 4-15: Message encryption.

Each $SM$ can relay ciphered (encrypted) data to the $DC$. This can be directly or via other relaying units. Since the data is encrypted using CP-ABE and the access structure also incorporated, there is no need for a further secure channel between the $SM$ and $DC$.

*KEY GENERATION*

In order to generate the decryption key, we let $S$ denote the input attribute set. For that, we assign every $i \notin S$ to be a negative attribute. Therefore, the secret key is defined as;

$$SK = \left(\vec{D}, \{D_i | i \in N\}\right) \tag{4.34}$$

where $\vec{D} = g_2^{y-r}$, $r = \sum_{i=1}^{n} r_i$, $r_i$ is a random selected from $Z_p$. For each $i \in N$, $D_i = g_2^{\frac{r_i}{t_i}}$ if $i \in S$; otherwise

$$D_i = g_2^{\frac{r_i}{t_{n+i}}} \tag{4.35}$$

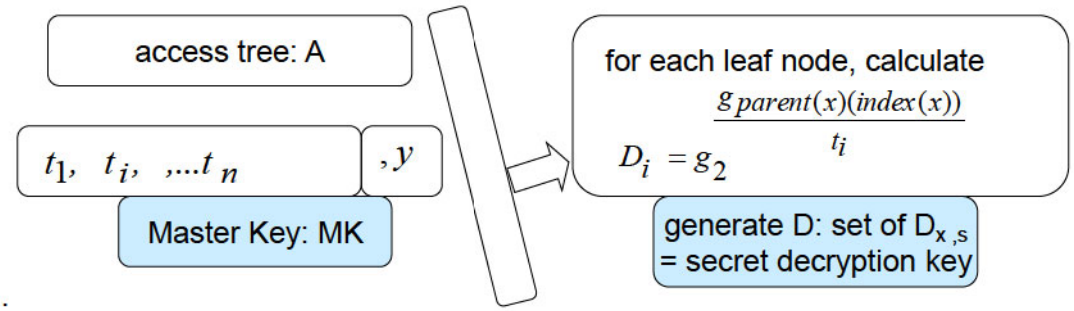


*Figure 4-16:* Key Generation.

*DECRYPTION*

We next show how decryption is accomplished. For that we assume that the input text is in the form;

$$CT = \left(\vec{C}, \overline{C}\{C_{i,0}, C_{i,1} | i \in N\}\right) \tag{4.36}$$

and we let

$$SK = \left(\vec{D}, \{D_i | i \in N\}\right) \tag{4.37}$$

For each $i \in N$, if the user's attributes is positive, then;

$$F_i = e(C_{i,0}, D_i) = e\left(g_1^{t_1 \cdot S}, g_2^{\frac{r_i}{t_i}} = (g_1, g_2)^{r_i \cdot s}\right) \tag{4.38}$$

However, if the user's attributes are negative, then

$$F_i = e(C_{i,1}, D_i) = e\left(g_1^{t_{n+i} \cdot S}, g_2^{\frac{r_i}{t_{n+i}}} = (g_1, g_2)^{r_i \cdot s}\right) \tag{4.39}$$

Finally decryption is accomplished as follows:

$$M = \frac{\vec{C}}{Y^S} = \frac{\vec{C}}{e\left(g_1, g_2\right)^{y.S}} \tag{4.40}$$

where

$$e(g_1, g_2)^{y.S} = e\left(g_1, g_2^{y-r}\right)^{r-S} . e(g_1, g_2)^{r.S} = e\left(\vec{C}, \vec{D}\right) \prod_{i=1}^{n} F_i \tag{4.41}$$

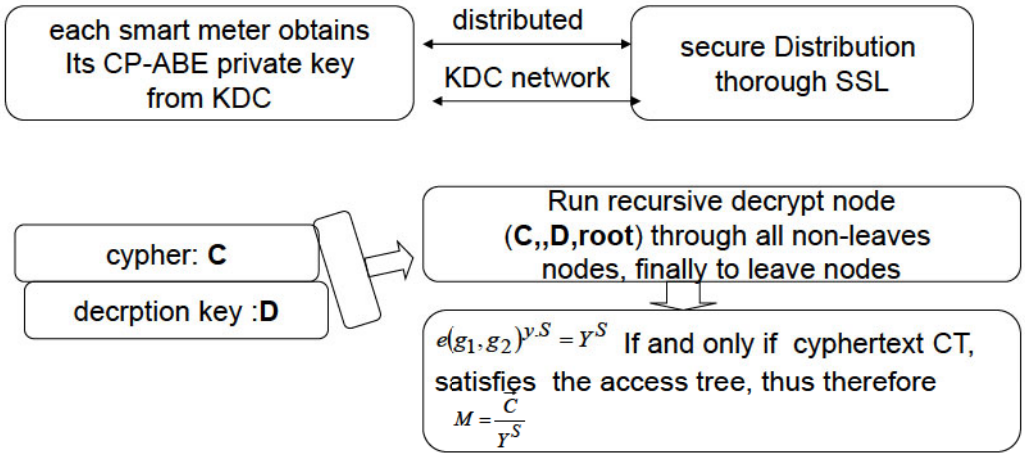


*Figure 4-17:* Key Distribution and Decryption in Smart Meters

The last three equations, demonstrate how an intended user can decipher the cyphertext. If the user is not the intended recipient, there is at least one attribute for which the user gets $F_i$ with the form $e(g_1,g_2)^{y_i \cdot x}$ such that he/she cannot compute $e(g_1,g_2)^{y_i \cdot x}$ .

### 4.5.6 Performance Analysis

Key performance indicators such as (1) signaling overhead (2) required transmission speed, (3) energy cost and (4) end to end latencies are the basis for evaluating any SG's Smart Metering based protocols. In this section, we carry out an analytical evaluation of the proposed framework in terms of such key metrics as well as general adherence to desirable privacy and security requirements.

#### 4.5.6.1 Overall Transmission Speed Requirements

The transmission speed requirements for the authentication and key agreement phase is directly related to the size (in bits) of the aggregate messages exchanged. We assume there are $m$ *SMs* groups, each of size $n$ , where $n \geq m$ . The *HSS* will always send a set of authentication vectors to *MME* for authentication of each group's members. The bit rate requirements in the *AMI* plus IoT network is:

$$R = \sum_{i=1}^{i=n} |message_i| = \sum bits(AMI - Network) \tag{4.42}$$

In evaluating the SM-AKA scheme we used the following parameters, whose values are provided in Table 4.2.

$ID_{gr-i}$ : - Smart Meter group's identity;

$SM - ID_i$ : -Identity of the $j^{th}$ *SM* device of the group;

$SN - Id$ : - Serving IoT network's identity;

$GK_{gr-i}$ : - Secret key shared between the $SM_i$ of the group and the $HSS$;

$K_{GMK}^{gr_{i-j}}$ : - Group Master Key shared between $SM_i$ and $SM_j$ of the group, $MME$ and the $HSS$;

$Ks_{i-j}^{grp-i}$ : - Secret key shared between the $SM$ group members;

$ERES$ : - Expected response;

$MAC$ : - Message Authentication Code sent by $SM_i$ to the $SM_j$;

$AUTN$ : - $Network$ authentication token generated by the HSS;

$RAND$ : - Random number generated by the entity $i$;

Table 4.2: Evaluation Parameters

| parameter | length(bytes) | parameter | length(bytes) |
|---|---|---|---|
| $SM-ID$ | 16 | $Ks_{i-j}^{grp-i}$ | 16 |
| $SN-Id$ | 6 | $TS$ | 4 |
| $ID_{gr-i}$ | 16 | $ERES$ | 4 |
| $GK_{gr-i}$ | 16 | $AUTN$ | 16 |
| $K_{gr-i}$ | 16 | $RAND$ | 16 |
| $K_{GMK}^{gr_{i-j}}$ | 32 | $MAC$ | 8 |

Overall our proposed scheme accomplishes the initial access authentication among the group members by communicating a total of seven messages among between the group leader ($SM_{gl-i}$) on behalf of all group members, $MME$ and $HSS$. The required bit rate is therefore approximated as follows:

$$R_{SM-AKA}=\sum_{i=1}^{i=7}\left|message_i\right|=544n+1264m \ \ bits \tag{4.43}$$

In our analysis of the transmission speed requirements we will compare the scheme with two other similar protocols which are:

The Choi's scheme [19], which requires the exchanging of a total of nine messages between the group's leader ($SM_{gl-i}$), $MME$ as well as $HSS$ in order to accomplish the access authentication. In this case the aggregate number of bits exchanged is computed from;

$$R_{choi}=\sum_{i=1}^{9}\left|mesage_i\right|=1200n+1408m \ \ \text{bits} \tag{4.44}$$

The scheme proposed in [20] employs a two-phase approach in establishing access authentication. In the first phase the group leader ($SM_{gl-i}$) is authenticated in a process that involves the exchange of five messages.

$$R_{phaseI} = \sum_{i=1}^{i=5} |message_i| = 2300 \ bits \tag{4.45}$$

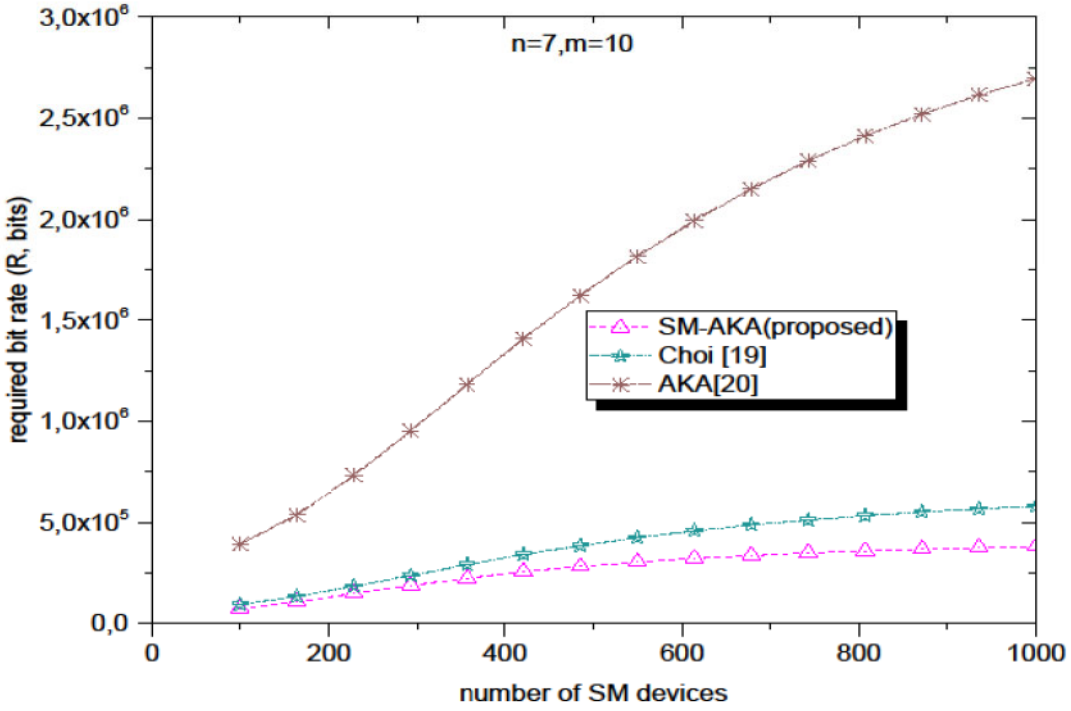


Figure 4-18: Required Bit Rates as a Function of the Number of SM Devices

Phase two completes the entire group's authentication by communicating three messages.

$$R_{phaseII} = \sum_{i=1}^{i=3} |message_i| = 1150 \ bits \tag{4.46}$$

Hence the number of bits exchanged for the scheme is;

$$R_{MTC-AKA} = 1150n + 1152m \ bits \tag{4.47}$$

A plot of the required speeds in bit rate terms is provided in Figure 4.18. The corresponding bandwidth requirement would be twice the bit rate in terms of the Nyquist criteria. As can be note both the proposed SM- AKA and Choi schemes require minimal bandwidth even when the number of Smart meter devices is increased significantly. The AKA scheme in [20]'s bandwidth requirement almost exponentially increases as the number of devices start to increase above 200. The same trends are observed when the number of groups are increased as can be seen in Figure 4.19.

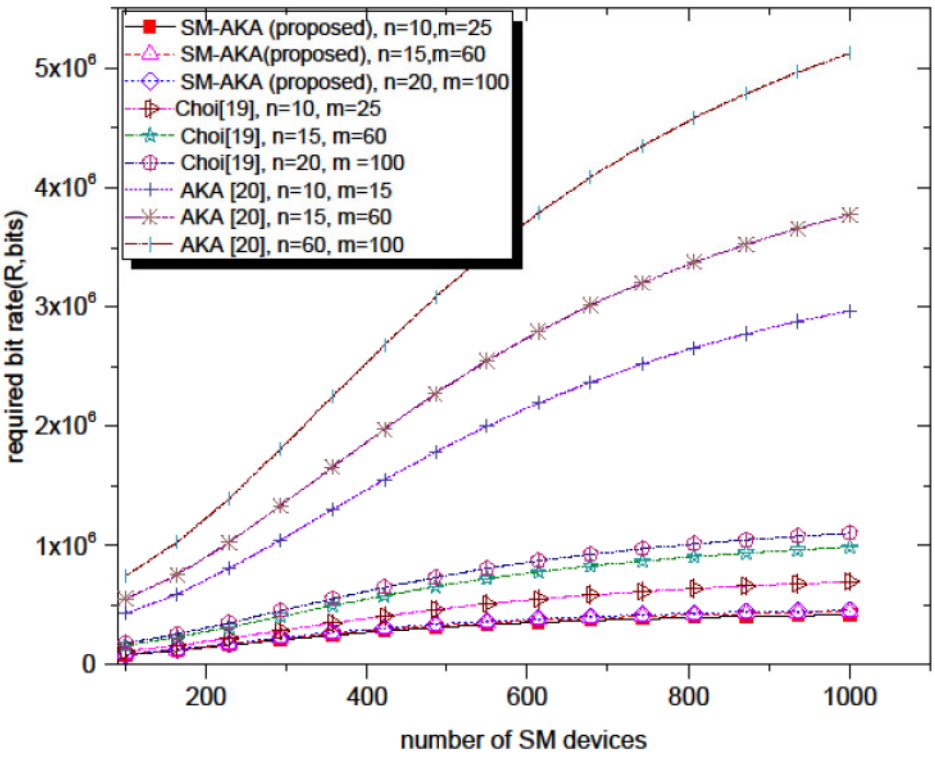


Figure 4-19: Required Transmission Speeds as a Function of the Number of SM and Number of Groups

#### 4.5.6.2 Signaling Overheads

With regards to signaling overheads of the proposed scheme, we will assume once again that each group comprises $n$, $SM$ devices and all in total we have $m$ groups in the $SG$.

Choi's Scheme presented in [19] requires $3n$ authentication messages to be exchanged between the $HSS$ and $MME$, as well as an additional $3m$ messages to be communicated the group's leader and the $MME$ hence all in total $3(n+m)$ overhead messages are exchanged.

The AKA scheme [20] will require a total of $3n+2m$ message exchanges for both the first and second phases of access authentication. Our proposed SM-AKA scheme as discussed before will require a total of $3m+2n$ message exchanges between the group, $MME$ and the $HSS$. throughout the access authentication phase.

Figure 4.20 plots the average signaling overhead volumes generated by the SM-AKA, Choi and AKA schemes.

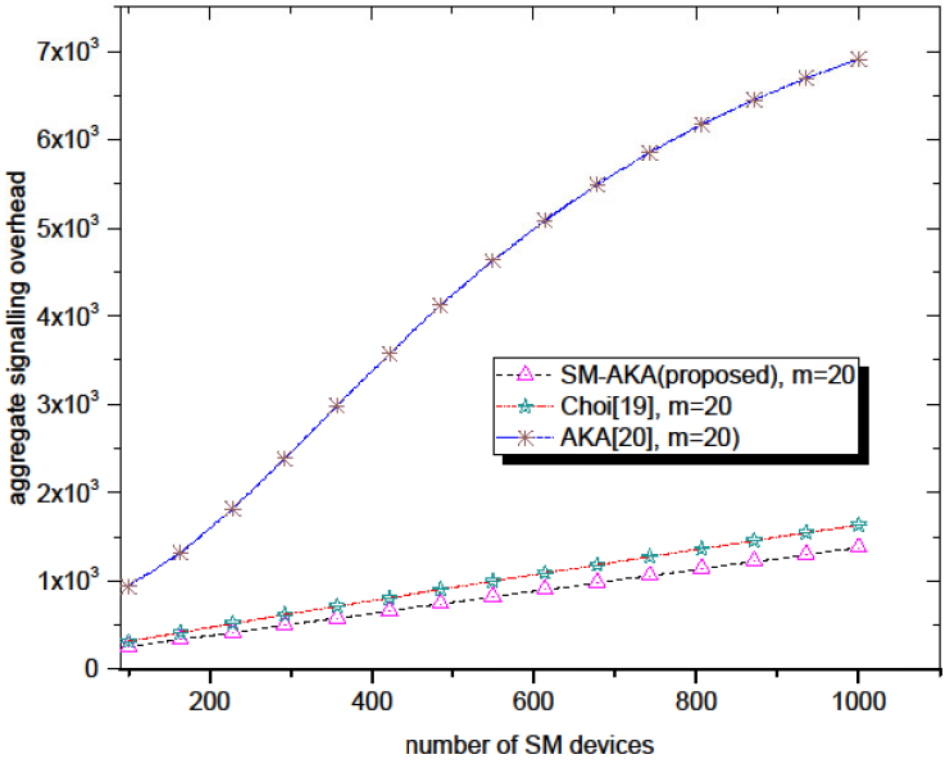


Figure 4-20: Signaling Overhead in the Network

Once again it is observed that the SM-AKA followed by the Choi schemes generate relatively much lower signaling overheads. The signaling overheads however, tend to increase in proportion to the number of devices incorporated in each group.

#### 4.5.6.1 Energy Costs

A brief analysis of the energy cost of the three schemes is provided next. In this case we are assuming that there are $n$ - $SMs$ that form a total of $m$ groups. We can analyze the energy costs as being directly related to the energy efficiency of each protocol. We assume the total energy cost in transmitting a single data packet between $SM$ and the $HSS$ to be equaling a single unit. Likewise the energy cost of transmitting the same packet between the $HSS$ and $MME$ is $c$, and that between the $MME$ and $DC$ is $b$.

We assume that the $SMs$ / $DC$ are further away from the $MME$ such that $c/a$ does not exceed $b/c$. From [166], the energy costs for each of the schemes is given as follows:

$$E_{SM-AKA} = 2bn + m(3a - 2b + 2c) \tag{4.48}$$

$$E_{Choi} = 2bn + m(4a - 2b + c) \tag{4.49}$$

$$E_{AKA[20]} = n(4a + 2c) \tag{4.50}$$

In the above three equations, $a$ denotes sets of the authentication vectors to $MME$ for the successful authentication of a single $SM$ device. A simple comparative analysis of the last three equations clearly shows that the proposed $SM - AKA$ scheme is more energy efficient.

#### 4.5.6.1 Overall end-to -end Latencies

In the proposed security framework, the privacy of the data is ensured by way of using $DH$ keys which are themselves exchanged in encrypted form. Signatures are also used to further enhance information exchanges from the root to leaves, while data is authenticated hashes on a hop by hop basis.

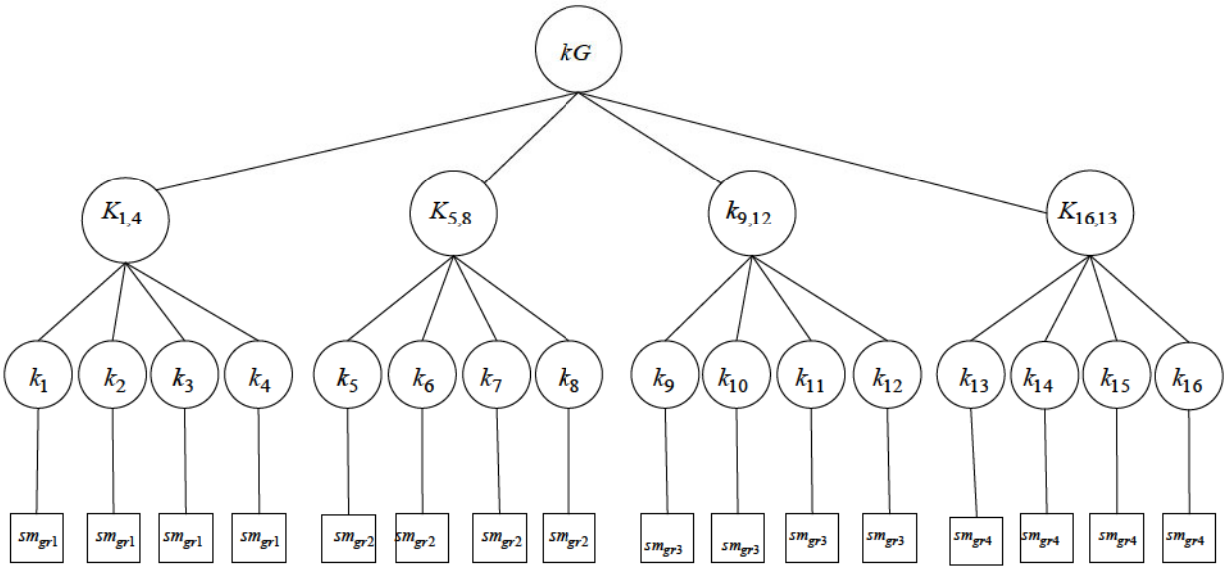


Figure 4-21: Multilevel (4) key Tree for Group Formation During Data Collection

In this part, we present the performance evaluation obtained in the security of D2D group device communications implementation. The general level of security requirements for the proposed framework is to prevent any forms of malicious attacks as well as guarantee several security requirements. Examples of such requirements include integrity and protection, privacy in group communication (GK), anonymity in GK, non-repudiation as well as identity disclosure.

As per the proposed hierarchical architecture and aggregation is performed by group leader, the size of groups is 4 *SMs* a single group. One of them is designated as a group leader and aggregates the messages/signals from the other three.

Table 4.3: Computational Parameters (SM side)

| Operation | Duration (ms)) |
|---|---|
| ciphering | 0.2 |
| decyphering | 5 |
| digital signature | 5 |
| hashing (h) | 0.04 |
| pairing | 40 |
| point multiplication | 1.5 |

The protocol's execution time is tested using the GUROBI Solver tool.

Table 4.4: Computational Parameters (core network)

| Operation | Duration (ms)) |
|---|---|
| digital signature | 5 |
| hashing (h) | 0.02 |
| pairing | 20.1 |
| point multiplication | 0.5 |
| LC calculation | 0.5 |

For the analysis of the transmission delay incurred in the proposed approach, the delay time only for the following operations is considered including the hash function.

$$T_{SM-AKA} = n(7T_{hash} + 4T_{AES} + 2T_{xor}) + m(2T_{hash} + T_{rand}) \quad (4.51)$$

$$T_{choi} = n(6T_{hash}2T_{\mathbf{mod}} + 2T_{AES} + T_{xor}) + . \\ .. + m(4 * T_{hash} + 2T_{rand} + T_{xor}) \quad (4.52)$$

$$T_{AKLA[20]} = n(4T_{hash} + T_{xor} + T_{rand} + k(6T_{hash} + T_{xor})) \quad (4.53)$$

The execution time more less increases linearly with increase in the number of *SM* devices in the group for all the schemes.

### 4.5.7 Overall Security Analysis

In this section we provide a general security analysis of the SM-AKA protocol. We rely on the Automated Validation of Internet Security Protocols and Applications (AVISPA) which was solely developed as a platform for the validation of security-sensitive protocols, will be relied

upon in this work [125]. The objective is to formalize protocols by automatically validating them and detecting errors.

*Smart Meter Device's Location/End User Privacy:* At the registration phase, the SM device as well as the end User's identities are each mapped to a pseudonym ID ($PID_i$) and thereafter the latter is used for authentication purposes rather than the real names/IDs. In this the identities and locations of both SM device and that of the end Users are concealed hence privacy is guaranteed.

*Mutual authentication:* The SM-AKA protocol provides robust mutual authentications between $BC\_HSS$, as well as among the individual $SM$ devices in a group. $HSS$ authenticates the $BC$ by way of verifying $MAC$ values computed using the BC's credentials such as $RID$ and $PID$. To authenticate HSS, the $BC$ checks the received $MAC''$ from the $MME$ and if they both match with the $XMAC'$, then both $MME$ and $HSS$ are authenticated.

Similarly, $HSS$ verifies and authenticates the $SM$ group by verifying their Lagrange components. Each member then uses these Lagrange components to compute the secret $s$ and compares it with the same value that was sent from the $KGC$.

*Backward /Forward Key Secrecy:* With the SM-AKA protocol the group key ($GK$) is updated and changed each time a device leaves or joins the group. When a device joins the group, $HSS$ is compelled to broadcast its secret node, thus a new $GK$ is computed.

Similarly, when a device exits, the remaining devices are compelled to update their $GK$.

*Attack resistivity:* The channel between the Billing Center and $SM$ group is open to various attacks. To safeguard against replay attacks, time-stamped key hint messages are periodically exchanged between the two parties. A hacker who successfully intercepts the key hints exchange will not be able to replay a message for the next key hint exchange message because of the time stamping.

*MiTM attack:* The channel between the $MME$ and $HSS$ is assumed to be secure (in terms of integrity, confidentiality, and entity authentication), and only the channel between individual $SM$ devices and $MME$ may be vulnerable to MiTM attacks.

## 4.6 Chapter Summary

The chapter reviewed cyber-physical security and the actions of adversaries towards compromising general security in SGs. The chapter adopts a balanced theoretic balanced analysis, thus in the process aiming to holistically and objectively present the base, inner working principles of the attacks. Notably in the same chapter, we have outlined various known attacks and possible intended out-

comes. These intended outcomes include disruption of normal operation of the SG and this ultimately has a huge economic impact. In the same chapter, we propose a secure and scalable framework for ensuring privacy and security in the *SG* IoT compatible communication architecture that provides interconnectivity to multiple authorities, as well as devices and elements which are part of the *SG* system. The framework's objective is to provide both security and privacy.

# 5. Towards Security and Privacy Guarantees in Future Generation Smart Grids

## 5.1 Introduction

The chapter devotes mainly towards addressing security and privacy guarantees for the various would-be services and applications, in future SGs in the advert of existing and future public networks such as IoT and related technologies. We also take cognizance of the fact that an SG architecture cognizance that power grid architectures are always influenced by the physical location of generation sources., whereas legacy electrical power grids always depended on mega-generation sites located remotely, modern and future SG infrastructural architectures will be significantly influenced by the multitudes of DERs with mostly relatively smaller generating capacities.

Overall, the ever-increasing numbers of objects and sensors incorporated into an SG architecture to realize the smartness bring about security vulnerability threats for the same devices and in a way partially the cause for slowing down the evolution of power grids. The threats are not only restricted to the objects and sensors but the services and applications as well. Mitigating these vulnerability threats will enhance future generation SGs'aims and objectives, viz efficiency and reliability as far as energy management is concerned. It is also necessary to highlight the need to explore, machine learning techniques, especially in SG energy management modeling aspects. The same applies to the incorporation of software-defined networking (SDN) approaches towards enhancing the control capabilities of the underlying ICT infrastructure platform as the latter is key to the success of future generation SGs. In particular security vulnerabilities can easily be detected in any part of the network within desirable real-time scales only if the network's control infrastructure is both robust and resilient enough. In particular, we pay attention to the potential use of IoT as the underlying ICT platform. The fact that it (IoT) is mostly wirelessly dominated, only adds more security vulnerability threats. In subsequent subsections, we overview, architectural, ICT infrastructures as well as proposing cyber security and private schemes for envisaged next-generation SGs.

## 5.2 Architectures

In this subsection, we summarily define an SG architecture concerning security and privacy

As was alluded to earlier, future SG architectures will interconnect multitudes of sensors, objects, and other supporting entities and systems. Typical such entities will include frequency sensors and

SMs. Key to its operations will be relaying the acquired data to dedicated processing points for further processing and appropriate action being taken from inferences generated [167].

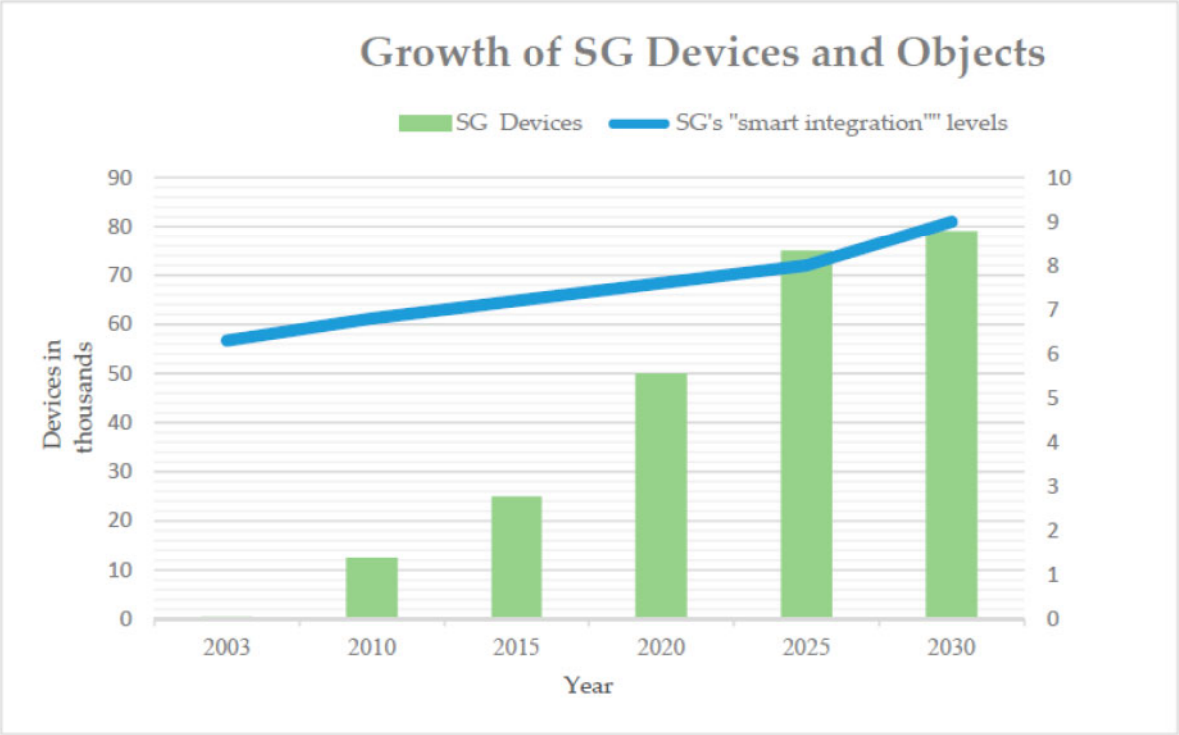


Figure 5-1: Proliferation of Objects and Devices in SGs

In the future end customers will be allowed to regulate their consumption behaviours as well as trading. Typically, energy will be stored during non-peak hours and then be released to support the grid during peak hours. The storage systems range from ESSs located conveniently across the SG and EVs that support V-2-G.

Abstractly, overall, future SG infrastructures will cluster together so many entities as illustrated in Figure 5.2, thus leading to elevated security vulnerabilities and threats. This necessitates them being addressed concurrently with the base SG power system infrastructure design trends. The problem will be even compounded by the fact that future SGs will be interconnected forming a seamless power supply system across the globe. The danger is that some utility operators will be able to enforce more effective security and privacy protection measures. In such scenarios, attackers (adversaries) will always use the weaker (compromised) section of the interconnected grids for infiltration. Generally, attack points of future SGs will include routing protocols, end-user data, control centers, and their databases, SMs, and sensors.

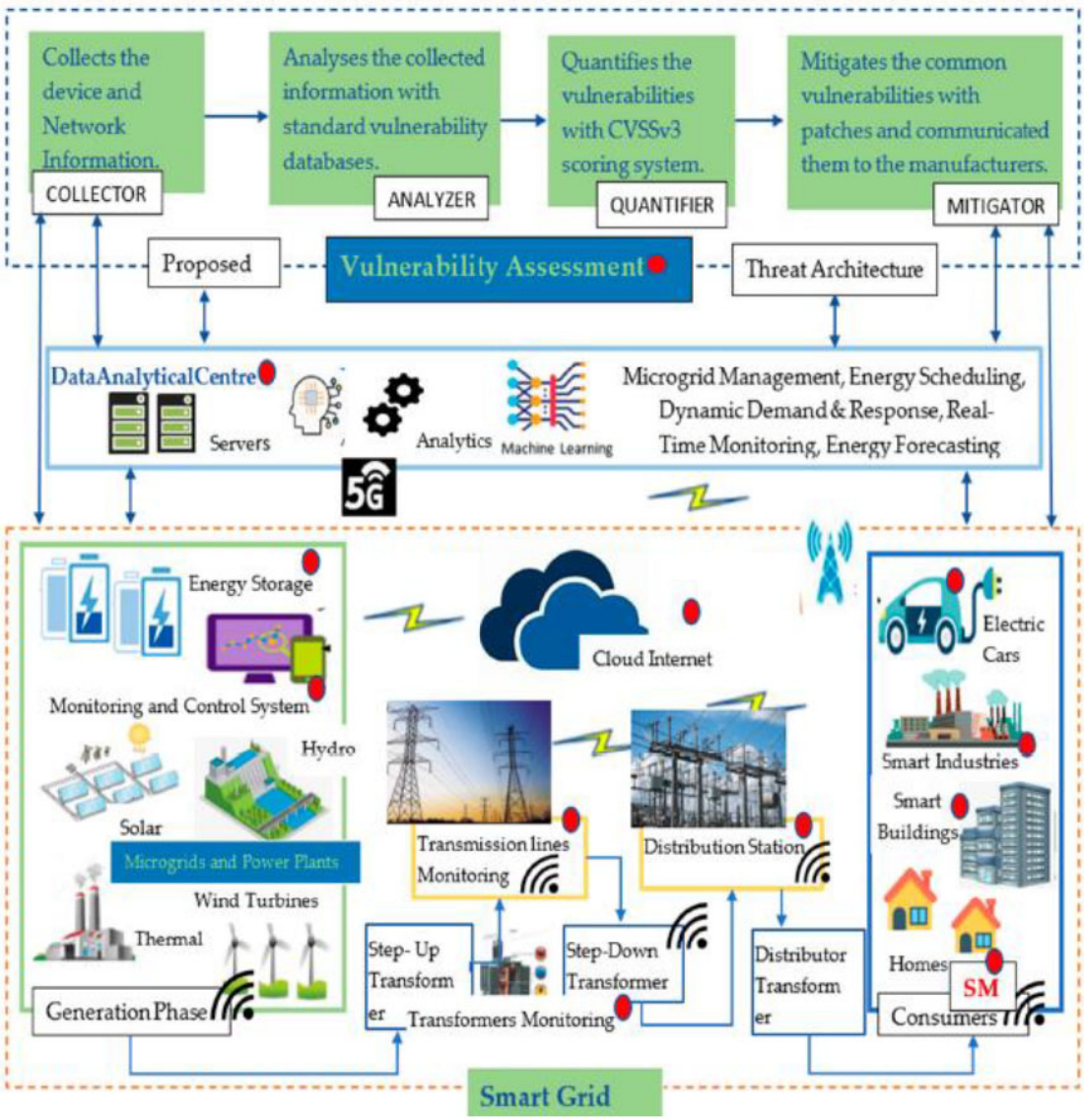


*Figure 5-2:* SG Vulnerabilities

Key highlights in this regard include, [168]:

- The routing protocols are being deliberately attacked to cause traffic jamming or buffer overflows in targeted sections of the network or endpoints (such as servers). Typical such examples would be interfering with the Inter-Control Center Communications Protocol (ICCP), such that it starts looping and in the process causing jamming and buffer over-flows.
- By nature, the key objects and devices are deployed in unprotected environments and thus prone to attack (physical damage) at any time.

- At software levels, key devices and sensors that require malware updating can easily be attacked, and in the process, adversaries gain their control.
- The privacy of end-users can easily be compromised in terms of behavioral tendencies. This is possible after gaining access to the SM's data trends.

As alluded to in various works of literature, an SG will be more reliable as well as efficient in its objectives by way of integrating the threat architecture and security vulnerability module with the power system supply architecture. The vulnerability assessment will always acquire necessary vital information about the device and network security and feed it to an analyzer. The latter, compares the received information with vulnerability databases, before making necessary vital inferences regarding threats. Such an approach has overwhelming advantages such as:

- Enhanced privacy of SM's data and the duplex connectivity between utility providers and end-users, thus precluding any data leakages.
- Eradication of any possible security lapses such as open ports, and hardcoded/weak passwords assists in lowering security compromises for key SG entities and nodes.
- Prevention of possible malfunctioning of the SG that might even lead to a grinding halt.
- The vendors or proprietors of the various components incorporated in the SG will constantly be updated with any vulnerabilities and their severity, and in the process, they will accordingly improve their embedded security for new devices.
- Vulnerabilities of the SG system are identified well in advance and ultimately removed before their actual exploitation by adversaries.

We thus in the next section will briefly focus on the communication subsystem.

### 5.3 Communication Subsystem

As the ICT subsystem is a key component that provides connectivity to all other entities in an SG, it must efficiently accomplish the following tasks:

- *Acquisition*: It should be able to facilitate the acquisition of data such as real-time power flow measurements, transmission line voltages and frequencies, state of circuit breakers e.tc, and relay such information to key processing centers.
- *Processing*: Use acquired data to regulate the states of the power system.

- *Implementation*: Timeous reaction to any required action. E.g., should be able to activate circuit breakers in affected sections of the SG
- *Communication:* Should be able to enable the necessary interactions among key grid entities by facilitating the communications medium, its availability, as well as reliability, is thus crucial [168].

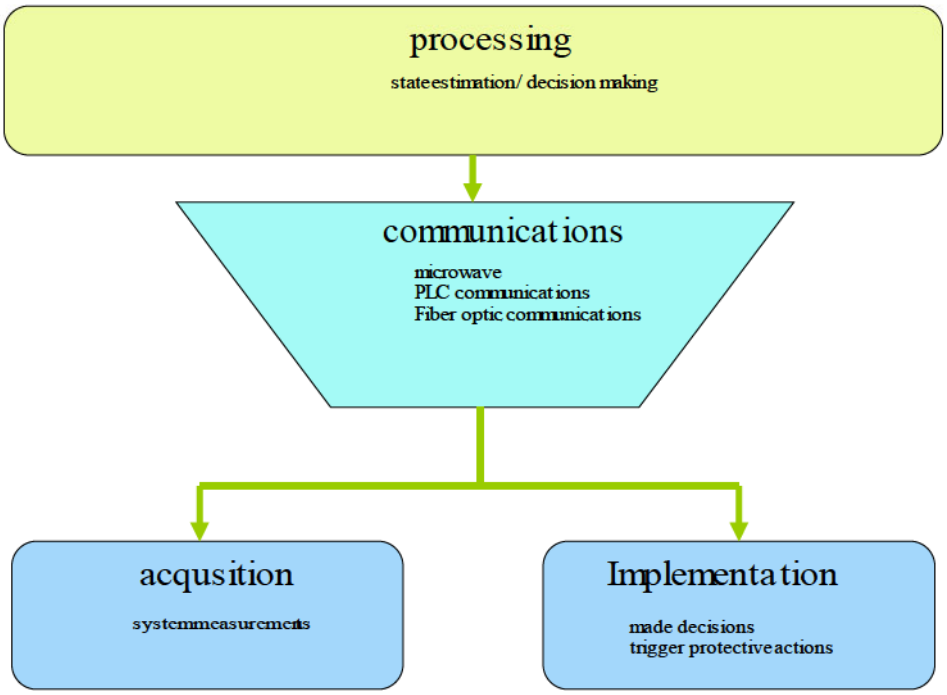


Figure 5-3: Key ICT Subsystem Categories

A logical architecture of an effective power system's ICT subsystem is illustrated by Figure 5.4 in which, the key commands related to actuation and measurements are either acquired from sensors or directly from elements and devices (A). Transmission is on the provided links (B). An illustration of how information is relayed among substations is also illustrated in the same Figure (D). Finally, item F shows how inter-control center communication across the available WAN is accomplished [170].

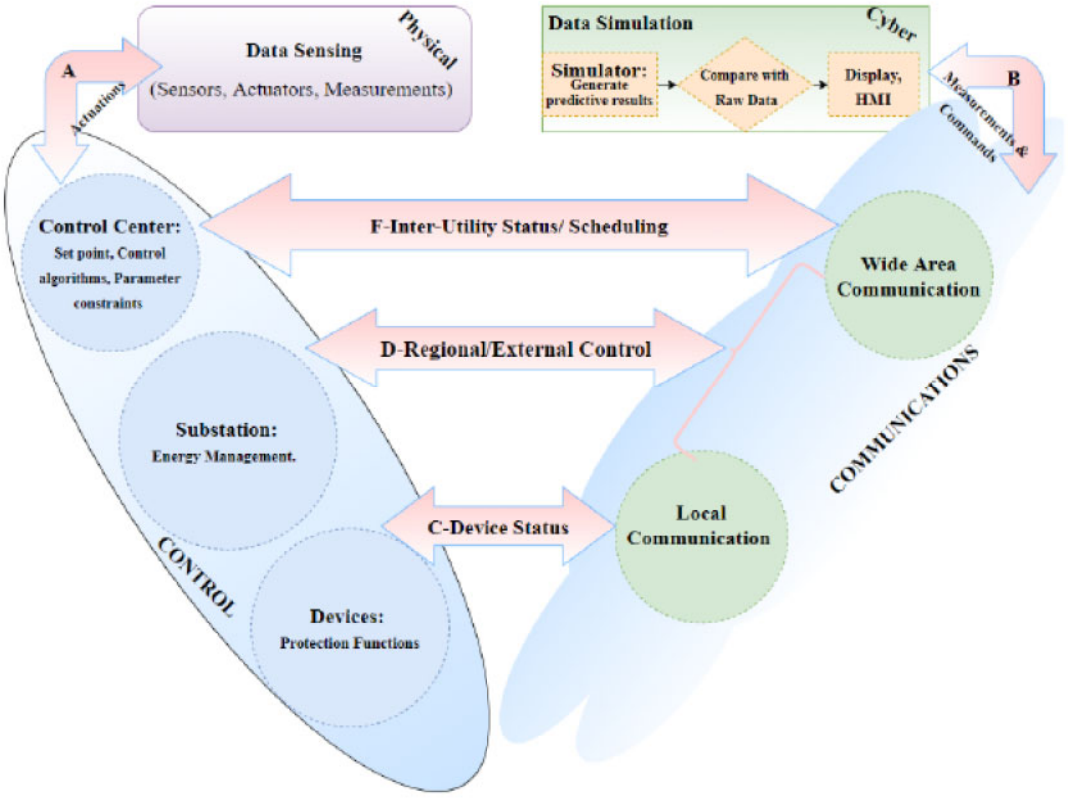


*Figure 5-4:* Key Logical Infrastructure

An enabling ICT infrastructure will suffice the security requirements such as:

- Authentication: all devices and elements constituting both the ICT and SG infrastructures should be able to support moderate or lightweight authentication methods. This is because most of them are constrained in both power and processing resources. Scalability is also necessary.
- Privacy: End users' privacy should be preserved over the communication links and paths.
- Availability: reliability and robustness of network connectivity for all connected elements of the SG must be ensured.
- Confidentiality: The communication protocols must provide secure procedures of authentication and data handling to ensure privacy
- Integrity: Data integrity must be protected at all times.

The various security threats and vulnerabilities can be modelled in various ways. Example of such modelling is provided in Figure 5.5. As discussed in earlier chapters, various security attacks such as spoofing, device tampering, repudiation, DoS and information disclosure are common.

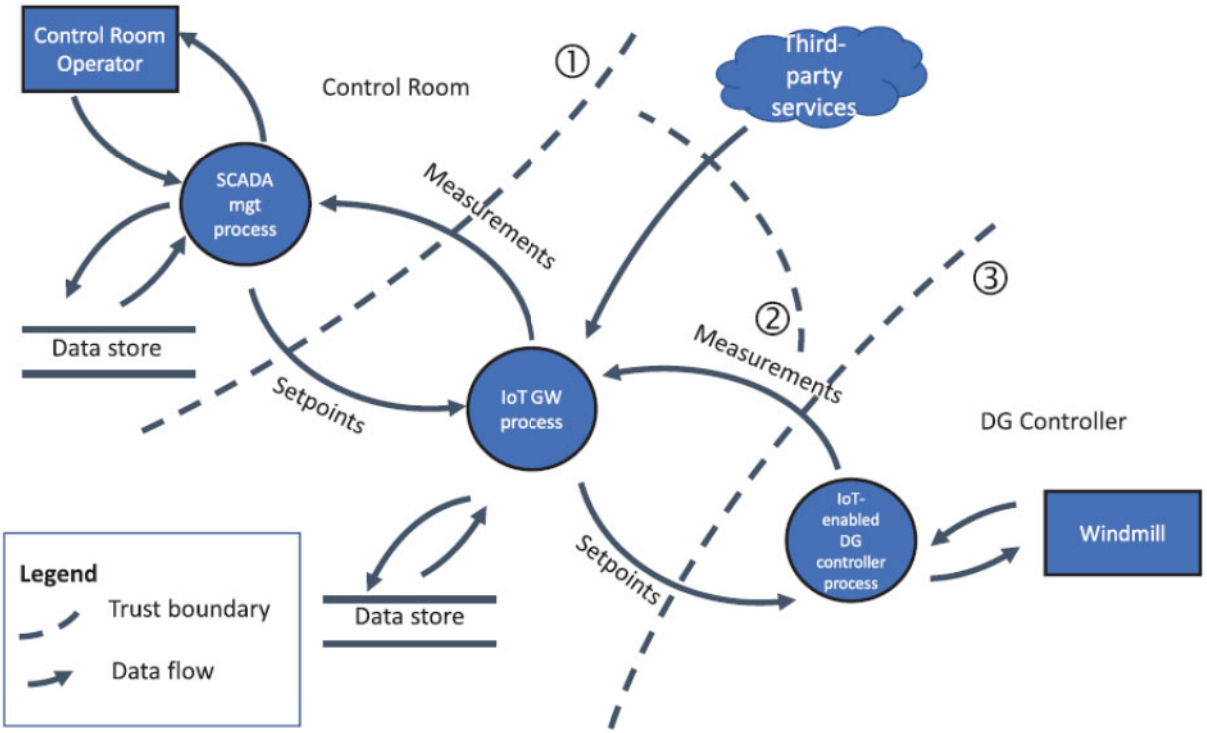


Figure 5-5: Data Flow Diagram for the Reactive Power Use Case

Three trust zones (boundaries) can be identified in this illustrated model namely between the control rooms and IoT Gateways, assuming we have advocated for an existing public ICT infrastructure such as IoT. This zone is marked as 1. Similarly, we can identify a second (2) trust zone, being between IoT Gateways and "Third-party services" as well as between IoT Gateways and DG controllers. The third and last trust zone would be between available cloud services, vendors, and other IoT Gateways [171].

## 5.4 Security and Privacy Framework

In this section, we describe a security and privacy framework for SGs. The framework is based on the Fog-Computing paradigm [172], [173]. It also rather uses a public network infrastructure, namely IoT, and thus will also take advantage of the use of new 5G network technologies such as D2D communication. In proposing such a framework, we are also taking into consideration current cyber security trends: We summarily list these trends as follows:

- The SG cyber-attack surface has expanded thus necessitating data security automation.
- An adoption of multi-layered as well as multi-factor authentication to enhance privacy. The adoption of new cybersecurity technology stack trends. This trend in development has means the cybersecurity technology stack gives guidance on the architecture framework needed to secure both privacy and security.
- Some SG elements and devices are mobile and hence this necessitates mobile software security enhancements.
- Periodic cybersecurity awareness training will ensure that both manufacturers and utility operators operate at the same pace and direction in combating security threats and vulnerabilities in modern SGs [174], [175].

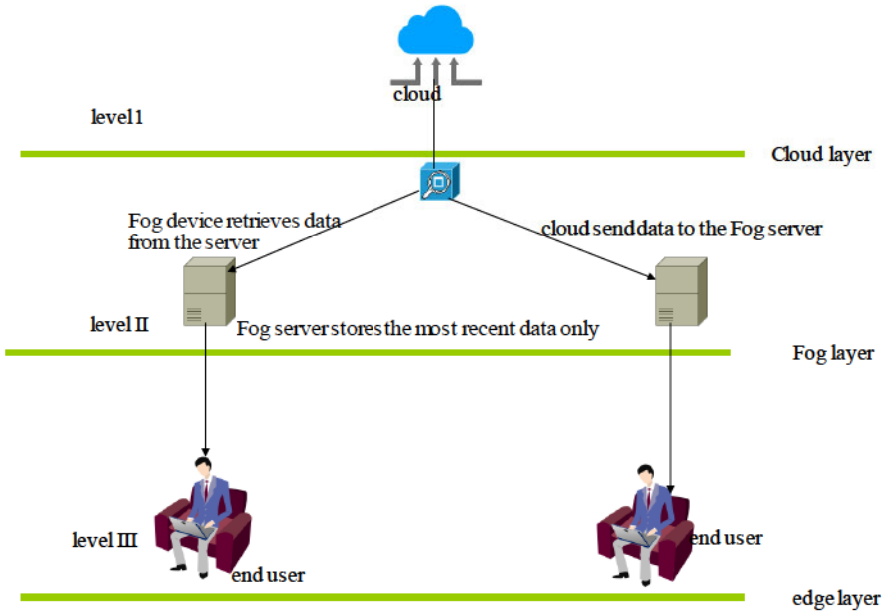


Figure 5-6: Typical cloud-fog Computing Architecture

Illustrated in Figure 5.6 is a Fog-Computing paradigm. The key entities would be the smart grid objects and sensors, Fog servers deployed within the vicinity of the clustered objects, devices, and elements constituting the SG. Finally, we have a centralized cloud server. The Fog layer is necessary to improve on round trip response times for some of the SG's services and applications. Overall, the proposed approach (i.e., Fog-cloud paradigm) approach has taken into consideration of the resources-constrained nature of some of the elements, devices, and objects constituting the SG infrastructure. To provide privacy as well as security in surveillance secure, secure authentication

and key exchange among the D2D communication compliant SG devices, elements, and objects. We make an overall assumption that the 5G network has evolved sufficiently enough At the SG base level, we will assume that all SG-associated devices, elements, and entities are under the coverage of 3GPP IoT-enabled network architecture as illustrated by in Figure 5.7.

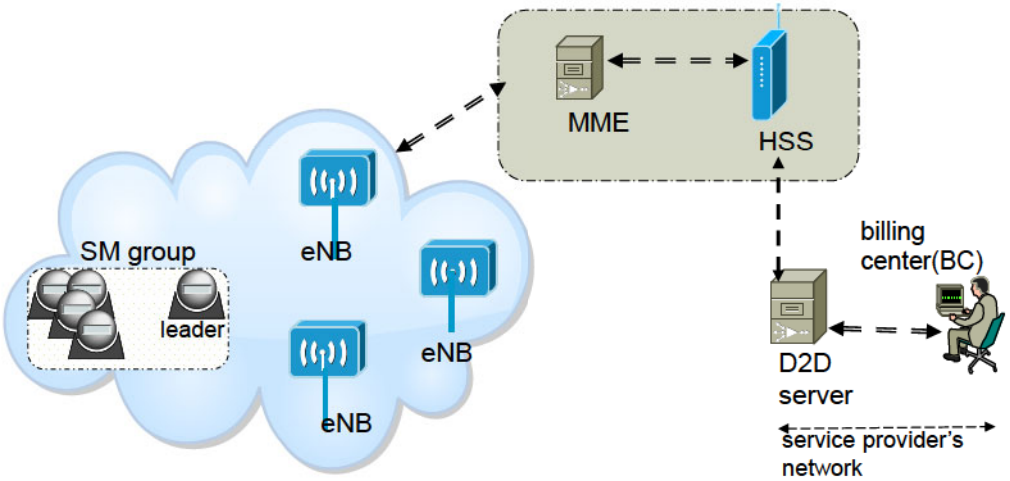


Figure 5-7: 3GPP Coverage in an IoT Network

By default, attributes information of the various elements, devices and objects are retained by the HSS. It also relies on the MME to verify each unit by way of granting a set of authentication tokens.

Our model framework will focus on both security and privacy preservations in the SG. Hence three components of the framework providing for data security, data aggregation, and privacy authentications will together provide complete security in the SG. We discuss and evaluate each of these in the next three sections.

### 5.4.1 A D2D Lightweight Customer Side Data Aggregation Scheme

The scheme takes into cognizance the fact that some of the elements involved are resource-constrained hence a lightweight form approach is chosen. In that way-SG messages will be delivered with absolute security guarantees, at low computational complexities and loads since most of the devices are constrained in terms of both power and computational memory.

#### 5.4.1.1 `Preamble

We commence the section, by initially defining a few parameters as follows:

$N$ – the number of plaintext vectors.

$r$ – a value characterizing the ring of vectors.

$l$ – the total number of operations.

$n$ – non-hard disturbed matrices of a public key

Next, we generate $l_o = n \times N \times \varepsilon_{\max} + (N-1) \times r$, $q = 2 \times l_o \times (2l+1)$, subject to $p = q \times r \times \varepsilon$ being prime and $\varepsilon < l_o$.

We further generate two matrices $\mathbf{A}$ and $\mathbf{B}$ of size $N * N$ over $GF(p)$ such that $\mathbf{M} = [\mathbf{A}|\mathbf{B}]$. This is followed by defining a scrambler matrix $\Delta$ of size $N * N$ over the same $GF(p)$.

By generating a noise matrix $\mathbf{D}_i$ for $i \in 1,2,...n$, we can subsequently compute a distributed matrix

$$M_i = [A_o | B_i + D_i \Delta] \tag{5.1}$$

Like wise we can compute a hard noise matrix;

$$M_o = [A_o | B_o + D_o \Delta] \tag{5.2}$$

By selecting a permutation $P(.)$, we can compute;

$$M_i = P(M_i),\ i \in \{1,2,...., n\} \tag{5.3}$$

From all this, we can deduce that the public key is defined by the $n+1$ matrices $\{M_o, M_1, ...., M_n\}$ alongside $\Delta$

We can now define both ciphering and deciphering as follows:

*Cyphering*

Let a message be defined vectorially as $m \in Z_r^N$ and noise as $M_o$. If we assign scrambling sequence $mM_o$ to a set of $n$ noise vectors $\sum_i r_i * M_i$, where $r_i < \varepsilon_{\max}$ and $n <_{\max}$

$$c = mM_o + \sum_{i=1}^{n} r_i * M_i \tag{5.4}$$

*Deciphering*

This is achieved by way of filtering the previously added noise sequences. In short, the permutation is reciprocated as:

$$\overset{\bullet}{c} = P^{-1}(c),\ c \in GF(p)^{2N} \tag{5.5}$$

The targeted destination computes the scrambled noise as:

$$e = \overset{\bullet}{c}_D - \overset{\bullet}{c}_U A^{-1} B \tag{5.6}$$

In the last equation $\overset{\bullet}{c}_D, \overset{\bullet}{c}_U$ are non-disturbed and disturbed halves of $\overset{\bullet}{c}$ respectively

$$\overset{\bullet}{e} = e\Delta - 1 \tag{5.7}$$

We also have

$$\ddot{e}_j = \dot{e}_j - \mu \quad \forall \ \dot{e} = \left[\dot{e}_1', \dot{e}_2, ...., \dot{e}_N\right] \tag{5.8}$$

For

$$\mu = \begin{cases} \dot{e}_j \bmod q & \dot{e}_j \bmod q < \frac{q}{2} \\ \left(\dot{e}_j \bmod q\right) - q & \text{otherwise} \end{cases} \tag{5.9}$$

Subject to $m_j = \ddot{e}_j q^{-1}$ and $i \in \{1,2,..., N\}$, $m = (m_1, m_2, ...m_N)$

### 5.4.1.2 The Proposed Aggregation Process Scheme

For simplicity's sake, in the interim, we will first assume that a dedicated secured connection is established between the control canter ( $CC$ ) and $APs$ via $SMs$ and $BSs$.

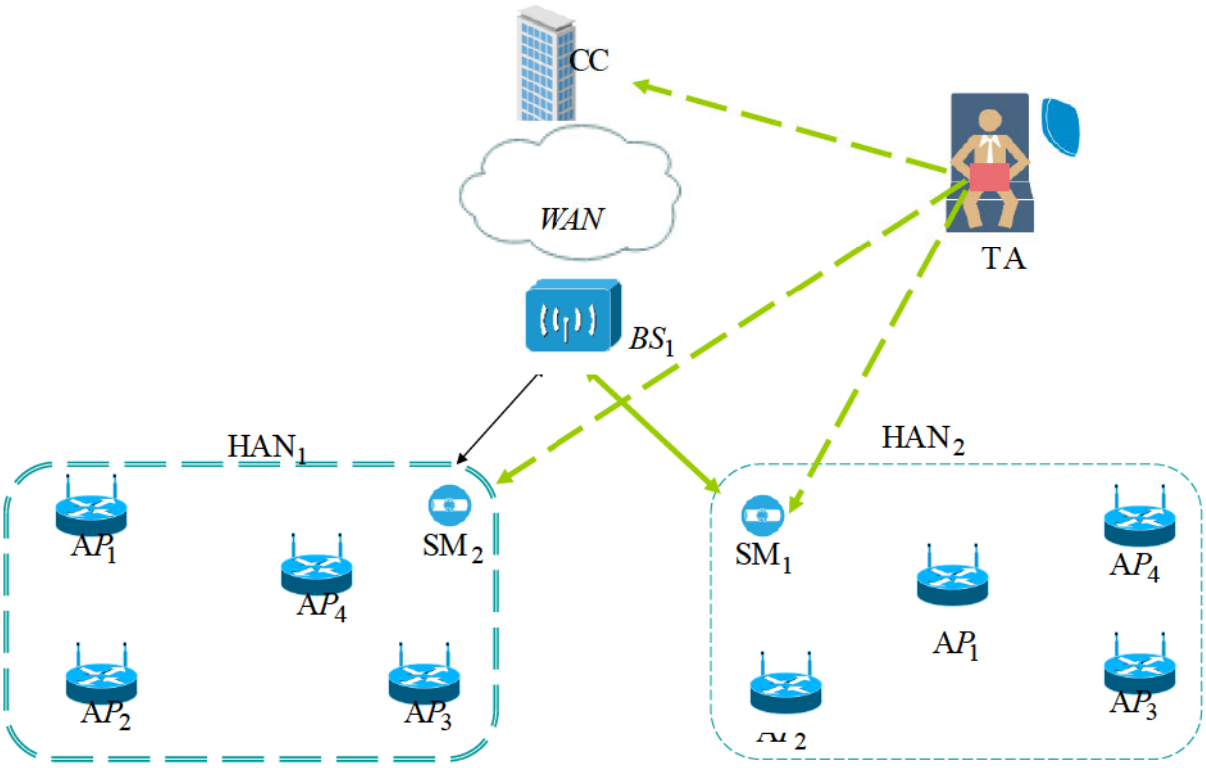


Figure 5-8: Model Configuration

We can thus elaborate on two distinct phases characterizing the operation, initialization and actual data aggregation.

*Initialization*

As is similar to the procedure, followed in chapter 3, the $TA$ assigns public and private keys to all parties

For the $CC$, if $M_{cc0}$ is the scrambling noise, and $\{M_{c1}, M_{cc2}, ..., M_{ccn}\}$ a set of $n$ softened noise sequences, then public keys are:

$$\{M_{cc0}, M_{cc1}, ..., M_{ccn}\} \tag{5.10}$$

The private keys will be;

$$P_{cc}(\bullet), M_{cc}, \Delta_{cc} \tag{5.11}$$

For the $BS$ similarly we have;

$M_{bs0}$ is the scrambling noise , whilst $\{M_{bs1}, M_{bs2}, ..., M_{bsn}\}$ is a set of $n$ softened noise sequences, then public keys are:

Whilst the private keys will be;

$$P_{bs}(\bullet), M_{bs}, \Delta_{bs} \tag{5.12}$$

For an individual $SM$

$M_{sm0}$ is the scrambling noise, whilst $\{M_{sm1}, M_{sm2}, ..., M_{smn}\}$ a set of $n$ softened noise sequences, then public keys are:

Whilst the private keys will be;

$$P_{sm}(\bullet), M_{sm}, \Delta_{sm} \tag{5.13}$$

Each $AP$ has its own ID ( $AP_i$ ) and it encrypts it before safely storing it:

$$ID_{j-enc} = ID_j * M_{sm0} + \sum_i r_i * M_{sm_i} \tag{5.14}$$

*Data Aggregation*

- At HAN level

As already stated, each household has a $HAN$ ., thus each $AP$ ciphers its read data $m_j = (m_1, m_2, ... m_w)$ according to;

$$c_j = m_j M_{cco} + \sum_{i=1} r_i * Mcc_i \tag{5.15}$$

It now dispatches it to the $AP$ for the current reading cycle. The receiving $AP$ aggregates the read data hommorphically;

$$c = \sum_j c_j \tag{5.16}$$

Ultimately it encrypts the aggregated data and relays it to the $SM$

$$AP_s \xrightarrow{c,ID_{s-enc}} SM . \tag{5.17}$$

The $SM$ will in turn validate and time stamp before sending it off to a $BS$. E.g this proceeds as follows:

The timestamp is $T_v$ and nonce comprises $\mathbf{f}$ vectors.

$$x = c\|\mathbf{T_v}\|\mathbf{f} \tag{5.18}$$

$$\dot{x} = P_{sm}^{-1}(x) \tag{5.19}$$

$$e = \dot{x}_D - \dot{x}_U \mathbf{A}_{sm}^{-1}\mathbf{B_{sm}} \tag{5.20}$$

$$\dot{e} = e\Delta_{sm}^{-1} = \left[\dot{e}_1', \dot{e}_2, ...., \dot{e}_N\right] \tag{5.21}$$

For each $\dot{e}_j, i \in \{1,2,...., N\}$ the $SM$ must calculate;

$$\mu = \begin{cases} \dot{e}_j \bmod q & \dot{e}_j \bmod q < \frac{q}{2} \\ \left(\dot{e}_j \bmod q\right) - q & \text{otherwise} \end{cases} \tag{5.22}$$

Subject to;

$$y_j = \ddot{e}_j q^{-1}, i \in \{1,2,...., N\} \tag{5.23}$$

and,

$$Y = (y_1, y_2, ... y_N) \tag{5.24}$$

Once accomplished the relaying is completed thus:

$$SM_s \xrightarrow{c,ID_{s-enc}} BS \tag{5.25}$$

- At $BS$ level

The $SM$ 's signature is validated by checking both $T_v$ and $\mathbf{f}$ before extracting the message:,

$$x = Y * M_{smo} + \sum_{i=1} r_i * Msm_i \tag{5.26}$$

It now aggregates the read data coming from various $SMs$ homomorphically.

$$C = \sum_k c_k \tag{5.27}$$

Next it ciphers the aggregated power consumption of the area using its private key:

$$P_{bs}(*), M_{bs}, \Delta_{bs} \tag{5.28}$$

$$g = c\|\mathbf{T}_w\|q \tag{5.29}$$

$$\overset{\bullet}{g} = P_{bs}^{-1}(g) \tag{5.30}$$

$$w = \overset{\bullet}{g}_D - \overset{\bullet}{g}_U \mathbf{A}_{bs}^{-1}\mathbf{B}_{bs} \tag{5.31}$$

$$\overset{\bullet}{w} = e\Delta_{bs}^{-1} = \left[\overset{\bullet}{w_1}', \overset{\bullet}{w_2}, ..., \overset{\bullet}{w_N}\right] \tag{5.32}$$

For each $\overset{\bullet}{e}_j, i \in \{1,2,..., N\}$ the $SM$ must calculate;

$$\mu = \begin{cases} \overset{\bullet}{w}_j \bmod q & \overset{\bullet}{\mathrm{w}}_j \bmod \mathrm{q} < \frac{\mathrm{q}}{2} \\ \left(\overset{\bullet}{w}_j \bmod \mathrm{q}\right) - q & \text{otherwise} \end{cases} \tag{5.33}$$

Subject to ;

$$d_j = \overset{\bullet\bullet}{w}_j q^{-1}, i \in \{1,2,..., N\} \tag{5.34}$$

and,

$$Y = (y_1, y_2, ... y_N) \tag{5.35}$$

Once accomplished it relays the encrypted data to the $CC$

$$BS_s \xrightarrow{c, ID_{bsenc}} CC \tag{5.36}$$

The $CC$ ultimately receives the aggregated power consumption data from $BS$ and likewise validates it

$$\overset{\bullet}{c} = P^{-1}(c) \tag{5.37}$$

$$s = \overset{\bullet}{c}_D - \overset{\bullet}{c}_U A_{cc}^{-1} B_{cc} \tag{5.38}$$

$$\overset{\bullet}{s} = s\Delta_{cc}^{-1} = \left[\overset{\bullet}{s_1}', \overset{\bullet}{s_2}, ..., s_N\right] \tag{5.39}$$

Once again for each $\overset{\bullet}{s}_k, k \in \{1,2,..., N\}$ the $CC$ calculates;

$$\mu_o = \begin{cases} \overset{\bullet}{s_k} \bmod q & \overset{\bullet}{\mathrm{s}}_k \bmod \mathrm{q} < \frac{\mathrm{q}}{2} \\ \left(\overset{\bullet}{s_{kj}} \bmod \mathrm{q}\right) - q & \text{otherwise} \end{cases} \tag{5.40}$$

Subject to;

$$m_k = \ddot{s}_k q^{-1}, k \in \{1,2,..., N\} \quad (5.41)$$

and,

$$m = (m_1, m_2, ...m_N) \quad (5.42)$$

*Requests for Power Reallocations*

For security purposes, consumption for each defined domain is approximated in advance, and only when demand exceeds this projected value, will a $AP$ request additional power. This is done via the $SM$ and $BS$. The following are the secured procedures that the $AP_j$ takes in sending this request $R$ to the $CC$;

It encrypts its $ID$ by time stamping it with value $T_d$ and nonce $L$

$$n_j = R \| ID_{j-enc} \| T_d \| L. \quad (5.43)$$

It further encrypts $n_j$ using the control canter's a public key

$$z_j = n_j * M_{cco} + \sum_{i=1} r_i * Mcc_i \quad (5.44)$$

The message will in turn be signed by the $BS$ enroute to the $CC$.

### 5.4.1.3 Analysis

The analysis of the efficacy of this framework's lightweight aggregation schemes is determined from both its security and performance. We thus will commence this section with security analysis.

#### 5.4.1.4.1 Security Analysis

During the data aggregation analysis, the scheme has the objective of satisfying both security as well as privacy. In summary, it must ensure data security as well as preserve confidentiality and messages integrity.

Privacy: The scheme conceals the finer details of power consumption from units such as $HANs$, $SMs$ and $BSs$. By this, we mean that each end user's daily power consumption is concealed from all these units, such that even if attackers intercepted the message(s), they will not be able to extract

the semantics as they are encrypted. The same applies to *APs* as they receive the individual readings in ciphered form. Subsequently, the use of encrypted IDs also means that APs and other entities would not find it easy to decipher the real identities of end-users. Peer APs will are only restricted to knowing the aggregated reading of each other, but not the finer detail. It is also important to point out that the aggregated data relayed by APs is encrypted and only *CC* has the decryption keys. As already outlined earlier *HANs* , *SMs* and *BSs* are relaying agents and not capable of extracting the semantics of the aggregated messages.

*Authenticity and Messages' Confidentiality and Integrity:*

The nature and manner in which encryption/decryption keys are assigned is such that only authorized parties can decrypt (decipher) messages. E.g. as earlier alluded to, *HANs* , *SMs* and *BSs* act as relay agents and only the *CC* has decryption keys that were provided(generated) *TA* from the onset. In that way, authenticity, confidentiality as well as integrity are maintained. Note that the use of time stamping together with signatures also makes it impossible for attackers to forge signatures to intercept the data messages.

*Data Security:* Over and above, measures already discussed, the framework utilizes a crypto-system based on the hidden lattice problem, thus considered to be hard. With this cryptosystem, no entity can extract the semantics of the original lattice from its disturbed version.

#### 5.4.1.4.2 Performance Analysis

*Communication Loads*

During a single data aggregation process, a minimal number of messages is exchanged. Moreover, cognizance is taken of the fact that *APs* and *SM* units are general computational resource-constrained and hence the minimized number of messages.

For every data reading and aggregation cycle, an AP sends a single message Overall, it is generally noted that the total communication loads for *BS* , *SM* and each *AP* is one message for each reading and aggregation cycle.

Figure 5.9 shows the communication load at *HAN* level during a data reading and aggregation round. As expected, as we increase the number of household appliances, the communication load also increases. For the *SM* load remains stagnant.

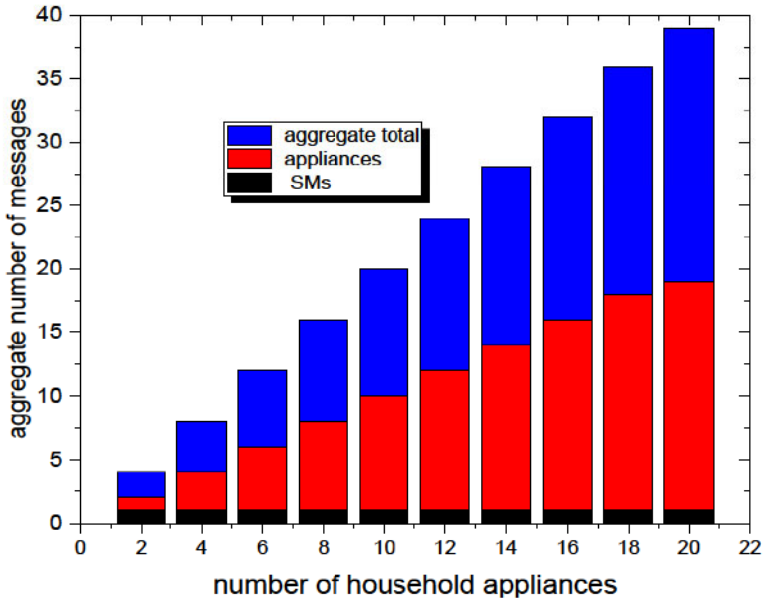


*Figure 5-9:* Communication Loads per Data Reading Cycle

Shown in Figure 5.10 is the total communication loads per day for a particular area (domain). In this case, we gradually increase the number of *APs* corresponding to the increase in the number of households, appliances, or expansion of the domain. Whereas the number of *APs* increase, each *AP*, *SM* or *BS* will still send a single message per reading and aggregation cycle. It can be observed that an increase in the number of *HANs* also leads to communication load moderately increases.

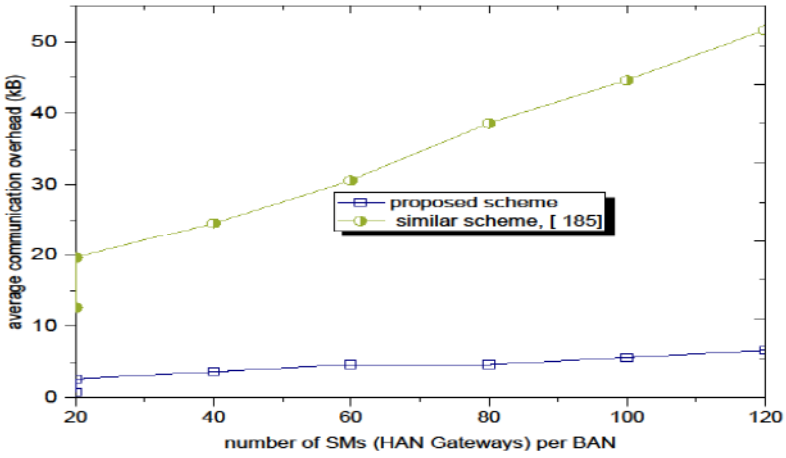


Figure 5-10: Communication Loads per 24-hour Cycle

**Computational Overhead**

According to the proposed scheme, each $AP$ performs a single encryption run per each data reading and aggregation cycle. The same applies to each $HAN$ if it houses a single $AP$. However, if it houses $n$ of them, then the number of encryption operations will also correspondingly increase to $^{n}$. By nature, the encryption is lightweight enough as it involves basic arithmetic operations.

$$C_{total} = [m*(n*T_e + T_s + T_v)] + T_d + T_v + T_s \tag{5.45}$$

In the previous equation, $m$ is the number of $BS$ in the area. $T_e$ is the computation time for one encryption process, $T_d$ is the time for one decryption process, $T_s$ is the time for one signing process, and $T_v$ is the time for one verification process. The provided table (Table 5.1) Summarises the Number of Operations

Table 5.1: Summary of Cryptographic Operations

| Number of cryptographic operations | Per data reading cycle | Per day |
|---|---|---|
| $AP_s\,(Group-1\,\&\,2)$ | $T_e$ | $h*T_e$ |
| $AP_s\,(Group-3\,\&\,4)$ | $T_e$ | $(h+2)*T_e$ |
| $SM$ | $T_e$ | $(h+6)*T_e$ |

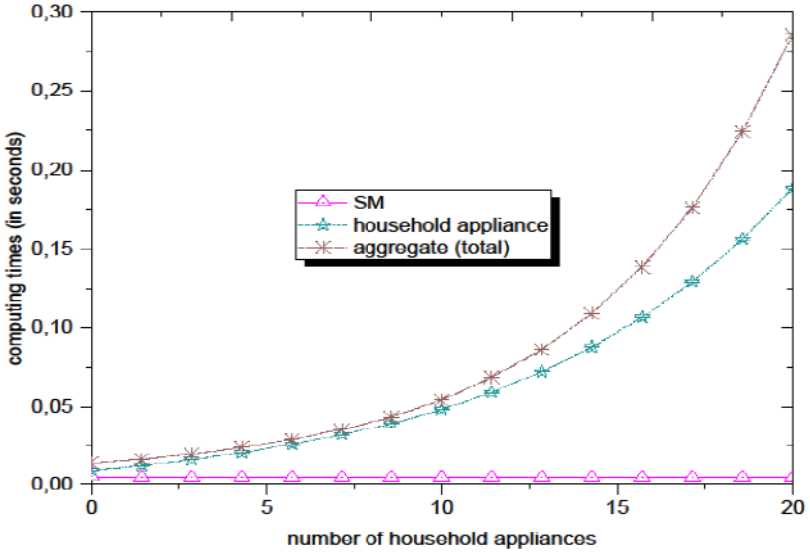


Figure 5-11: Plot of Computational Delay Times

A plot of the computational loads versus the number of appliances is provided in Figure 5.11 for each data reading and aggregation cycle. It can be observed that the computational load of the

individual *APs* is independent of their number in a household. Once again a *SM* 's load is stagnant as it only is required to perform a single signing process regardless of the number of messages included.

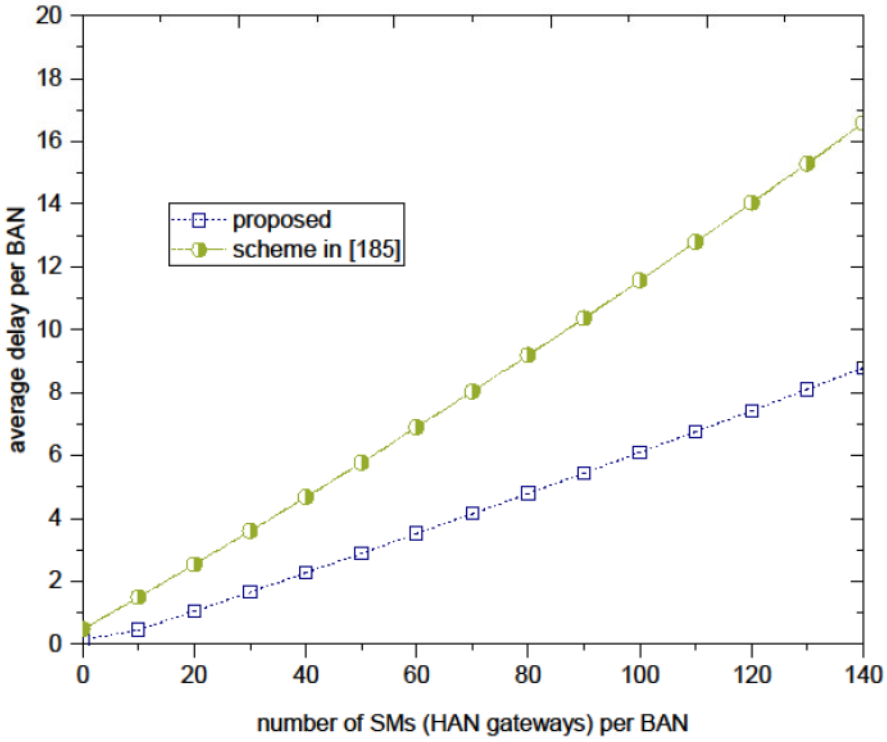


Figure 5-12: Computational Delays

In Figure 5.12, the aggregated daily computation load for a single cluster is plotted for varying numbers of both *HANs* and *APs* e. As indicated, the computation overhead increases by the increase of APs and HANs' numbers, but still within a bounded limit; the total computation delay for a cluster of 100 HANs that each one of them has 20 APs is around 90 seconds per day.

### 5.4.2 A Fog- Cloud-Based Lightweight Authentication Scheme

Note that cloud computing alone has some inherent shortcomings that include, increased end-to-end delays (latencies), lack of mobility support as well as location awareness. As a result real-time and other delay-sensitive applications and services cannot be served under a cloud computing paradigm. Partly this can be offset by cloud centers as close as possible to the core/ central network. Similarly, privacy and security-related services and applications would experience undue latencies, despite the need for speedy reaction measures in preventing and detecting security breaches propagating further in the SG space. Infusing of Fog Computing will better the environment's friendliness, hence allowing the cloud-based services and applications to operate better. The pros of Fog

computing include minimization of round trip latencies, conservation of available network bandwidth, a more secured environment, and a more reliable operation of the services and applications.

Thus, in this proposed scheme, the Fog-Cloud SG system once again is assumed to comprise TA, CC, and entities such as substations units, and Fog nodes. Each residential customer has $SM$ installed and is responsible for taking all power consumption-related data. Specifically, a TA handles the initial registration of all entities that are incorporated into the SG

The CC acts as a central server that receives data from all SMs and processes as well as analyses it. It also dispatches grid commands towards SMs substations, and other entities such as sensors and circuit breakers to ensure stability and reliability of the grid's operations.

The Fog Node will generally handle data flows between end customers via SMs and the CC. In a way, it acts as an intermediary processing point between end-users and the CC.

All substation units will generally await the SG operators' commands before relinquishing power to end-users.

End users are assumed to reside in houses, each of which is fitted with an SM. The sole purpose of an SM is to acquire data related to power consumption in real-time, before relaying it to the CC via a set of intermediaries depending on the network configurations.

#### 5.4.2.1 Threat Model and Design Goals

As already stated, both the CC and TA and CC are exclusively trusted entities. Several attack threats directed towards the SG system such as randomly chosen, known, and targeted Plaintext are assumed.

We thus would like to take into account these threats in designing a multifunctional, diversiform fog-based privacy-preserving scheme. It should realize the following objectives:

The proposed scheme should guarantee both privacy and diversified tariffs. With regards to fair pricing, diversified tariffs must be guaranteed by the scheme. This will enable the CC to accordingly advise end-users in dynamically adjusting their power consumption patterns and behaviors daily.

It is also hoped that the proposed scheme will provide support for multifunctional statistics. In short, it should enable the CC to aggregate the end user's power consumption data in a privacy-

preserving way. In that way, the CC will be able to compute more complex and higher-order statistic functions to provide various services. The scheme should also achieve efficiency as well as the robustness of the SG grid system.

Illustrated in Figure 5.13, the Fog-Computing paradigm. Based SG system Entities such as sensors, HANs, BANs, Gateways, CCs are connected via the existing IoT network. Fog servers are also deployed within the vicinity of the clustered objects, devices, and elements constituting the SG. As cited before, the Fog layer is necessary to improve on round trip response times for some of the SG's services and applications. Overall, the proposed approach (i.e., Fog-cloud paradigm) approach has taken into consideration the resources constrained nature of some of the elements, devices, and objects constituting the SG infrastructure. Note that this framework will also be able to provide SG infrastructural network context information which ultimately is used by applications and services to optimize context awareness. Its support for location-awareness; means it can fully support device mobility. To provide privacy as well as security in surveillance secure, secure authentication and key exchange among the D2D communication compliant SG devices, elements, and objects. We make an overall assumption that the SG network has evolved sufficiently enough. At its base level, will further assume that all associated devices, elements, and entities are under the coverage of 3GPP IoT-enabled network architecture (Figure 5.7).

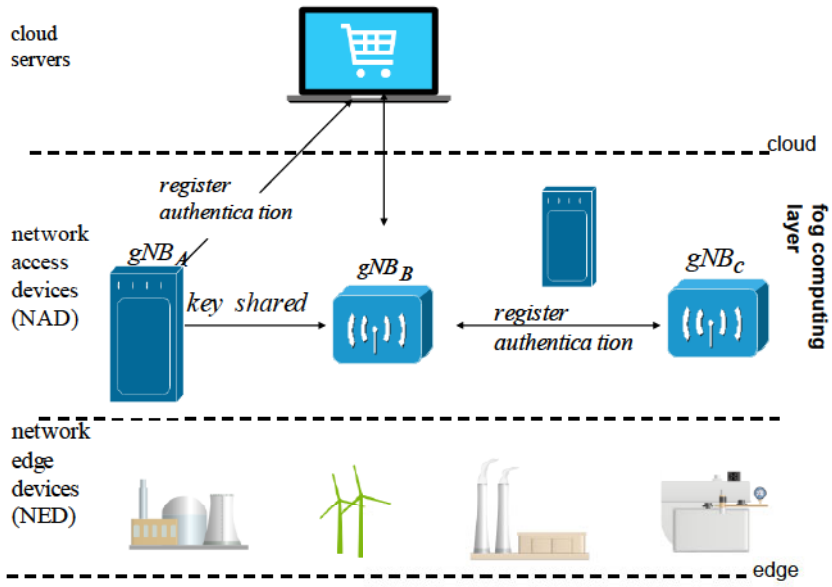


Figure 5-13: Fog Computing Paradigm Alternative

Fog computing easily provides a local overview whereas a global overview will still be provided by cloud computing. Primarily a fog computing model comprises key elements such as (i) network edge device (NED), (ii) network access device (NAD), i.e., fog node, in the proximity of a NAD, and (iii) cloud server which will act as a CC

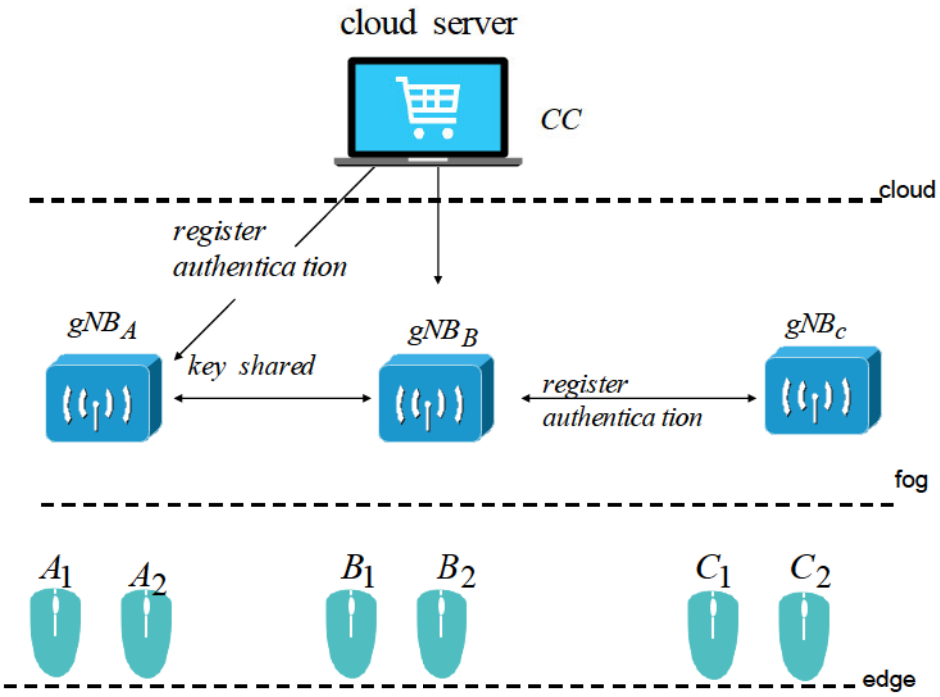


Figure 5-14: Authentication Delegation at Fog Layer

The NEDs will mostly be populated by various deice-constrained devices such as micro-powered smart devices and sensors acquiring data in a defined area from a specified locality. The NAD, has relatively enhanced with more computation capabilities, and given that it has a more reliable power supply, it can thus be bestowed with authentication functionalities as it will always be available. This is exemplified in Figure 5.14.

### 5.4.2.2 Proposed Security Framework

The data exchanges between the various entities constituting the AMI traverse one or multiple collectors and possibly through other SMs acting as relay points. D2D communications is assumed. As such all SMs deployed in the SG are assumed to be D2D communication compliant and physically unclonable. Data load handling in SMs is addressed by way of data aggregation in which the data from various remote SMs is combined before being relayed across the network via a designated relaying $SM$. The same relaying $SM$ becomes a group leader ($SM_{gl}$). In that way, both the bandwidth as well as links are utilized more efficiently.

It is important to ensure that both security and high-level privacy are maintained throughout. By default, the service will involve secure authentication as well as key agreement and exchange among the D2D communication compliant smart surveillance cameras. Data exchanges between the various entities constituting the service may traverse several intermediate relay units. The system exploits the fog computing layer to reduce any undesired end-to-end latencies due to constraint computing resources within the devices. Besides, the Fog layer has several entities such as gNBs and other wireless access points hence it is necessary that within this layer level, interaction among the entities is facilitated so that loads can be evened.

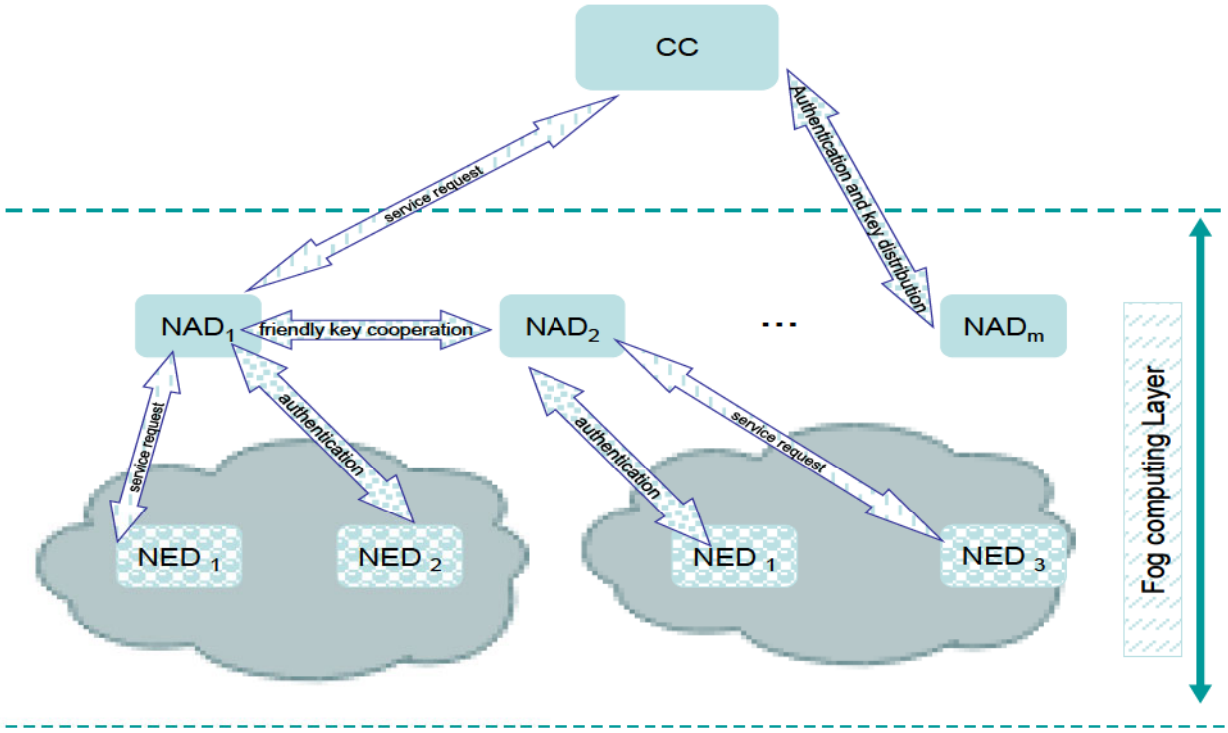


Figure 5-15: D2D Aided Fog Computing

Figure 5.15 illustrates a D2D aided Fog computing model example. Several authentication scenarios are supported. In case the mobile smart surveillance cameras are mobile and it moves to a new NAD, then the most recently attached NAD will assist in the authentication process.

#### 5.4.2.3 Initial Service Registration

Because of security threats in a particular region, several varying size groups of surveillance cameras (edge devices) are deployed. Each surveillance camera or edge device has to register with the cloud computing service (CCS) via a secured link. It will generally follow the following procedural steps:

$ED_i$ formalizes a request to be registered with the CCS.

CCS imitates and $n-$ bit counter $gcount$ which will be automatically incremented for each formal request received.

CSS increments $gcount$, i.e. $[gcount]+1$ , computing a transaction sequence number,

$$T_{seq} = \{gcount\}+1 \tag{5.46}$$

a secret key $K_{ec}$ , and a pseudo;

$$\text{ID } PID = \{pid_1, pid_{2,\ldots} pid_n\} \tag{5.47}$$

that are assumed unlinkable.

The CSS dispatches the parameters generated in the previous steps together with a group key $GK$ to the $ED_i$.

#### 5.4.2.4 Authentication with Fog layer

This takes place when for the first time a member in a group wishes to exchange data (mages captured) to the CCS. . The procedural steps can be summarised as follows:

$ED_i$ contacts the nearest network access device (NAD) and furnishes it with:

$$ED_i \rightarrow NAD : M_{A_1} : \{AID, N_x, T_{seq}\} \tag{5.48}$$

The information is generated as follows: $N_x = N_e \oplus K_{ec}$ is computed by $ED_i$, where, where $N_e$ is a randomly generated number. Similarly $ED_i$ generates $AID = h(ID_{ED_i} \| K_{ec} \| T_{seq})$ and $ID_{ED_i}$ is the surveillance camera's ID. $K_{ec}$ is computed from any one of the unused $pid$ s i.e

$$K_{ec} = AID = pid_j, k_{em_j} \tag{5.49}$$

Because at this stage the two parties are unknown to each other, this information (request message) will be rerouted to the CCS.

$$NAD \rightarrow CCS : M_{A_2} : \{Fwd, M_{A_1}\} \tag{5.50}$$

Upon reception of the message $M_{A_2}$ from NAD, it verifies this information. This it carries out as follows: Firstly it locates the $T_{seq}$ from the local database (DB) and it turn retrieves $ID_{ED_i}$ as well as $K_{ec}$ from the same local DB to use them for the verification process. If verification succeeds,

the CSS generates a communication key $CK$ and a new one $T_{seq_{new}}$. Ultimately the surveillance camera ($ED_i$)the following:

$$e1 = k(K_{ec} \| T_{seq}) \oplus T_{seq_{new}} \tag{5.51}$$

$$e2 = h(K_{ec} \| ID_{ED_i}) \oplus CK \tag{5.52}$$

and

$$\mathrm{Re}s_{CCS} = h(e1 \| e2 \| K_{ec}) \tag{5.53}$$

as well as updating;

$$T_{seq} = T_{seq_{new}} \tag{5.54}$$

CCS then confirms all this to the NAD in the form of a response message $M_{A_3}$

Upon receiving the confirmation message $M_{A_3}$ from CCS, the NAD accordingly generates a tracking number, $Track$ No. as well as a random number $R_n$ before computing;

$$\mathrm{TN} = \mathrm{h}(\mathrm{CK} \| \mathrm{R_n}) \oplus Track \text{ No.} \tag{5.55}$$

and

$$\mathrm{Res_{NAF}} = h(Track\ No. \| CK \| R_n) \tag{5.56}$$

It then sends a confirmation message $M_{A_4}$ to the surveillance camera $ED_i$.

Once $ED_i$, receives the message $M_{A_4}$, it will verify the validity of the response parameters $\mathrm{Re}s_{CCS}$ and $\mathrm{Re}s_{NAD}$ before decoding $T_{seq_{new}}$ and $CK$. Ultimately it will also update $T_{seq}$ to $T_{seq_{new}}$.

Because in D2D fog-assisted computing, neighbouring devices (i.e., in a group) can assist one another by secluding any outsider (hackers). In this case, they will share a channel (link) key $K_{ij}$. In this case, the authentication process can be summarised as follows:

When it becomes necessary for another surveillance camera $ED_j$ to liaise with a NAD, then the NAD can authenticate it with the help of the most recently authenticated device in this case $ED_i$. In this case, $ED_j$ furnishes its identity as an alias identity:

$$AID = h(ID_{ED_j}, \| GK \| T_{seq}) \tag{5.57}$$

as well as generating a common group authentication request;

$$G_{auth} = h(ID_{ED_j} \| R_n \| GK \| K_{ij}) \tag{5.58}$$

Once $ED_i$ has received a request message $M_{B_1}$ from $ED_j$ it will carry out the necessary verifications before sending a confirmation message $M_{B_2}$ to the NAD.

Upon reception of the confirmation message $M_{B_2}$ from $ED_i$ the NAD validates all key parameters including the Track number ( $TrackNo.$ ), and also decodes $tk$ . After successful validation of all key parameters, it will send a response message $M_{B_4}$ to $ED_i$.

Upon receiving $M_{B_4}$ from NAD, it checks the validity of $\mathrm{Re}s_{NAD}$ as well as encoding the $^{tk}$ key. The latter is done using both the link key ( $K_{ij}$ ) and the group key ( $KC$ )

$$tk^{\#} = h(GK \| ID_{ED_j} \| K_{ij}) \oplus tk \tag{5.59}$$

Ultimately it sends a confirmation message $M_{B_4}$ to $ED_j$ .

#### 5.4.2.5 Analysis

In this section, we separately evaluate the proposed scheme in terms of security and performance.

*C. Security analysis*

We justify that our protocol satisfies the following security requirements:

**Mutual Authentication:** As mentioned earlier, it is mandatory that all the SG's objects and devices that are D2D communications compliant mutually authenticate with the 3GPP network using the supported AKA authentication framework. Once accomplished connection requests can securely be channeled between the SG device (object) and 3GPP network as it is now guaranteed that all terminals (entities constituting the SG system) are legitimate. Note that the connection request message has the remote SG devices' broadcasted HMAC code. The 3GPP network will use a locally stored HMAC key to verify the legitimacy of the broadcasting entity (device). The system also facilitates peer SG devices to mutually authenticate via an unsecured available channel. To accomplish that, a randomly generated HMAC key is also distributed from the 3GPP network to the devices involved. As this key once-off key is only exchanged via secure channels, attackers are unable to mislead a responding device by replaying previously exchanged messages, neither can a legitimate SG device be impersonated using another set of DHKE messages.

**Secure Data Transmission**: In our proposal, we have assumed that data is exchanged only after sessions have been authenticated. As the session keys are generated by ECDH and only transmitted via secured channels privacy-compromising is ruled out Note that ECDH is based on Computational Diffie-Hellman (CDH) problem, adversaries cannot find the symmetric key used. Hence only legitimized parties can read content messages but even an intermediary like the 3GPP network will not have knowledge of the actual key used for the particular session.

**Session Key backward/ Forward Secrecy**: The scheme guarantees that attackers cannot retrieve keys from previous or future sessions. This is to guard against situations where a party has exited the SG and then afterward be used for malicious actions in the SG. Similarly, new entrants may not be able to exploit previous transactions. We note that the session key backward/forward secrecy is consolidated by the fact that the stored HMAC keys are only used for message authentication and verification purposes.

**Device Anonymity:** The scheme uses device pseudo identities. As such attackers may only be aware that live sessions exist on the network, but would not be able to decode that sender and destination's real identities and locations.

**Traceability**: The scheme requires that a confirmation message be sent upon successful connection establishment. In that way, if too many failed attempts are detected on one particular point that would serve as an indicator that attackers are attempting to infiltrate.

**Message non-Repudiation**: It is procedural with the proposed scheme that messages be sent via a secured channel, or the insecure channel with either HMAC code or a sequence number appended: the broadcast message, DHKE request message, and DHKE response message are protected using HMAC code. In that way, message non-repudiation is guaranteed and ensured.

**Performance Evaluation**

We carry out a performance analysis of the proposed scheme, and in this regard, we compare it to similar protocols such as the 5G-IoT D2D [180], LIKE [181], and UAKA-D2D [179]. Our focus is on performance aspects such as computational loads, communication overheads, memory requirements for protocol execution, latencies incurred by unknown attacks as well as energy efficiency.

*Computational Overhead*

We use the Bouncy Castle API which is quite similar to the Java Cryptography Architecture (JCA) is relied upon in executing simulation codes for cryptography calculations and time measurement. All the two are embedded in NetSim's IoT library

The differences in terms of requirements for cryptographical functions used in each scheme, as well as key size are taken into account when running the simulations. However, we ultimately used a 128-bit key throughout. In comparing computational overheads we focus on the experimental

computational time of running each of the algorithms. Obtained results in Figure 5-16, show that the proposed scheme, by comparison, requires less computational time among all 3 schemes.

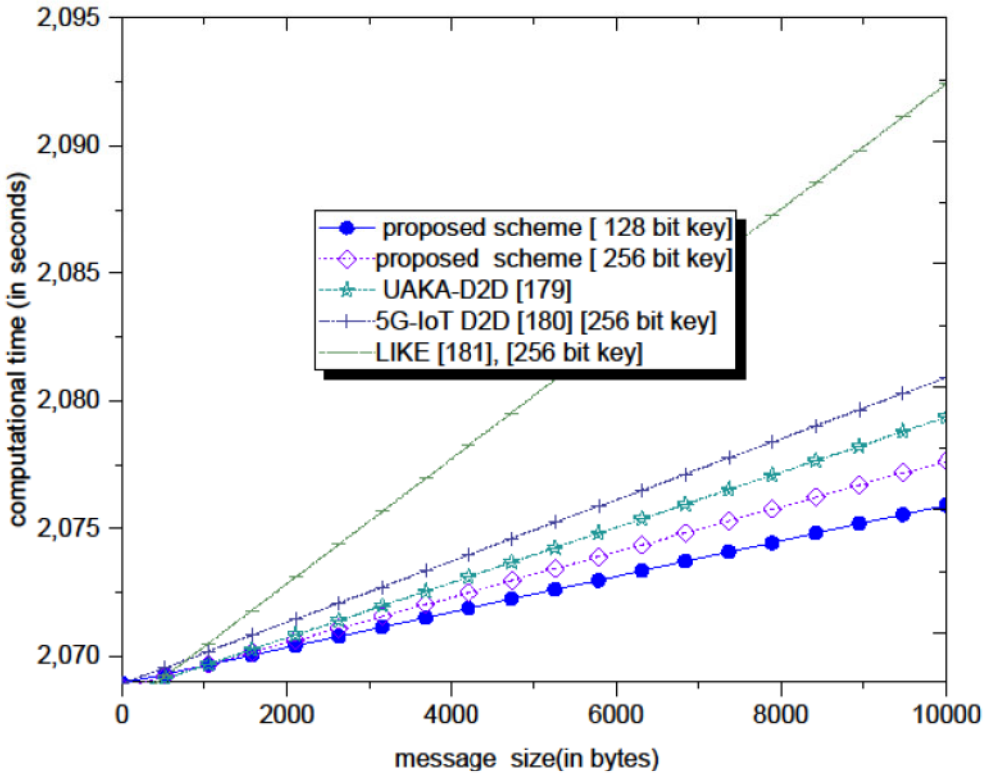


Figure 5-16: Computational Time Comparisons

Moreover, by further analysis it is ascertained that the proposed scheme, by comparison, is 27 % faster than the 5G-IoT D2d scheme, 55% faster, than the LIKE scheme in [181]. Note that the LIKE scheme utilizes asymmetric ECDSA digital signatures.

*Transmission Overhead*

One of the scheme's desirable objectives is that of keeping transmission overheads to a minimum since the environment is naturally bandwidth constrained. The overheads for the scheme comprise the aggregate number of signaling messages exchanged, the length of controlling messages in the protocol, and the supported data rate of the network. We maintain propagation distances of 300 meters, and a propagation speed of $3\times10^{8} ms^{-1}$ .

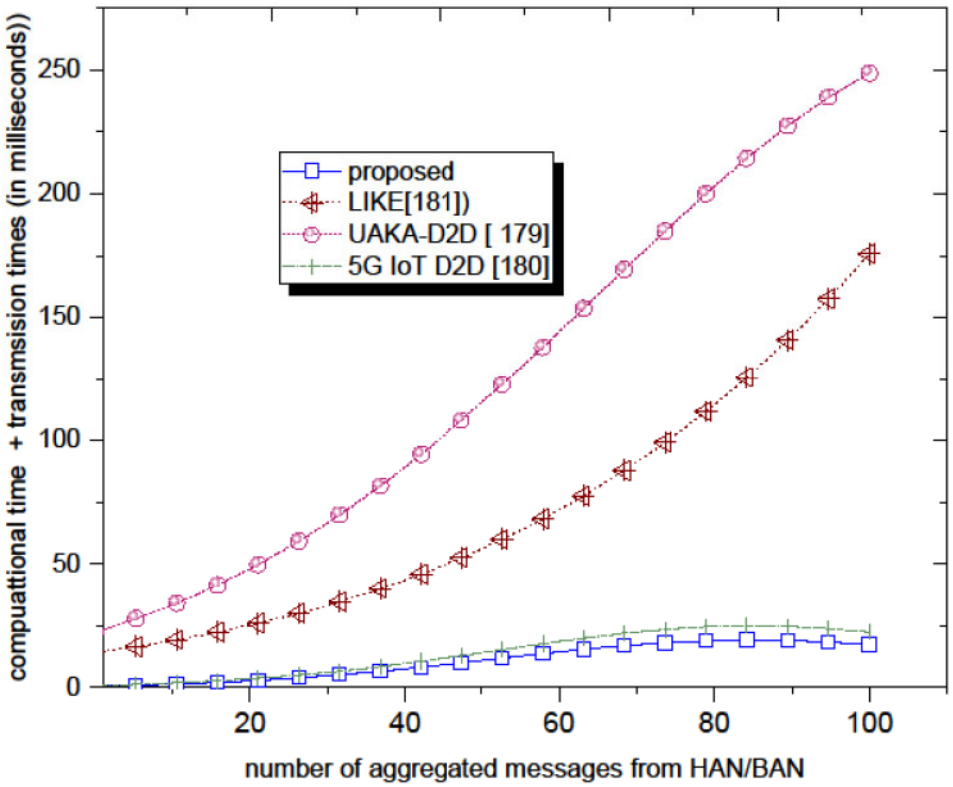


Figure 5-17: Transmission Overheads

For the propagation delays, inter-site distance (ISD)/2 250 meters are chosen to simulate the average UE-UE distance, and the propagation speed of the signals is 3 108 ms-1 and uplink and downlink data rates of 30 Mbps and 60 Mbps respectively. All keys have a fixed length of 250 bits, The 5G-GUTI ‘s length s 100 bits, 5G-SUCI is 256 bits, the message tag is 8 bits, a random nonce is 32 bits, the timestamp is 32 bits, and the session ID is 64 bits. Several simulation runs are carried out and then results are averaged Overall the proposed scheme minimizes transmission overheads as can be observed in the results plotted in Figure 5.17.

*Average Delay*

Since the proposed protocol operates in an uncertain environment in terms of attacks by adversaries, we assume that the protocol will re-initialize each time an attack is registered Thus we measure the average time required for the protocol to accomplish a task under threats of unknown and unanticipated attacks. This part of the simulation is run in MATLAB 2021a. The in-built finddelay function (in MATLAB) uses the xcorr function to determine the cross-correlation between each pair of signals at all possible lags specified by the user. A fragment of the syntax is as follows:

```
r = xcorr(x,y)
r = xcorr(x)
r = xcorr(__,maxlag)
r = xcorr(__,scaleopt)
[r,lags] = xcorr(__)
```

Using the syntax above, a normalized cross-correlation between each pair of signals is then calculated. The estimated delay is given by the negative of the lag for which the normalized cross-correlation has the largest absolute value.

The simulation is run several times and time delays (representing the average time required for the scheme to complete its tasks) are averaged. Figure 5-18 plots the mean execution times. From the same graph, the proposed scheme registers the lowest time delays by comparisons.

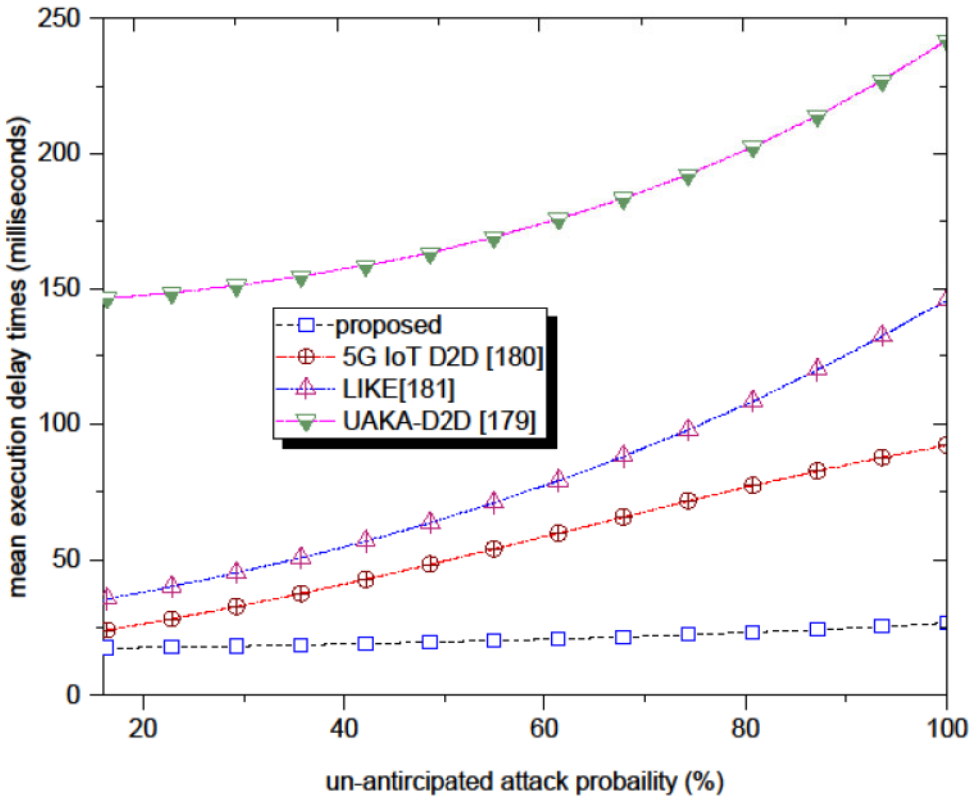


Figure 5-18: Average Mean Execution Delays

*E. Energy Consumption for UE*

Energy consumption and efficiency thereof of any security-related protocol will generally be a function of the volumes of signaling messages exchanged due to the cryptographic algorithms used and the times taken to transmit the same signaling messages. Using the LTE data transfer power model carried out in [182], and related approaches in [183], and [184], we compare by estimate the

energy consumption of the proposed versus the UAKA D2d [179], 5G IoT D2D [180] and LIKE [181].

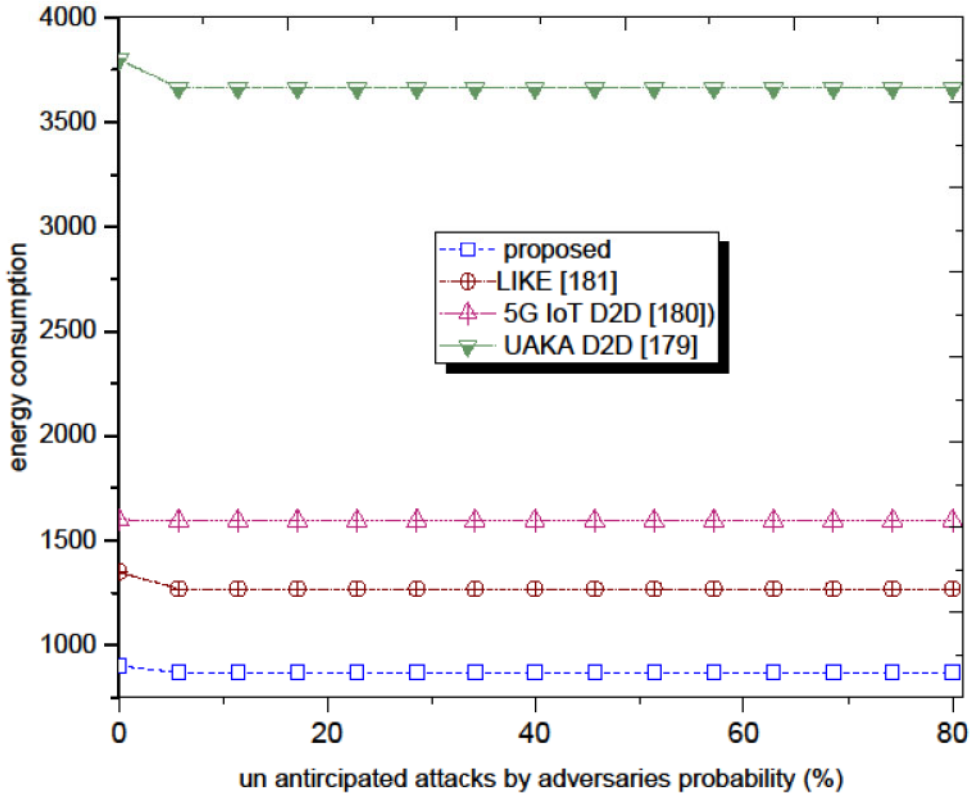


Figure 5-19: Energy Efficiency of the Various Schemes

Using the approaches elaborated in [182], [183], and [184], we finally, the average energy consumptions for the proposed scheme together with the three other similar schemes. Their energy consumption is plotted in Figure 5-19. By comparison, the proposed is much more energy efficient as it utilises much lesser energy for its executions. Partly this is attributed to it relying on the HMAC to replace the power-consuming asymmetric ECDSA and use ECDH to replace the power-consuming modular exponentiation based DHKs. Its use of relatively shorter signaling messages also helps to save energy.

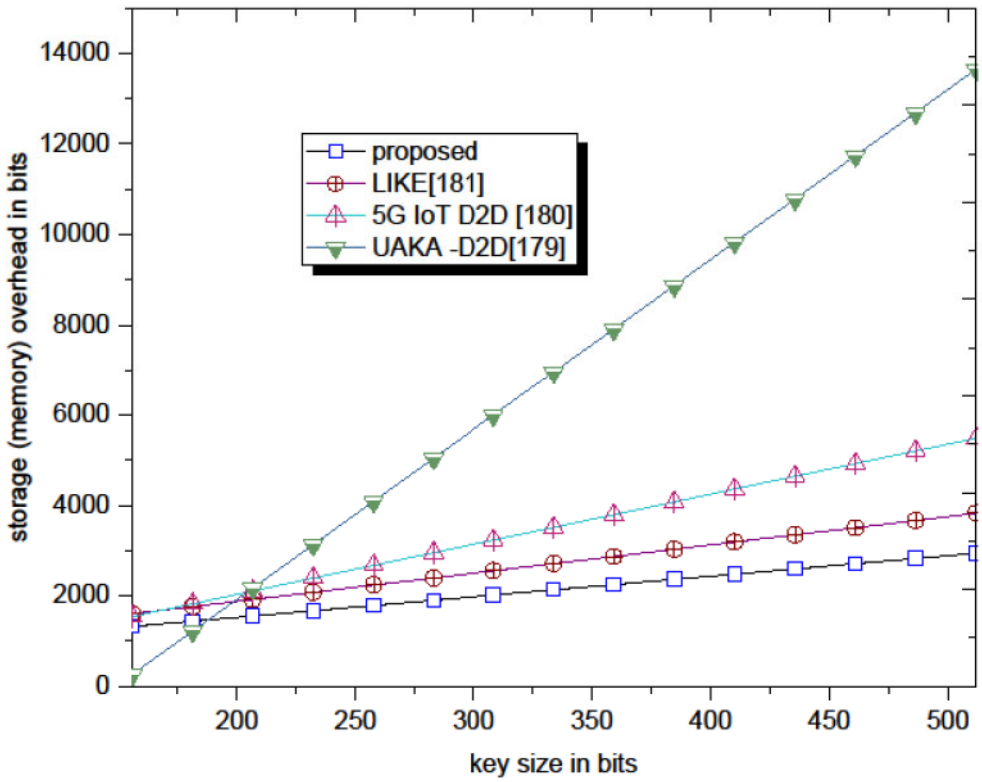


Figure 5-20: Storage Overheads Versus Key Size

*Memory (storage) Overheads*

The amount of memory to initialize a protocol is explored here. Because of the resource-constrained nature of most SG devices, objects, and systems, we need to maintain much smaller storage overheads. Example overhead includes items such as key parameters and all distributed materials from TA including pseudo-identities, tokens, and private keys. The computed storage overheads for the proposed and three other schemes namely, UAKA D2d [179], 5G IoT D2D [180], and LIKE [181] are plotted in Figure 5-20 in which it can be observed that the proposed scheme has the lowest storage overhead for initialization irrespective of key size.

## 5.5 Chapter Summary

The chapter devotes mainly towards addressing security and privacy guarantees for the various would-be services and applications, in future SGs in the advert of existing and future public networks such as IoT and related technologies. We also take cognizance of the fact that an SG architecture cognizance that power grid architectures are always influenced by the physical location of generation sources., whereas legacy electrical power grids always depended on mega-generation sites located remotely, modern and future SG infrastructural architectures will be significantly influenced by the multitudes of DERs with mostly relatively smaller generating capacities.

# 6. Conclusion and Future Work

## 6.1 Introduction

Future SGs can be regarded as the "next generation" of engineered power systems blended with ICT technologies to hence their operational efficiencies and reliability. In a way, various entities are networked together to monitor, control, and regulate such a power system. The emergence of Fog-cloud computing paradigms and related models has contributed immensely towards running SG-related services efficiently. Various entities such as smart metering, sensor/data aggregation typically generate large volumes of data for data analysis and inferences that would further enhance the SG's efficiency. This is because the acquisition of key data from various sensors, and systems assist it in making smart decisions, however, challenges arise, regarding security and privacy.

Throughout this dissertation, the focus is on addressing privacy and security challenges for the various applications and services. Finally, efficient security and privacy-preserving framework (in the form of two proposed schemes) is presented.

In the introductory stages, the work explores general architectures as well as operations of MGs and SGs. Security and privacy concerns during data aggregating and relaying to billing centers are also reviewed.

The second part of the thesis reviews the various security categories and threats. A survey of existing privacy and security schemes is carried out. The work also explores existing security solutions that are primarily based on procedures, such as ciphering/deciphering, confidentiality-related mechanisms, cyber security methods, and anonymization techniques.

## 6.2 Key Findings

Summarily, the dissertation contributes the following:

- In the introductory chapter (Chapter 1), it is generally noted that privacy and security threats issues are quite prevalent in the SG. This is because, by nature of its operations, the SG incorporates many interconnected servers that form delicate cyberspace that serves the various key applications and services that will ensure the overall power grid's efficiency, robustness, and resilience. Motivation as well as key aims, and objectives were also spelled out in this same chapter

- In chapter 2 we carry out a formulation as well as analysis of an MG's day-ahead dispatch problem with DGs subject to non-convex cost function and load dynamics. We first propose an operational framework that addresses the DG's 'valve point" loading effect as well as optimizes its performance. The impact of DSM on convex and non-convex EMS problems with different load participation levels is investigated. Further, the day-ahead scheduling horizon of fifteen-minute resolution time interval(s) is considered to examine the effect of load dynamics in the microgrid. The state-of-art optimization algorithm, Quantum Particle Swarm optimization is employed to solve the proposed problem of non-convex DGs cost optimization. It is demonstrated that the proposed algorithm efficiently solves the non-convex EMS problem. The proposed algorithm efficiently solves the non-convex problem from the obtained simulation results and yields a 4.34 % reduction in operating cost compared to the case where demand-side management participation levels are not considered. Overall the chapter generally concludes that:
    - The SG in general and cyber security infrastructural standards ought to be properly defined.
    - This set of standards will assist in easily enabling cost-effective SG services and applications related to energy (power) distribution, fault diagnostics and rectifications, energy management and smart charging and recharging of EVs.
- In Chapter 3, an analysis is carried out of a Lightweight Privacy-Preserving Scheme for SG HANs. The proposed scheme centered on forecasting power consumption demands for a particular neighborhood, and overall, because most attacks occur, during the transmission of data across the ICT subsystem. This is followed by a further proposal as well as an evaluation of a Group based Authentication and Data Security Scheme for Smart Metering. Both security, as well as performance analysis of the proposed scheme, is carried out. Overall the scheme offers the following:
    - Relatively, low volumes of messages are exchanged between the various parties in the proposed protocol scheme. This is partly because most of them are first aggregated, then dispatched as a multiparty message.
    - The proposed scheme has a much reduced computational overhead when compared with its traditional equivalents resulting in its associated computational times being comparably less.

- With regards to its overall computational complexity relatively, we note that it rises with increases in power demand messages. We thus can conclude that the proposed scheme guarantees privacy and at the same time it minimizes computational and communication overhead levels.

- Chapter 4 extensively reviewed cyber-physical security and the actions of adversaries towards compromising general security in SGs. The chapter tries to adopt a balanced theoretic balanced analysis, thus in the process aiming to holistically and objectively present the base, inner working principles of the attacks. Herein, we propose a secure and scalable framework for ensuring privacy and security in the $SG$ IoT compatible communication architecture that provides interconnectivity to multiple authorities, as well as devices and elements which are part of the $SG$ system. The framework's objective is to provide both security and privacy.
  - Overall performance analysis demonstrates that the proposed scheme requires less transmission bandwidth, hence quite ideal for operating in bandwidth-constrained environments.
  - The scheme utilizes lesser signalling overheads. We however also observe that the signaling overheads tend to increase in proportion to the number of devices incorporated in each group.
  - It is quite energy efficient in operational terms and has reduced end-to-end latencies (turnaround time scales).
  - Security-wise it satisfies most of the key requirements such as privacy, Backward /Forward Key Secrecy, Attack resistivity as well as secured mutual authentication

In chapter 5, proposed is a Fog-Cloud paradigm-based security framework that balances security guarantees and practical, scalable techniques to provide privacy for real-time implementation. The framework is in the form of two proposed schemes as follows:

- A D2D Lightweight Customer Side data Aggregation Scheme takes into cognizance the fact that some of the elements involved are resource-constrained hence a lightweight form approach is chosen. In this way-SG messages will be delivered with absolute security guarantees, at low computational complexities and loads since most of the devices are constrained in terms of both power and computational memory.

- A Fog- Cloud-Based Lightweight Authentication Scheme.

Overall the following is deduced about the proposed framework:

  - That by comparison requires less computational time in comparison with similar schemes already proposed in various literature.
  - It minimizes transmission overheads.
  - It registers the relatively lower time delays.
  - It is much more energy-efficient as it utilizes much lesser energy for its executions. Partly this is attributed to it relying on the HMAC to replace the power-consuming asymmetric ECDSA and use ECDH to replace the power-consuming modular exponentiation based DHKs. Its use of relatively shorter signaling messages also helps to save energy.
  - It requires a very low storage overhead for initialization irrespective of key size.

## 6.3 Future Research Direction

Future research work will be on further enhancing privacy and security in modern SGs with IoT as the underlying communications infrastructure. Envisaged tasks will include the development of Hybrid Testbeds that closely mimic actual SG environments in terms of security threats. Taking into account the dynamics of the components as is characteristic of future systems will be taken into account. Existing and legacy testbeds are mostly software-based, whereas their physical counterpart though affording high fidelity can be prohibitively expensive. Hence the need to shift to hybrid testbeds that will incorporate both software and hardware.

Promoting the inter-connectivity of Testbeds built by the various universities will also help promote more collaborative research efforts among peers. Similarly incorporating Software Defined Networking (SDN) would be another paradigm would asset in verifying the effectiveness of SDN in future SG infrastructures.

## References


[1]. T. Kurbatova and T. Perederii, "Global trends in renewable energy development," 2020 IEEE KhPI Week on Advanced Technology (KhPIWeek), 2020, pp. 260-263, doi: 10.1109/KhPIWeek51551.2020.9250098.

[2]. S. Lanka, S. Ehsan and A. Ehsan, "A review of research on emerging technologies of the Internet of Things and augmented reality," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp. 770-774, doi: 10.1109/I-SMAC.2017.8058283..

[3]. M. Gujar, A. Datta and P. Mohanty, "Smart Mini Grid: An innovative distributed generation based energy system," 2013 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia), 2013, pp. 1-5, doi: 10.1109/ISGT-Asia.2013.6698768.

[4]. M. Caruso, V. Boscaino, R. Miceli, M. Cellura and C. Spataro, "Optimal energy management of smart grids with plug-in hybrid electric vehicles," 2015 International Conference on Renewable Energy Research and Applications (ICRERA), 2015, pp. 1275-1278, doi: 10.1109/ICRERA.2015.7418613.

[5]. L. Che, M. Shahidehpour, A. Alabdulwahab and Y. Al-Turki, "Hierarchical Coordination of a Community Microgrid With AC and DC Microgrids," in IEEE Transactions on Smart Grid, vol. 6, no. 6, pp. 3042-3051, Nov. 2015, doi: 10.1109/TSG.2015.2398853.

[6]. W. Zhao, X. Zhang, Y. Li and N. Qian, "Improved master-slave control for Smooth Transition Between Grid-connected and Islanded Operation of DC Microgrid Based on I -ΔV Droop," 2020 IEEE 9th International Power Electronics and Motion Control Conference (IPEMC2020-ECCE Asia), 2020, pp. 1194-1198, doi: 10.1109/IPEMC-ECCEAsia48364.2020.9367870.

[7]. R. Liu, X. Hai, S. Du, L. Zeng, J. Bai and J. Liu, "Application of 5G network slicing technology in smart grid," 2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), 2021, pp. 740-743, doi: 10.1109/ICBAIE52039.2021.9389979.

[8]. Bing Qi, Hui Bai, Bin Li, Chao Dong and Wei He, "The research on user interface information interaction technology application in smart home," 2015 4th International Conference on Computer Science and Network Technology (ICCSNT), 2015, pp. 1165-1168, doi: 10.1109/ICCSNT.2015.7490940.

[9]. C. Ji, P. Yu, W. Li, P. Zhao and X. Qiu, "Comprehensive vulnerability assessment and optimization method for smart grid communication transmission systems," 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2017, pp. 975-978, doi: 10.23919/INM.2017.7987409.

[10]. F. Luo, G. Ranzi, X. Wang and Z. Y. Dong, "Service Recommendation in Smart Grid: Vision, Technologies, and Applications," 2016 9th International Conference on Service Science (ICSS), 2016, pp. 31-38, doi: 10.1109/ICSS.2016.12.

[11]. P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," in IEEE Security & Privacy, vol. 7, no. 3, pp. 75-77, May-June 2009, doi: 10.1109/MSP.2009.76.

[12]. F. Knirsch, G. Eibl and D. Engel, "Error-Resilient Masking Approaches for Privacy Preserving Data Aggregation," in IEEE Transactions on Smart Grid, vol. 9, no. 4, pp. 3351-3361, July 2018, doi: 10.1109/TSG.2016.2630803.

[13]. D. Bagri and S. K. Rathore, "Research Issues Based on Comparative Work Related to Data Security and Privacy Preservation in Smart Grid," 2018 4th International Conference on Computing Sciences (ICCS), 2018, pp. 88-91, doi: 10.1109/ICCS.2018.00021.

[14]. A. Mohammadali and M. S. Haghighi, "A Privacy-Preserving Homomorphic Scheme with Multiple Dimensions and Fault Tolerance for Metering Data Aggregation in Smart Grid," in IEEE Transactions on Smart Grid, doi: 10.1109/TSG.2021.3049222.

[15]. D. Liu et al., "Research on Technology Application and Security Threat of Internet of Things for Smart Grid," 2018 5th International Conference on Information Science and Control Engineering (ICISCE), 2018, pp. 496-499, doi: 10.1109/ICISCE.2018.00110.

[16]. R. Marah, I. E. Gabassi, S. Larioui and H. Yatimi, "Security of Smart Grid Management of Smart Meter Protection," 2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), 2020, pp. 1-5, doi: 10.1109/IRASET48871.2020.9092048.

[17]. A. I. Kawoosa and D. Prashar, "A Review of Cyber Securities in Smart Grid Technology," 2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM), 2021, pp. 151-156, doi: 10.1109/ICCAKM50778.2021.9357698.

[18]. V. Kayalvizhy and A. Banumathi, "A Survey on Cyber Security Attacks and Countermeasures in Smart Grid Metering Network," 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), 2021, pp. 160-165, doi: 10.1109/ICCMC51019.2021.9418303.

[19]. Choi, D., Choi, H.-K., & Lee, H. C.-S. (2015). A group-based security protocol for machine-type communications in LTE-advanced. Wireless Networks, 21(2), 405–419.

[20]. Lai, C., Li, H., Li, X., & Cao, J. (2013). A novel group access authentication and key agreement protocol for machine-type communication. Transactions on Emerging Telecommunications Technolo- gies, 26(3), 414–431

[21]. H. S. V. S. K. Nunna, A. Sesetti, A. K. Rathore and S. Doolla, "Multiagent-Based Energy Trading Platform for Energy Storage Systems in Distribution Systems With Interconnected Microgrids," in IEEE Transactions on Industry Applications, vol. 56, no. 3, pp. 3207-3217, May-June 2020, doi: 10.1109/TIA.2020.2979782.

[22]. V. K. Saini, V. Gupta, R. Kumar, B. K. Panigrahi and M. A. Mahmud, "Cloud Energy Storage Systems for Consumers and Prosumers in Residential Microgrids," 2020 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), 2020, pp. 1-6, doi: 10.1109/PEDES49360.2020.9379740.

[23]. Y. Varetsky, V. Konoval and M. Seheda, "Modeling Power Flow within a Microgrid for Energy Storage Sizing," 2020 IEEE 7th International Conference on Energy Smart Systems (ESS), 2020, pp. 150-153, doi: 10.1109/ESS50319.2020.9160148.

[24]. S. Heo, J. Han and W. -K. Park, "Energy Storage System with Dual Power Inverters for Islanding Operation of Microgrid," 2020 IEEE International Symposium on Circuits and Systems (ISCAS), 2020, pp. 1-4, doi: 10.1109/ISCAS45731.2020.9180604.

[25]. W. Xinyun and M. Xiaochun, "Research on Coordinated Control of Hybrid Energy Storage in Microgrid Parallel/Off-Grid Mode Switching," 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), 2020, pp. 352-356, doi: 10.1109/ITAIC49862.2020.9338935.

[26]. J. Xiao, L. Bai, F. Li, H. Liang and C. Wang, "Sizing of Energy Storage and Diesel Generators in an Isolated Microgrid Using Discrete Fourier Transform (DFT)," in IEEE Transactions on Sustainable Energy, vol. 5, no. 3, pp. 907-916, July 2014, doi: 10.1109/TSTE.2014.2312328.

[27]. M. R. Sandgani and S. Sirouspour, "Coordinated Optimal Dispatch of Energy Storage in a Network of Grid-Connected Microgrids," in IEEE Transactions on Sustainable Energy, vol. 8, no. 3, pp. 1166-1176, July 2017, doi: 10.1109/TSTE.2017.2664666.

[28]. R. Zhao, Y. Yang, C. Zhang, Z. Wei and M. Deng, "Multi-Energy Storage Control Based on SOC for DC-Microgrid," 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2019, pp. 222-226, doi: 10.1109/IAEAC47372.2019.8997734.

[29]. H. Zou, S. Mao, Y. Wang, F. Zhang, X. Chen and L. Cheng, "A Survey of Energy Management in Interconnected Multi-Microgrids," in IEEE Access, vol. 7, pp. 72158-72169, 2019, doi: 10.1109/ACCESS.2019.2920008.

[30]. S. Wang, H. Gangammanavar, S. D. Ekşioğlu and S. J. Mason, "Stochastic Optimization for Energy Management in Power Systems With Multiple Microgrids," in IEEE Transactions on Smart Grid, vol. 10, no. 1, pp. 1068-1079, Jan. 2019, doi: 10.1109/TSG.2017.2759159.

[31]. A. Parisio, C. Wiezorek, T. Kyntäjä, J. Elo, K. Strunz and K. H. Johansson, "Cooperative MPC-Based Energy Management for Networked Microgrids," in IEEE Transactions on Smart Grid, vol. 8, no. 6, pp. 3066-3074, Nov. 2017, doi: 10.1109/TSG.2017.2726941.

[32]. D. An, Q. Yang, W. Yu, X. Yang, X. Fu and W. Zhao, "SODA: Strategy-Proof Online Double Auction Scheme for Multimicrogrids Bidding," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 7, pp. 1177-1190, July 2018, doi: 10.1109/TSMC.2017.2651072.

[33]. K. Rahbar, C. C. Chai and R. Zhang, "Energy Cooperation Optimization in Microgrids With Renewable Energy Integration," in IEEE Transactions on Smart Grid, vol. 9, no. 2, pp. 1482-1493, March 2018, doi: 10.1109/TSG.2016.2600863.

[34]. W. Shi, X. Xie, C. Chu and R. Gadh, "Distributed Optimal Energy Management in Microgrids," in IEEE Transactions on Smart Grid, vol. 6, no. 3, pp. 1137-1146, May 2015, doi: 10.1109/TSG.2014.2373150.

[35]. Kim, H.M., Lim, Y. and Kinoshita, T., 2012. An intelligent multiagent system for autonomous microgrid operation. *Energies*, 5(9), pp.3347-3362.

[36]. Y. Liu et al., "Distributed Robust Energy Management of a Multimicrogrid System in the Real-Time Energy Market," in IEEE Transactions on Sustainable Energy, vol. 10, no. 1, pp. 396-406, Jan. 2019, doi: 10.1109/TSTE.2017.2779827.

[37]. H. Afrakhte, and P. Bayat, "A contingency based energy management strategy for multi-microgrids considering battery energy storage systems and electric vehicles". *Journal of Energy Storage*, Volume 27, 2020, p.101087.

[38]. H. Farzin, M. Fotuhi-Firuzabad and M. Moeini-Aghtaie, "Role of Outage Management Strategy in Reliability Performance of Multi-Microgrid Distribution Systems," in IEEE Transactions on Power Systems, vol. 33, no. 3, pp. 2359-2369, May 2018, doi: 10.1109/TPWRS.2017.2746180.

[39]. H. Farzin, M. Fotuhi-Firuzabad and M. Moeini-Aghtaie, "Enhancing Power System Resilience Through Hierarchical Outage Management in Multi-Microgrids," in IEEE Transactions on Smart Grid, vol. 7, no. 6, pp. 2869-2879, Nov. 2016, doi: 10.1109/TSG.2016.2558628.

[40]. Z. Wang, B. Chen, J. Wang and C. Chen, "Networked Microgrids for Self-Healing Power Systems," in IEEE Transactions on Smart Grid, vol. 7, no. 1, pp. 310-319, Jan. 2016, doi: 10.1109/TSG.2015.2427513.

[41]. Z. Wang, B. Chen, J. Wang and J. kim, "Decentralized Energy Management System for Networked Microgrids in Grid-Connected and Islanded Modes," in IEEE Transactions on Smart Grid, vol. 7, no. 2, pp. 1097-1105, March 2016, doi: 10.1109/TSG.2015.2427371.

[42]. M. Ghadimi and S. -M. Moghaddas-Tafreshi, "Interaction Model in a Resilient Standalone Multi-Microgrid System," 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), 2019, pp. 56-60, doi: 10.1109/SGCF.2019.8782339.

[43]. A. Hussain, V. Bui and H. Kim, "Resilience-Oriented Optimal Operation of Networked Hybrid Microgrids," in IEEE Transactions on Smart Grid, vol. 10, no. 1, pp. 204-215, Jan. 2019, doi: 10.1109/TSG.2017.2737024.

[44]. S. Hojjatinejad and M. Ghassemi, "Resiliency Enhancement against Wildfires," 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2021, pp. 1-5, doi: 10.1109/ISGT49243.2021.9372206.

[45]. Technology Roadmap - Smart Grids – Analysis - IEA.

[46]. P2030 - Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads (ieee.org), https//standards ieee.org/P2030/html

[47]. V. C. Gungor et al., "A Survey on Smart Grid Potential Applications and Communication Requirements," in IEEE Transactions on Industrial Informatics, vol. 9, no. 1, pp. 28-42, Feb. 2013, doi: 10.1109/TII.2012.2218253.

[48]. L. Ling, Y. Hongyong and C. Xia, "Model Differences between IEC 61970/61968 and IEC 61850," 2013 Third International Conference on Intelligent System Design and Engineering Applications, 2013, pp. 938-941, doi: 10.1109/ISDEA.2012.224.

[49]. A. Semjan and N. Ji, "Experience Sharing - Challenges and Solutions on IEC 61850 Substation Commissioning and Supervision in Thailand," 2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia), 2019, pp. 228-234, doi: 10.1109/GTDAsia.2019.8715970.

[50]. T. S. Ustun and S. M. S. Hussain, "IEC 62351-4 Security Implementations for IEC 61850 MMS Messages," in IEEE Access, vol. 8, pp. 123979-123985, 2020, doi: 10.1109/ACCESS.2020.3001926.

[51]. G. S. Robinson, "ANSI's role in standards development," in IEEE Micro, vol. 17, no. 6, pp. 84-85, Nov.-Dec. 1997, doi: 10.1109/40.641600.

[52]. S. S. Pedersen and Birger Mo, "Risks and risk management for competitive electricity markets, report from CIGRE TF C5-2.02," International Symposium CIGRE/IEEE PES, 2005., 2005, pp. 156-163, doi: 10.1109/CIGRE.2005.1532738.

[53]. T. Johnson and P. Rosa, "The working methods and basic rules of standardization in the standardization sector of the international telecommunication union: ITU-T," in IEEE Communications Magazine, vol. 46, no. 10, pp. 100-107, October 2008, doi: 10.1109/MCOM.2008.4644126.

[54]. Y. Wakasa and T. Ishikuma, "International Standardization for low-carbon society — Trends in international standardization of energy efficiency," 2012 Proceedings of SICE Annual Conference (SICE), 2012, pp. 686-687.

[55]. J. Kossack and B. McQueen, "European progress towards standardization in ATT Communications," Proceedings of VNIS '93 - Vehicle Navigation and Information Systems Conference, 1993, pp. 307-311, doi: 10.1109/VNIS.1993.585638.

[56]. C. Neureiter, D. Engel, J. Trefke, R. Santodomingo, S. Rohjans and M. Uslar, "Towards consistent smart grid architecture tool support: From use cases to visualization," IEEE PES Innovative Smart Grid Technologies, Europe, 2014, pp. 1-6, doi: 10.1109/ISGTEurope.2014.7028834.

[57]. R. Wang, Y. Guo, F. Guan, J. Ma, S. Sun and Z. Yang, "A Construction Method of Power Grid Abnormal State KPI Based on AHP," 2019 IEEE 3rd Conference on Energy Internet and Energy System Integration (EI2), 2019, pp. 2498-2501, doi: 10.1109/EI247390.2019.9061812.

[58]. "ISO/IEC/IEEE International Standard - Systems and software engineering -- Life cycle processes -- Risk management," in ISO/IEC/IEEE 16085:2021(E) , vol., no., pp.1-60, 15 Jan. 2021, doi: 10.1109/IEEESTD.2021.9325968.

[59]. R.Armenta, J. Bazmohammadi, A. Cervantes, J.Saez, D.Vasquez, C. Guerrero, " Energy Management System Optimization in Islanded Microgrids: An Overview and Future Trends", 2021, 10.13140/RG.2.2.11905.17769.

[60]. M. LAGOUIR, A. BADRI and Y. SAYOUTI, "An Optimal Energy Management System of Islanded Hybrid AC/DC Microgrid," 2019 5th International Conference on Optimization and Applications (ICOA), 2019, pp. 1-6, doi: 10.1109/ICOA.2019.8727621.

[61]. U. B. Tayab, F. Yang, M. El-Hendawi and J. Lu, "Energy Management System for a Grid-Connected Microgrid with Photovoltaic and Battery Energy Storage System," 2018 Australian & New Zealand Control Conference (ANZCC), 2018, pp. 141-144, doi: 10.1109/ANZCC.2018.8606557.

[62]. Nanfang Yang, D. Paire, Fei Gao and A. Miraoui, "Power management strategies for microgrid-A short review," 2013 IEEE Industry Applications Society Annual Meeting, 2013, pp. 1-9, doi: 10.1109/IAS.2013.6682500.

[63]. S. K. Sahoo, A. K. Sinha and N. K. Kishore, "Control Techniques in AC, DC, and Hybrid AC–DC Microgrid: A Review," in IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 6, no. 2, pp. 738-759, June 2018, doi: 10.1109/JESTPE.2017.2786588.

[64]. M. Najafzadeh, R. Ahmadiahangar, O. Husev, I. Roasto, T. Jalakas and A. Blinov, "Recent Contributions, Future Prospects and Limitations of Interlinking Converter Control in Hybrid AC/DC Microgrids," in IEEE Access, vol. 9, pp. 7960-7984, 2021, doi: 10.1109/ACCESS.2020.3049023.

[65]. N. Javaid, S. M. Hussain, I. Ullah, M. A. Noor, W. Abdul, A. Almogren, A. Alamri," Demand Side Management in Nearly Zero Energy Buildings Using Heuristic Optimizations", Energies, Volume 10 , 2017.

[66]. G. Sugumar, R. Selvamuthukumaran, T. Dragicevic, U. Nyman, K. G. Larsen and F. Blaabjerg, "Formal validation of supervisory energy management systems for microgrids," IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society, 2017, pp. 1154-1159, doi: 10.1109/IECON.2017.8216197.

[67]. A. Ouammi, Y. Achour, D. Zejli and H. Dagdougui, "Supervisory Model Predictive Control for Optimal Energy Management of Networked Smart Greenhouses Integrated Microgrid," in IEEE Transactions on Automation Science and Engineering, vol. 17, no. 1, pp. 117-128, Jan. 2020, doi: 10.1109/TASE.2019.2910756.

[68]. H. Murdock, D. Gibb, T. André, Renewables 2020 Global Status Report, Technical Report, REN21 COMMUNITY, 2020.

[69]. S. Pannala, N. Patari, A. K. Srivastava and N. P. Padhy, "Effective Control and Management Scheme for Isolated and Grid Connected DC Microgrid," in IEEE Transactions on Industry Applications, vol. 56, no. 6, pp. 6767-6780, Nov.-Dec. 2020, doi: 10.1109/TIA.2020.3015819.

[70]. M. Grami, M. Rekik and L. Krichen, "A Power management Strategy for Interconnected Microgrids," 2020 20th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), 2020, pp. 213-218, doi: 10.1109/STA50679.2020.9329333.

[71]. F. Nejabatkhah, Y. W. Li, A. B. Nassif and T. Kang, "Optimal design and operation of a remote hybrid microgrid," in CPSS Transactions on Power Electronics and Applications, vol. 3, no. 1, pp. 3-13, March 2018, doi: 10.24295/CPSSTPEA.2018.00001.

[72]. K. S. El-Bidairi, H. D. Nguyen, S. Jayasinghe, T. S. Mahmoud, I. Penesis, A hybrid energy management and battery size optimization for standalone microgrids: A case study for Flinders Island, Australia, Energy Conversion and Management 175 (2018) 192 – 212.

[73]. N. Hou, Y. W. Li and L. Ding, "Communicationless Power Management Strategy for the Multiple DAB-Based Energy Storage System in Islanded DC Microgrid," 2020 IEEE Energy Conversion Congress and Exposition (ECCE), 2020, pp. 4656-4661, doi: 10.1109/ECCE44975.2020.9236420.

[74]. D. E. Olivares, J. D. Lara, C. A. Cañizares and M. Kazerani, "Stochastic-Predictive Energy Management System for Isolated Microgrids," in IEEE Transactions on Smart Grid, vol. 6, no. 6, pp. 2681-2693, Nov. 2015, doi: 10.1109/TSG.2015.2469631.

[75]. M. Faisal, M. A. Hannan, P. J. Ker, A. Hussain, M. B. Mansor and F. Blaabjerg, "Review of Energy Storage System Technologies in Microgrid Applications: Issues and Challenges," in IEEE Access, vol. 6, pp. 35143-35164, 2018, doi: 10.1109/ACCESS.2018.2841407.

[76]. Q. Xu, N. Vafamand, L. Chen, T. Dragičević, L. Xie and F. Blaabjerg, "Review on Advanced Control Technologies for Bidirectional DC/DC Converters in DC Microgrids," in IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 9, no. 2, pp. 1205-1221, April 2021, doi: 10.1109/JESTPE.2020.2978064.

[77]. A. Venkataraman et al., "Development of a power mix management system for REIDS microgrids," 2016 Asian Conference on Energy, Power and Transportation Electrification (ACEPT), 2016, pp. 1-5, doi: 10.1109/ACEPT.2016.7811510.

[78]. Á. Navarro-Rodríguez, P. García, R. Georgious and J. García, "Adaptive Active Power Sharing Techniques for DC and AC Voltage Control in a Hybrid DC/AC Microgrid," in IEEE Transactions on Industry Applications, vol. 55, no. 2, pp. 1106-1116, March-April 2019, doi: 10.1109/TIA.2018.2873543.

[79]. T. F. Santos and V. H. Ferreira, "Voltage control in microgrids with minimum adjustment in distributed generation units," 2018 Simposio Brasileiro de Sistemas Eletricos (SBSE), 2018, pp. 1-6, doi: 10.1109/SBSE.2018.8395876.

[80]. [23] G. Banerjee, A. Klingmann, M. Valov, D. Lafferte, C. Hachmann and M. Braun, "Protection and Dynamic Analysis during Bottom-Up Restoration Process in MV/LV Microgrids," 2019 International Conference on Smart Energy Systems and Technologies (SEST), 2019, pp. 1-6, doi: 10.1109/SEST.2019.8849086.

[81]. S. Wang, X. Wang and W. Wu, "Cloud Computing and Local Chip-Based Dynamic Economic Dispatch for Microgrids," in IEEE Transactions on Smart Grid, vol. 11, no. 5, pp. 3774-3784, Sept. 2020, doi: 10.1109/TSG.2020.2983556.

[82]. X. Zhu, L. T. Yang, H. Chen, J. Wang, S. Yin and X. Liu, "Real-Time Tasks Oriented Energy-Aware Scheduling in Virtualized Clouds," in IEEE Transactions on Cloud Computing, vol. 2, no. 2, pp. 168-180, April-June 2014, doi: 10.1109/TCC.2014.2310452.

[83]. A. K. Podder, O. Chakraborty, S. Islam, N. Manoj Kumar and H. H. Alhelou, "Control Strategies of Different Hybrid Energy Storage Systems for Electric Vehicles Applications," in IEEE Access, vol. 9, pp. 51865-51895, 2021, doi: 10.1109/ACCESS.2021.3069593.

[84]. E. Hossain, D. Murtaugh, J. Mody, H. M. R. Faruque, M. S. Haque Sunny and N. Mohammad, "A Comprehensive Review on Second-Life Batteries: Current State, Manufacturing Considerations, Applications, Impacts, Barriers & Potential Solutions, Business Strategies, and Policies," in IEEE Access, vol. 7, pp. 73215-73252, 2019, doi: 10.1109/ACCESS.2019.2917859.

[85]. J. M. Guerrero, P. C. Loh, T. Lee and M. Chandorkar, "Advanced Control Architectures for Intelligent Microgrids—Part II: Power Quality, Energy Storage, and AC/DC Microgrids," in IEEE Transactions on Industrial Electronics, vol. 60, no. 4, pp. 1263-1270, April 2013, doi: 10.1109/TIE.2012.2196889.

[86]. S. S. Vignesh and G. Udayakumar, "An integrated three layer hierarchical control and protection of photovoltaic generators in microgrid," 2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS), 2016, pp. 1-6, doi: 10.1109/ICETETS.2016.7603091.

[87]. O. Babayomi, Y. Li, Z. Zhang, R. Kennel and J. Kang, "Overview of Model Predictive Control of Converters for Islanded AC Microgrids," 2020 IEEE 9th International Power Electronics and Motion Control Conference (IPEMC2020-ECCE Asia), 2020, pp. 1023-1028, doi: 10.1109/IPEMC-ECCEAsia48364.2020.9368069.

[88]. H. Shuai, J. Fang, X. Ai, W. Yao, J. Wen and H. He, "On-Line Energy Management of Microgrid via Parametric Cost Function Approximation," 2020 IEEE Power & Energy Society General Meeting (PESGM), 2020, pp. 1-1, doi: 10.1109/PESGM41954.2020.9281641.

[89]. D. Semënov, G. Mirzaeva, C. D. Townsend and G. C. Goodwin, "Recent development in AC microgrid control — A survey," 2017 Australasian Universities Power Engineering Conference (AUPEC), 2017, pp. 1-6, doi: 10.1109/AUPEC.2017.8282457.

[90]. Anuradha M. Annaswamy; Massoud Amin, "IEEE Vision for Smart Grid Controls: 2030 and Beyond," in IEEE Vision for Smart Grid Controls: 2030 and Beyond , vol., no., pp.1-168, 20 June 2013, doi: 10.1109/IEEESTD.2013.6577608.

[91]. S. Chren, B. Rossi and T. Pitner, "Smart grids deployments within EU projects: The role of smart meters," 2016 Smart Cities Symposium Prague (SCSP), 2016, pp. 1-5, doi: 10.1109/SCSP.2016.7501033.

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

[93]. M. S. Ali, A. Sultana, J. N. Supti, M. T. A. Bhuyan and A. H. Md Shatil, "Enhancing Smart Grid in Bangladesh power distribution system using substation automation," 2015 International Conference on Electrical & Electronic Engineering (ICEEE), 2015, pp. 25-28, doi: 10.1109/CEEE.2015.7428282.

[94]. D. Jeong, J. Byun and S. Park, "Zone-aware service system with nomadic resources for cost-effective pervasive infrastructure," in IEEE Transactions on Consumer Electronics, vol. 60, no. 3, pp. 329-337, Aug. 2014, doi: 10.1109/TCE.2014.6937315.

[95]. S. Matsumoto et al., "Wide-Area Situational Awareness (WASA) system based upon international standards," 11th IET International Conference on Developments in Power Systems Protection (DPSP 2012), 2012, pp. 1-6, doi: 10.1049/cp.2012.0032.

[96]. H. C. Güldorum, İ. Şengör and O. Erdinç, "Charging Management System for Electric Vehicles considering Vehicle-to-Vehicle (V2V) Concept," 2020 12th International Conference on Electrical and Electronics Engineering (ELECO), 2020, pp. 188-192, doi: 10.1109/ELECO51834.2020.00050.

[97]. D. Liu et al., "Research on Technology Application and Security Threat of Internet of Things for Smart Grid," 2018 5th International Conference on Information Science and Control Engineering (ICISCE), 2018, pp. 496-499, doi: 10.1109/ICISCE.2018.00110.

[98]. Deepali and K. Bhushan, "DDoS attack mitigation and resource provisioning in cloud using fog computing," 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon), 2017, pp. 308-313, doi: 10.1109/SmartTechCon.2017.8358387.

[99]. G. ZHU, H. YUAN, Y. ZHUANG, Y. GUO, X. ZHANG and S. QIU, "Research on network intrusion detection method of power system based on random forest algorithm," 2021 13th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), 2021, pp. 374-379, doi: 10.1109/ICMTMA52658.2021.00087.

[100]. W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf and Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security," in IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10250-10276, Oct. 2020, doi: 10.1109/JIOT.2020.2997651.

[101]. R. Wang, Jia Liu, G. Zhang, Shuanghong Huang and Ming Yuan, "Energy efficient power allocation for relay-aided D2D communications in 5G networks," in China Communications, vol. 14, no. 6, pp. 54-64, 2017, doi: 10.1109/CC.2017.7961363.

[102]. L. Hou, Y. Zhang, Y. Yu, Y. Shi and K. Liang, "Overview of Data Mining and Visual Analytics towards Big Data in Smart Grid," 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI), 2016, pp. 453-456, doi: 10.1109/IIKI.2016.83.

[103]. B. Ahn, T. Kim, J. Choi, S. -w. Park, K. Park and D. Won, "A Cyber Kill Chain Model for Distributed Energy Resources (DER) Aggregation Systems," 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2021, pp. 1-5, doi: 10.1109/ISGT49243.2021.9372209.

[104]. A. A. Sadawi, M. S. Hassan and M. Ndiaye, "A Survey on the Integration of Blockchain With IoT to Enhance Performance and Eliminate Challenges," in IEEE Access, vol. 9, pp. 54478-54497, 2021, doi: 10.1109/ACCESS.2021.3070555.

[105]. Y. Gong, Y. Cai, Y. Guo and Y. Fang, "A Privacy-Preserving Scheme for Incentive-Based Demand Response in the Smart Grid," in IEEE Transactions on Smart Grid, vol. 7, no. 3, pp. 1304-1313, May 2016, doi: 10.1109/TSG.2015.2412091.

[106]. M. Fanlin and Y. Wei, "Summary of Research on Security and Privacy of Smart Grid," 2020 International Conference on Computer Communication and Network Security (CCNS), 2020, pp. 39-42, doi: 10.1109/CCNS50731.2020.00017.

[107]. F. Knirsch, G. Eibl and D. Engel, "Error-Resilient Masking Approaches for Privacy Preserving Data Aggregation," in IEEE Transactions on Smart Grid, vol. 9, no. 4, pp. 3351-3361, July 2018, doi: 10.1109/TSG.2016.2630803.

[108]. C. Richardson, N. Race and P. Smith, "A privacy preserving approach to energy theft detection in smart grids," 2016 IEEE International Smart Cities Conference (ISC2), 2016, pp. 1-4, doi: 10.1109/ISC2.2016.7580882.

[109]. P. Kong and Y. Song, "Joint Consideration of Communication Network and Power Grid Topology for Communications in Community Smart Grid," in IEEE Transactions on Industrial Informatics, vol. 16, no. 5, pp. 2895-2905, May 2020, doi: 10.1109/TII.2019.2912670.

[110]. *R. Alharbi, & Lin, X. (2012). "LPDA: A Lightweight Privacy-preserving Data Aggregation Scheme for Smart Grid.* International Conference on Wireless Communications and Signal Processing (WCSP)*., 2012.*

[111]. F. Li, B. Luo and P. Liu, "Secure Information Aggregation for Smart Grids Using Homomorphic Encryption," 2010 First IEEE International Conference on Smart Grid Communications, 2010, pp. 327-332, doi: 10.1109/SMARTGRID.2010.5622064.

[112]. R. Lu, X. Liang, X. Li, X. Lin and X. Shen, "EPPA: An Efficient and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," in IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 9, pp. 1621-1631, Sept. 2012, doi: 10.1109/TPDS.2012.86.

[113]. H. Li, X. Lin, H. Yang, X. Liang, R. Lu and X. Shen, "EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, pp. 2053-2064, Aug. 2014, doi: 10.1109/TPDS.2013.124.

[114]. A. Abdallah and X. Shen, "Lightweight Security and Privacy Preserving Scheme for Smart Grid Customer-Side Networks," in IEEE Transactions on Smart Grid, vol. 8, no. 3, pp. 1064-1074, May 2017, doi: 10.1109/TSG.2015.2463742.

[115]. D. He, N. Kumar, S. Zeadally, A. Vinel and L. T. Yang, "Efficient and Privacy-Preserving Data Aggregation Scheme for Smart Grid Against Internal Adversaries," in IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2411-2419, Sept. 2017, doi: 10.1109/TSG.2017.2720159.

[116]. A. Abdallah and X. S. Shen, "A Lightweight Lattice-Based Homomorphic Privacy-Preserving Data Aggregation Scheme for Smart Grid," in IEEE Transactions on Smart Grid, vol. 9, no. 1, pp. 396-405, Jan. 2018, doi: 10.1109/TSG.2016.2553647.

[117]. C. A. Melchor, G. Castagnos and P. Gaborit, "Lattice-based homomorphic encryption of vector spaces," 2008 IEEE International Symposium on Information Theory, 2008, pp. 1858-1862, doi: 10.1109/ISIT.2008.4595310.

[118]. T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in IEEE Transactions on Information Theory, vol. 31, no. 4, pp. 469-472, July 1985, doi: 10.1109/TIT.1985.1057074.

[119]. Y. Huang, C. Lin and F. Leu, "Verification of a Batch of Bad Signatures by Using the Matrix-Detection Algorithm," 2011 First International Conference on Data Compression, Communications and Processing, 2011, pp. 299-306, doi: 10.1109/CCP.2011.46.

[120]. P. Gope and B. Sikdar, "An Efficient Data Aggregation Scheme for Privacy-Friendly Dynamic Pricing-Based Billing and Demand-Response Management in Smart Grids," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 3126-3135, Aug. 2018, doi: 10.1109/JIOT.2018.2833863.

[121]. C. Thoma, T. Cui and F. Franchetti, "Privacy preserving smart metering system based retail level electricity market," 2013 IEEE Power & Energy Society General Meeting, 2013, pp. 1-5, doi: 10.1109/PESMG.2013.6672616.

[122]. M. A. Mustafa, S. Cleemput, A. Aly and A. Abidin, "An MPC-based protocol for secure and privacy-preserving smart metering," 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2017, pp. 1-6, doi: 10.1109/ISGTEurope.2017.8260202.

[123]. C. Efthymiou and G. Kalogridis, "Smart Grid Privacy via Anonymization of Smart Metering Data," 2010 First IEEE International Conference on Smart Grid Communications, 2010, pp. 238-243, doi: 10.1109/SMARTGRID.2010.5622050.

[124]. J. C. L. Cheung, T. W. Chim, S. M. Yiu, V. O. K. Li and L. C. K. Hui, "Credential-Based Privacy-Preserving Power Request Scheme for Smart Grid Network," 2011 IEEE Global Telecommunications Conference - GLOBECOM 2011, 2011, pp. 1-5, doi: 10.1109/GLOCOM.2011.6134566.

[125]. AVISPA- Automated Validation of Internet Security Protocols [Online]. Available:http://www.avispa-project.org.

[126]. J. Y. Hwang, S. Lee, B. Chung, H. S. Cho and D. Nyang, "Short Group Signatures with Controllable Linkability," 2011 Workshop on Lightweight Security & Privacy: Devices, Protocols, and Applications, 2011, pp. 44-52, doi: 10.1109/LightSec.2011.12.

[127]. F. Diao, F. Zhang and X. Cheng, "A Privacy-Preserving Smart Metering Scheme Using Linkable Anonymous Credential," in IEEE Transactions on Smart Grid, vol. 6, no. 1, pp. 461-467, Jan. 2015, doi: 10.1109/TSG.2014.2358225.

[128]. S. Ullah, E. Khan, S. Ullah and W. Ali, "A light-weight secret key-based privacy preserving technique for home area networks in smart grid," 2017 13th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD), 2017, pp. 895-899, doi: 10.1109/FSKD.2017.8393395.

[129]. M. A. Mustafa, S. Cleemput, A. Aly and A. Abidin, "A Secure and Privacy-Preserving Protocol for Smart Metering Operational Data Collection," in IEEE Transactions on Smart Grid, vol. 10, no. 6, pp. 6481-6490, Nov. 2019, doi: 10.1109/TSG.2019.2906016.

[130]. Li Yan et al., "Study on the remote communication technology in the construction of power user electric energy data acquire system," 2014 China International Conference on Electricity Distribution (CICED), 2014, pp. 43-46, doi: 10.1109/CICED.2014.6991660.

[131]. R. S. Katti, R. Sule and R. G. Kavasseri, "WiP abstract: Multicast authentication in the smart grid with one-time signatures from sigma-protocols," 2013 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), 2013, pp. 239-239.

[132]. A. Saxena and B. Soh, "A new paradigm for group cryptosystems using quick keys," The 11th IEEE International Conference on Networks, 2003. ICON2003., 2003, pp. 385-389, doi: 10.1109/ICON.2003.1266221.

[133]. T. Ma, Y. Jiang, H. Wen, B. Wu, X. Guo and Z. Chen, "Physical Layer Assist Mutual Authentication scheme for smart meter system," 2014 IEEE Conference on Communications and Network Security, 2014, pp. 494-495, doi: 10.1109/CNS.2014.6997521.

[134]. H. Lee, J. Ryu, Y. Lee and D. Won, "Security Analysis of Blockchain-based User Authentication for Smart Grid Edge Computing Infrastructure," 2021 15th International Conference on Ubiquitous Information Management and Communication (IMCOM), 2021, pp. 1-4, doi: 10.1109/IMCOM51814.2021.9377422.

[135]. H. Nicanfar, P. Jokar and V. C. M. Leung, "Smart grid authentication and key management for unicast and multicast communications," 2011 IEEE PES Innovative Smart Grid Technologies, 2011, pp. 1-8, doi: 10.1109/ISGT-Asia.2011.6167151.

[136]. D. S. Gupta and G. P. Biswas, "Identity-Based/Attribute-Based cryptosystem using threshold value without Shamir's Secret Sharing," 2015 International Conference on Signal Processing, Computing and Control (ISPCC), 2015, pp. 307-311, doi: 10.1109/ISPCC.2015.7375046.

[137]. L. Martin, "Identity-Based Encryption Comes of Age," in Computer, vol. 41, no. 8, pp. 93-95, Aug. 2008, doi: 10.1109/MC.2008.299.

[138]. W. Dai et al., "Implementation and Evaluation of a Lattice-Based Key-Policy ABE Scheme," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 5, pp. 1169-1184, May 2018, doi: 10.1109/TIFS.2017.2779427.

[139]. V. M. Shelke and J. Kenny, "Data Security in cloud computing using Hierarchical CP-ABE scheme with scalability and flexibility," 2018 International Conference on Smart City and Emerging Technology (ICSCET), 2018, pp. 1-5, doi: 10.1109/ICSCET.2018.8537272.

[140]. Y. Zhang, J. Li and H. Yan, "Constant Size Ciphertext Distributed CP-ABE Scheme With Privacy Protection and Fully Hiding Access Structure," in IEEE Access, vol. 7, pp. 47982-47990, 2019, doi: 10.1109/ACCESS.2019.2909272.

[141]. H. K. -. So, S. H. M. Kwok, E. Y. Lam and K. Lui, "Zero-Configuration Identity-Based Signcryption Scheme for Smart Grid," 2010 First IEEE International Conference on Smart Grid Communications, 2010, pp. 321-326, doi: 10.1109/SMARTGRID.2010.5622061.

[142]. Y. Jiang and M. Du, "Provable Security Analysis on Unbounded Hierarchical Identity-Based Encryption and Attribute-Based Encryption," 2016 3rd International Conference on Information Science and Control Engineering (ICISCE), 2016, pp. 510-513, doi: 10.1109/ICISCE.2016.116.

[143]. R. Eriguchi and N. Kunihiro, "Strongly Secure Ramp Secret Sharing Schemes from Any Linear Secret Sharing Schemes," 2019 IEEE Information Theory Workshop (ITW), 2019, pp. 1-5, doi: 10.1109/ITW44776.2019.8989107.

[144]. R. Eriguchi and N. Kunihiro, "Strongly Secure Ramp Secret Sharing Schemes from Any Linear Secret Sharing Schemes," 2019 IEEE Information Theory Workshop (ITW), 2019, pp. 1-5, doi: 10.1109/ITW44776.2019.8989107.

[145]. Y. Ye, L. Zhang, W. You and Y. Mu, "Secure Decentralized Access Control Policy for Data Sharing in Smart Grid," IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2021, pp. 1-6, doi: 10.1109/INFOCOMWKSHPS51825.2021.9484474.

[146]. N. Zhao and S. Su, "An Improvement and a New Design of Algorithms for Seeking the Inverse of an NTRU Polynomial," 2011 Seventh International Conference on Computational Intelligence and Security, 2011, pp. 891-895, doi: 10.1109/CIS.2011.201.

[147]. G. Chen, Z. Fu and Z. Xu, "A CRS-based convolution algorithm for NTRUEncrypt," 2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2019, pp. 233-236, doi: 10.1109/IMCEC46724.2019.8984006.

[148]. M. B. Line, I. A. Tøndel and M. G. Jaatun, "Cyber security challenges in Smart Grids," 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies, 2011, pp. 1-8, doi: 10.1109/ISGTEurope.2011.6162695.

[149]. N. Komninos, E. Philippou and A. Pitsillides, "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," in IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933-1954, Fourthquarter 2014, doi: 10.1109/COMST.2014.2320093.

[150]. GitHub - tbuktu/ntru: Java implementation of NTRUEncrypt and NTRUSign

[151]. L. Wei, L. P. Rondon, A. Moghadasi and A. I. Sarwat, "Review of Cyber-Physical Attacks and Counter Defense Mechanisms for Advanced Metering Infrastructure in Smart Grid," 2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D), 2018, pp. 1-9, doi: 10.1109/TDC.2018.8440552.

[152]. H. Zhang, B. Liu and H. Wu, "Smart Grid Cyber-Physical Attack and Defense: A Review," in IEEE Access, vol. 9, pp. 29641-29659, 2021, doi: 10.1109/ACCESS.2021.3058628.

[153]. S. Ruj, A. Nayak, and I. Stojmenovic, A security architecture for data aggregation and access control in smart grids, 1111.2619, ArxivpreprintarXiv, 2011

[154]. A. Fu, J. Song, S. Li, G. Zhang, and Y. Zhang, ''A privacy-preserving group authentication protocol for machine-type communication in LTE/LTE-A networks,'' Security Communication. Networks., vol. 9, no. 13, pp. 2002–2014, 2016

[155]. K.-R. Jung, A. Park, and S. Lee, ''Machine-type-communication (MTC) device grouping algorithm for congestion avoidance of MTC oriented LTE network,'' in Security-Enriched Urban Computing and Smart Grid. Berlin, Germany: Springer, 2010, pp. 167–178

[156]. Y.-W. Chen, J.-T. Wang, K.-H. Chi, and C.-C. Tseng, ''Group-based authentication and key agreement,'' Wireless Personal. Communications., vol. 62, no. 4, pp. 965–979, 2012.

[157]. C. Lai, H. Li, R. Lu, and X. S. Shen, ‘‘SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks,’’ Computer. Networks., vol. 57, no. 17, pp. 3492–3510, 2013.

[158]. R. Jiang, C. Lai, J. Luo, X. Wang, and H. Wang, ‘‘EAP-based group authentication and key agreement protocol for machine-type communications,’’ Int. Journal of Distributed Sensor Networks., vol. 9, no. 11, p. 304601, 2013.

[159]. D. Choi, H.-K. Choi, and S.-Y. Lee, ‘‘A group-based security protocol for machine-type communications in LTE-advanced,’’ Wireless Networks., vol. 21, no. 2, pp. 405–419, 2015

[160]. H. K. Maji, M. Prabhakaran, and M. Rosulek, “Attribute based signatures,” in Topics in cryptology-CT-RSA 2011, vol. 6558 of Lecture Notes in Comput. Sci., pp. 376–392, Springer, Heidelberg, Germany, 2011.

[161]. Choi, D., Choi, H.-K., & Lee, H. C.-S. (2015). A group-based security protocol for machine-type communications in LTE-advanced. Wireless Networks, 21(2), 405–419.

[162]. Choi, D., Choi, H.-K., & Lee, H. C.-S. (2015). A group-based security protocol for machine-type communications in LTE-advanced. Wireless Networks, 21(2), 405–419.

[163]. Lai, C., Li, H., Li, X., & Cao, J. (2013). A novel group access authentication and key agreement protocol for machine-type communication. Transactions on Emerging Telecommunications Technolo- gies, 26(3), 414–431

[164]. L. Sumi and V. Ranga, "Sensor enabled Internet of Things for smart cities," 2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC), 2016, pp. 295-300, doi: 10.1109/PDGC.2016.7913163.

[165]. A. I. Kawoosa and D. Prashar, "A Review of Cyber Securities in Smart Grid Technology," 2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM), 2021, pp. 151-156, doi: 10.1109/ICCAKM50778.2021.9357698.

[166]. A. Sivasangari, D. Deepa, L. L, J. A and V. R, "IoT and Machine Learning Based Smart Grid System," 2021 5th International Conference on Computer, Communication and Signal Processing (ICCCSP), 2021, pp. 1-4, doi: 10.1109/ICCCSP52374.2021.9465493.

[167]. E. H. Et-Tolba, M. Maaroufi and M. Ouassaid, "A multi-agent system architecture modeling for smart grid context," 2014 International Conference on Next Generation Networks and Services (NGNS), 2014, pp. 178-181, doi: 10.1109/NGNS.2014.6990249.

[168]. A. H. Faranadia, A. M. Omar and S. Z. M. Noor, "Power Quality Assessment of Grid Connected Photovoltaic System on Power Factor," 2018 AEIT International Annual Conference, 2018, pp. 1-6, doi: 10.23919/AEIT.2018.8577408.

[169]. S. Zhao et al., "Smart and Practical Privacy-Preserving Data Aggregation for Fog-Based Smart Grids," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 521-536, 2021, doi: 10.1109/TIFS.2020.3014487.

[170]. S. Zahoor, N. Javaid, A. Khan, B. Ruqia, F. J. Muhammad and M. Zahid, "A Cloud-Fog-Based Smart Grid Model for Efficient Resource Utilization," 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), 2018, pp. 1154-1160, doi: 10.1109/IWCMC.2018.8450506.

[171]. D. A. Chekired, L. Khoukhi and H. T. Mouftah, "Fog-Based Distributed Intrusion Detection System Against False Metering Attacks in Smart Grid," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 2019, pp. 1-6, doi: 10.1109/ICC.2019.8761752.

[172]. S. Han, S. Zhao, Q. Li, C. Ju and W. Zhou, "PPM-HDA: Privacy-Preserving and Multifunctional Health Data Aggregation With Fault Tolerance," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 9, pp. 1940-1955, Sept. 2016, doi: 10.1109/TIFS.2015.2472369.

[173]. S. Li, K. Xue, Q. Yang and P. Hong, "PPMA: Privacy-Preserving Multisubset Data Aggregation in Smart Grid," in IEEE Transactions on Industrial Informatics, vol. 14, no. 2, pp. 462-471, Feb. 2018, doi: 10.1109/TII.2017.2721542.

[174]. M. Yang, T. Zhu, B. Liu, Y. Xiang and W. Zhou, "Machine Learning Differential Privacy With Multifunctional Aggregation in a Fog Computing Architecture," in IEEE Access, vol. 6, pp. 17119-17129, 2018, doi: 10.1109/ACCESS.2018.2817523.

[175]. H. Wu, L. Wang and G. Xue, "Privacy-Aware Task Allocation and Data Aggregation in Fog-Assisted Spatial Crowdsourcing," in IEEE Transactions on Network Science and Engineering, vol. 7, no. 1, pp. 589-602, 1 Jan.-March 2020, doi: 10.1109/TNSE.2019.2892583.

[176]. Wang M, Yan Z, Niemi V. UAKA-D2D: Universal Authentication and Key Agreement Protocol in D2D Communications. *Mob Netw Appl* Jun. 2017;22(3):510–25.

[177]. Seok B, Sicato JCS, Erzhena T, Xuan C, Pan Y, Park JH. Secure D2D communication for 5G IoT network based on lightweight cryptography. *Appl Sci* 2020;10(1).

[178]. Baskaran SBM, Raja G. A Lightweight Incognito Key Exchange Mechanism for LTE-A Assisted D2D Communication. In: 2017 9th Int. Conf. Adv. Comput. ICoAC 2017; 2018. p. 301–7.

[179]. A Close Examination of Performance and Power Characteristics of 4G LTE Networks. ww.cs.columbia.edu/~lierranli/coms6998-7Spring2014/papers/rrclte_mobisys2012.pdf.

[180]. C. Guo, Y. Yang, Y. Zhou, K. Zhang and S. Ci, "A Quantitative Study of Energy Consumption for Embedded Security," 2021 IEEE Wireless Communications and Networking Conference (WCNC), 2021, pp. 1-5, doi: 10.1109/WCNC49053.2021.9417382.

[181]. N. R. Potlapally, S. Ravi, A. Raghunathan and N. K. Jha, "A study of the energy consumption characteristics of cryptographic algorithms and security protocols," in IEEE Transactions on Mobile Computing, vol. 5, no. 2, pp. 128-143, Feb. 2006, doi: 10.1109/TMC.2006.16.

[182]. M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu and X. S. Shen, "A Lightweight Message Authentication Scheme for Smart Grid Communications," in IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 675-685, Dec. 2011, doi: 10.1109/TSG.2011.2160661.

## Appendix A: Particle Swarm Optimization (PSO) Codes in MATLAB

Code I

```
function f=ofun(x)
% objective function (minimization)
of=10*(x(1)-1)^2+20*(x(2)-2)^2+30*(x(3)-3)^2;

% constraints (all constraints must be converted into <=0 type)
% if there is no constraints then comments all c0 lines below

c0=[];
c0(1)=x(1)+x(2)+x(3)-5;      % <=0 type constraints
c0(2)=x(1)^2+2*x(2)-x(3);    % <=0 type constraints

% defining penalty for each constraint
for i=1:length(c0)
    if c0(i)>0
        c(i)=1;
    else
        c(i)=0;
    end
end
penalty=10000;              % penalty on each constraint violation
f=of+penalty*sum(c);        % fitness function
```

---

Code II : pso.m.

```
Tic
clc
clear all
close all
rng default

LB=[0 0 0];          %lower bounds of variables
UB=[10 10 10];       %upper bounds of variables

% pso parameters values
m=3;              % number of variables
n=100;            % population size
wmax=0.9;         % inertia weight
wmin=0.4;         % inertia weight
c1=2;             % acceleration factor
c2=2;             % acceleration factor

% pso main program-------------------------------------------------Start
maxite=1000;     % set maximum number of iteration
maxrun=10;       % set maximum number of runs need to befor run=1:maxrun
    run
% pso initialization
    for i=1:n
        for j=1:m
            x0(i,j)=round(LB(j)+rand()*(UB(j)-LB(j)));

        end
```

```
    end
    x=x0;       % initial population
    v=0.1*x0;   % initial velocity
    for i=1:n
        f0(i,1)=ofun(x0(i,:));
    end
    [fmin0,index0]=min(f0);
    pbest=x0;                % initial pbest
    gbest=x0(index0,:);      % initial gbest                              End

% pso initialization ----------------------------------------------------------------start

    % pso algorithm
    ite=1; tolerance=1;
    while ite<=maxite && tolerance>10^-12

        w=wmax-(wmax-wmin)*ite/maxite; % update inertial weight

        % pso velocity updates
        for i=1:n
            for j=1:m
                v(i,j)=w*v(i,j)+c1*rand()*(pbest(i,j)-x(i,j))...
                        +c2*rand()*(gbest(1,j)-x(i,j));

            end
        end

        % pso position update
        for i=1:n
            for j=1:m
                x(i,j)=x(i,j)+v(i,j);
            end
        end

        % handling boundary violations
        for i=1:n
            for j=1:m
                if x(i,j)<LB(j)
                    x(i,j)=LB(j);
                elseif x(i,j)>UB(j)
                    x(i,j)=UB(j);
                 end
            end
         end

        % evaluating fitness
        for i=1:n
            f(i,1)=ofun(x(i,:));
        end

        % updating pbest and fitness
        for i=1:n
            if f(i,1)<f0(i,1)
           pbest(i,:)=x(i,:);
           f0(i,1)=f(i,1);
        end
```

```
        [fmin,index]=min(f0);    % finding out the best particle
        ffmin(ite,run)=fmin;     % storing best fitness
        ffite(run)=ite;          % storing iteration count

        % updating gbest and best fitness
        if fmin<fmin0
            gbest=pbest(index,:);
            fmin0=fmin;
        end

        % calculating tolerance
        if ite>100;
            tolerance=abs(ffmin(ite-100,run)-fmin0);
        end

        % displaying iterative results
        if ite==1
            disp(sprintf('Iteration    Best particle    Objective fun'));
       end
disp(sprintf('%8g  %8g          %8.4f',ite,index,fmin0));
ite=ite+1;

     end

    % pso algorithmgbest;
    fvalue=10*(gbest(1)-1)^2+20*(gbest(2)-2)^2+30*(gbest(3)-3)^2;
    fff(run)=fvalue;
    rgbest(run,:)=gbest;
disp(sprint));

end
end

% pso main program disp(sprintf('\n'));

disp(sprintf('************************************************************'));
disp(sprintf('Final Results-----------------------------'));
[bestfun,bestrun]=min(fff) best_varia-
bles=rgbest(bestrun,:)
disp(sprintf('************************************************************')); toc

% PSO convergence characteristic
plot(ffmin(1:ffite(bestrun),bestrun),'-k');
xlabel('Iteration');
ylabel('Fitness function value'); ti-
tle('PSO convergence characteristic')
%###############################################################################
```

end

## Appendix B: NTRUEncrypt and NTRUSign Implementation in Java

```
package net.sf.ntru.sign;

import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;

import net.sf.ntru.polynomial.DenseTernaryPolynomial;
import net.sf.ntru.polynomial.IntegerPolynomial;
import net.sf.ntru.polynomial.Polynomial;
import net.sf.ntru.polynomial.ProductFormPolynomial;
import net.sf.ntru.polynomial.SparseTernaryPolynomial;
import net.sf.ntru.sign.NtruSign.FGBasis;
import net.sf.ntru.sign.SignatureParameters.BasisType;
import net.sf.ntru.sign.SignatureParameters.TernaryPolynomialType;
```

## Appendix C: Journals and Publication


[1] **P. Khumalo**, L. Bopape, B. Nleya, and A. Mutsvangwa, "A GROUP AUTHENTICATION AND DATA SECURITY SCHEME FOR SMART METERING IN SMART GRIDS," PONTE International Scientific Researchs Journal, vol. 76, 01/01 2020.

[2] **P. Khumalo**, B. Nleya, and A. J. J. o. O. Mutsvangwa, "A controllable deflection routing and wavelength assignment algorithm in OBS networks." Journal of Optics vol. 48, no. 4, pp. 539-548, 2019.


**Publications**


[1] M. Gomba, R. Chidzonga, B. Nleya, and **P. Khumalo**, "Balancing between Demand and Trading in Microgrids," in 2020 International SAUPEC/RobMech/PRASA Conference, 2020, pp. 1-5: IEEE.

[2] **P. Khumalo**, B. Nleya, A. Gomba, and A. Mutsvangwa, "Services and Applications Security in IoT Enabled Networks," in 2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC), 2018, pp. 1-7: IEEE.

[3] **P. Khumalo**, B. Nleya, and A. Mutsvangwa, "Intermediate node buffering-based contention minimization scheme," in Southern Africa Telecommunication Networks and Applications Conference (SATNAC) 2019, 2019: TELKOM.

[4] **P. Khumalo**, B. Nleya, A. Mutsvangwa, and R. Chidzonga, "Quality of Transmsision Aware Routing and Wavelength Assignment Algorithm for Blocking Minimization in Translucent Optical Networks," in 2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD), 2020, pp. 1-5: IEEE.

[5] B. Nleya, **P. Khumalo**, and A. Mutsvangwa, "A Restricted Intermediate Node Buffering-Based Contention Control Scheme for OBS Networks," in 2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), 2019, pp. 1-6: IEEE.

[6] **Z.P Khumalo**, B. Nleya, "Secured Smart Grid Network for Advanced Metering Infrastructure (AMI*)", SAIEE/ Smart Grid Conference Proceedings*, ESKOM Training centre,Midrand JHB, 25-27 Feb,,. ISBN no. 978-0-62071202-6.

[7] **Z.P Khumalo**, B. Nleya. Renewable Energy Technology for Saving and Generating Pollution Free Energy in South Africa. *SAUPEC Proceedings*, Three River Lodge (VUT) Johannesburg.26 to 28 January 2016, ISBN no. 978 1 77012386.

[8] **Z.P Khumalo**, B. Nleya, "Data Re-Sequencing Delays in Smart Grids". *Proceedings of the IEEE's 3rd international conference on advanced computing and Communication Engineering*. Coastland Hotel, Durban28 to 29 November 2016. ISBN-987-1-5090-2576-6.

[9] **Z.P Khumalo**, B. Nleya, "A Review of Energy Efficiency Considerations in Optical Backbone Supported Clouds",*Proceedings of SAIEE's Conference on SMART GRIDs*, ESKOM Training centre Midrand JHB, 19-21 Sept, 2017.

[10] **Z.P Khumalo**, B. Nleya, "System Architecture and Security Overview for Smart Grids", *Proceedings of SAIEE's Conference on SMART GRIDs,* ESKOM Training centre, Midrand JHB, 19-2 Sept., 2017

[11] **Z.P Khumalo** and B. Nleya, "Secure Power Line Communication Based Network for Advance Metering Infrastructure",*SAUPEC Conference Proceedings*, Protea Hotel , Stellenbosh, 30 January, 01 February 2017.

[12] **ZP Khumalo**, Green Energy for Energy for Rural Area of South Africa. *JGED Journal of Green Economy and Development*. Salt Rock Hote, North Coast, 13-15 July, 2016.

[13] **Z. P Khumalo**, "Long Term Evolution LTE and Green Technology for Public Safety", *JGED Journal of Green Economy and Development*.,Salt Rock Hotel, North Coast,13- 15 July, 2016.

[14] **Z. P Khumalo** and Bakhe Nleya, "Secured Smart Grid Network for Advanced Metering Infrastructure (AMI)", Research Publications (Engineering and Built Environment),DUT, February, 2016.

[16] **Khumalo, Philani**, and Bakhe Nleya. "Sleep-Mode/Traffic Grooming Versus Device Reliability Overview." *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*. IEEE, 2018.

[16] **Z. P Khumalo** and B .Nleya, "A Survey of Energy Efficient Optical Backbone Network Approaches for Supporting Cloud Computing", *IEEE International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD 2018)*