An enhanced cybersecurity algorithm for the smart grid SCADA System.

An enhanced cybersecurity algorithm for the Smart Grid SCADA System

By

Kholofelo Hope Halefose

(207224693)

Submitted in fulfilment of the requirements for the degree

MASTER OF COMPUTING: INFORMATION TECHNOLOGY (COMMUNICATION NETWORKS)

in the

DEPARTMENT OF INFORMATION TECHNOLOGY

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

at

TSHWANE UNIVERSITY OF TECHNOLOGY

Supervisor: Dr. TE Mathonsi

Co-Supervisors: Dr. T Muchenje & Dr. DP du Plessis

May 2023

Declaration

I, Kholofelo Hope Halefose, declare that this thesis research study entitled *An enhanced cybersecurity algorithm for the Smart Grid SCADA System* is my own work. It is being submitted in partial fulfilment of the requirements for the Master of Computing Degree: Information Technology, at Tshwane University of Technology, Pretoria. I further declare that all sources cited or quoted are indicated and acknowledged using a comprehensive list of references.

Signature	Date
……..	……

Dedications

I dedicate this study to my parents − my mother, Kedibone Maria Halefose, and my late father, John Setsepa Kgwedi − they are my inspiration for pursuing my studies. I also dedicate this work to my children, who have always been my source of strength and my reason for not giving up; and my reason for always striving to be the best version of myself.

Acknowledgments

Firstly, I would like to thank God for the strength and wisdom he has given me to conduct this study. Secondly, my gratitude goes to my supervisors, Dr. TE Mathonsi, Dr. T Muchenje & Dr. Du Plessis, for their endless guidance, warm encouragement, critical comments, patience, and support throughout. Their direction and feedback were always constructive and positive. Thirdly, I thank my family for their continuous support. Last but not least, to my amazing partner, whose words of encouragement and push for tenacity have kept me going − thank you for always believing in me.

Publications

Parts of this research study have been submitted and accepted for publication in the following journal and conference proceedings:

Journal:

1. Kholofelo Hope Halefose, Topside E. Mathonsi, Tonderai Muchenje, and Deon P. Du Plessis, “An Enhanced Cybersecurity Algorithm for Smart Grid”. Submitted to Journal of Advances in Information Technology.

Conference proceedings:

1. Kholofelo Hope Halefose, Topside E. Mathonsi, Tonderai Muchenje, and Deon P. Du Plessis, “Implementation of an Enhanced Cybersecurity Algorithm for Smart Grid”. Proceedings of the 2022 International Conference on Computational Science and Computational Intelligence (CSCI'22), 14 – 16 December 2022, Las Vegas, USA, Page 1029 – 1034, ISBN-13: 979-8-3503-2028-2, DOI 10.1109/CSCI58124.2022. Available at: https://american-cse.org/csci2022-ieee/csci2022.zip or https://ieeexplore.ieee.org/xpl/conhome/1803739/all-proceeding.

Abstract

Smart Grid development is a global initiative to ensure that utilities provide future systems architecture that will integrate all the processes and systems required for an intelligent electricity network. The Smart Grid is necessary and imminent; and without it, it will be impossible to manage and control modern ways of power generation, transmission, and distribution. Unlike the old traditional power grid in which automation systems were isolated from the corporate networks, the Smart Grid is more prone to cyberattacks, due to the nature of its complexity. In addition to that, the reliance of the Smart Grid on the Supervisory Control and Data Acquisition (SCADA) system for automated control and monitoring increases the vulnerabilities of the Smart Grid to cyber risks, cyber-threats, and cyberattacks. To fully protect the Smart Grid SCADA system communication, the existing Smart Grid SCADA protocols must ensure end-to-end authentication, data integrity, confidentiality, and availability, Denial of Service (DoS) attacks targeting the availability. DoS attacks are considered one of the major threats to the Smart Grid SCADA system, because a successful attack can lead to a blackout. This research study proposed an enhanced cybersecurity algorithm by integrating the N-th degree truncated polynomial ring units (NTRU) algorithm into the Toom-Cook algorithm, to ensure secure end-to-end authentication and communication during data transmission while reducing complexity. The NS-2 simulator was used to simulate, evaluate, and measure the effectiveness of the proposed enhanced cybersecurity algorithm (ECS). The ECS algorithm was compared with the best-known algorithms, namely, the elliptic curve cryptography (ECC) algorithm, and Rivest, Shamir, Adleman (RSA), used for protecting the Smart Grid SCADA System. By comparison with RSA and ECC, the simulation results show that ECS achieved high-speed encryption of 1.4ms and high decryption speed of 2.9ms with the use of minimal computing power. The ECS only sustained a 0.5% packet loss during the launch of a DoS attack, making it suitable for the SCADA system, with real-time constraints and hardware

limitations. Furthermore, the ECS addresses the data-integrity, confidentiality, availability, and authentication issues of the Smart Grid SCADA system.

Keywords: Smart Grid, SCADA, enhanced cybersecurity algorithm, NTRU algorithm, and Toom-Cook algorithm

Table of Contents

List of Tables

List of Figures

List of Algorithms

List of Abbreviations

AES	Advanced Encryption Standards
AGC	Automatic Generation Control
AMI	Advanced Metering Infrastructure
ANSI	American National Standards Institute
API	Application Programming Interface
AVR	Automatic Voltage Regulation
BANs	Business Area Networks
CIA	Confidentiality, Integrity and Availability
CSWG	Cyber Security Working Group
DCS	Distributed Control Systems
DH	Diffie–Hellman
DMS	Distribution Management System
DNP3	Distributed Network Protocol
DoS	Denial of Service
DDoS	Distributed Denial of Service
DR	Demand-Response
DSM	Demand Side Management
ECS	Enhanced Cybersecurity
EMS	Energy Management System
GIS	Geographical Information System
HANs	Home Area Networks
IACS	Industrial Automation and Control Systems
ICS	Industrial Control Systems
ICT	Information Communication and Technology
IDSA	Intrusion Detection System Approach
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IoT	Internet of Things
ISA	International Society of Automation
ISO	International Organization for Standardization

IT	Information Technology
ITU-T	International Telecommunication Union-Telecommunication
LA	Learning Algorithm
LAN	Local Area Network
LIOC	Low Orbit Ion Cannon
KEM	Key-Encapsulation Mechanism
MDM	Meter Data Management
MITM	Man in the Middle
MPLS	Multiprotocol Label Switching
MSU	Master Station Unit
MTU	Master Terminal Unit
NILM	Non-invasive Load Monitoring
NIST	National Institute of Standards and Technology
NISTR	National Institute of Standards and Technology Interagency Report
NTRU	N-th degree Truncated Polynomial Ring Units
NS-2	Network Simulator-2
OMS	Outage Management System
OT	Operational Technology
PAC	Process Automation Controller
PKC	Public Key Cryptography
PKCSs	Public Key Cryptosystems
PLC	Programmable Logic Controller
PMU	Phasor Measurement Unit
PPS	Professional Provident Society
QoS	Quality of Service
RTU	Remote Terminal Unit
RTP	Real-Time Price
SA	South Africa
SCADA	Supervisory Control and Data Acquisition
SG	Smart Grid
SGDR	Smart Grid Demand-Response

SGIP	Smart Grid Interoperability Panel
SKC	Symmetric Key Cryptography
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
US	United States
UWB-IR	Ultra-WideBand Impulse Radio
VHF	Very High Frequency
WAMS	Wide Area Management System
WANs	Wide Area Networks

Chapter 1: Introduction

1.1 Background to the Study

A smart grid is an electricity network that uses digital and other advanced technologies to monitor and manage the transporting of electricity from all generation sources to meet the varying electricity demands of end users. SCADA is a category of software applications for controlling industrial processes, which is the gathering of data in real-time from remote locations in order to control equipment and conditions. The traditional power grid as we know it is evolving into a modern Smart Grid with interconnected smart devices. This evolution has made the Smart Grid SCADA system vulnerable to cyberattacks and other security threats.

In the Smart Grid SCADA system, vulnerabilities can impact any of three main components, namely: the master station unit (MTU), the remote telemetry unit (RTU), and the communication networks. Since RTUs are spreading out over large areas, they are more vulnerable than others and are at a higher security risk. DoS attacks target the availability of the cybersecurity objectives. The goal of a DoS attack is to disrupt some legitimate activity, such as making the RTUs unable to communicate with one another. A DoS attack is achieved by sending messages to the target that interfere with its operation, and make it hang, reboot, crash, or perform useless work. DoS attacks are considered one of the major threats to the Smart Grid SCADA system, because a successful attack on the RTU can lead to a blackout.

With the Smart Grid being considered a critical infrastructure for any country, it is imperative to protect it against cyberattacks. A successful cyberattack on critical infrastructure poses a significant risk − it threatens the country's economy, national security, and public health and safety. Cybersecurity is a crucial security requirement in Smart Grid and NIST. Thus US Departments (2012) provides guidelines for Smart Grid cybersecurity implementation. Such includes three (3) cybersecurity objectives that must be achieved, namely: confidentiality, integrity, and availability. Researchers have attempted to discover, design, and propose cybersecurity algorithms as well as a security

scheme that improves the cybersecurity of the Smart Grid. However, Cyberattackers are becoming more advanced every day; and new and advanced cyberattacks are being introduced and launched in the online world at a very rapid pace. In 2014, when CyberEdge set its first CyberEdge Report (CDR) in motion, 62% of organizations were said to have been compromised by successful cyberattacks. In 2021 that number has risen to 86%. The percentage of organizations experiencing a successful attack rose by 5.5%, which is the largest increase in the past six (6) years (CyberEdge Group, 2021).

The continuous and repeated cyberattacks on critical infrastructure demonstrate the need for improved cyber security for the Smart Grid SCADA system. To fully protect the Smart Grid SCADA system communication, the existing SCADA protocols must provide end-to-end authentication, data integrity, confidentiality, and availability (Shahzad et al., 2014). According to Yadav et al. (2017), most of the Smart Grid SCADA system vulnerabilities are exploited via remote access. Furthermore, Ghosh et al. (2019) support that statement, indicating that one of the main reasons for that vulnerability is the lack of strong encryption and real-time monitoring. Algorithms are a crucial part of technology, presenting secure authentication, integrity, and encryption. Authentication, key management, encryption, and decryption play vital roles in successfully implementing cybersecurity for the Smart Grid SCADA system. Therefore, the purpose of this study is to design an ECS algorithm that will improve and strengthen cybersecurity for the Smart Grid SCADA system.

1.2 Research Motivation

Eskom generates approximately 95% of the electricity used in South Africa, and approximately 45% of the electricity used in Africa (Expatica, 2021). To have an effective and efficient supply of electricity without any form of destruction, it is imperative that the Smart Grid SCADA system be protected against cyber threats and attacks. To achieve this an ECS algorithm should be designed in such a way that malicious users cannot gain unauthorized access to the Smart Grid SCADA network and systems. Therefore, this research study proposes an ECS algorithm that can protect and prevent malicious users

from gaining unauthorized access to the Smart Grid SCADA system during data transmission. In addition, the interest in carrying out this research study was to develop my research skills in solving research problems; and also to learn more about the Smart Grid SCADA System cybersecurity and various cybersecurity algorithms used to protect against transmission control protocol/internet protocol (TCP/IP)-based attacks, DoS, and other existing cyber threats.

Moreover, this research study is motivated by the increasing number of cyberattacks whether globally or on a national scale. Globally, one of the noteworthy cyberattacks was that on the Ukrainian power grid in December 2015. Here the hacker accessed the SCADA information, disrupted the normal operation, and caused the disconnection of thirty (30) substations in total, affecting 225,000 customers for approximately three (3) hours (Ashraf, 2021). The hackers temporarily degraded the power grid with a new malware type known as BlackEnergy. This hacking behaviour was then repeated in December 2016. Such provided a wakeup call for public and private sector entities (Lawrence, 2018). Nationally, in 2019, South Africa's critical infrastructure, City Power, which supplies South Africa's largest city, Johannesburg, suffered a ransomware attack that left residents in the dark (News24, 2019).

In addition to this, more South African companies, namely, Transnet, Momentum Metropolitan, Tracker SA, Nedbank, and Telkom SA, among many others have fallen victim to cyberattacks of recent months. Cyberattacks such as Stuxnet, Aurora, and Maroochy on the SCADA systems give us clear insight into the damage a determined adversary can cause to any country's security, economy, and healthcare systems. The Smart Grid is essential for critical infrastructure protection because of the type of service it provides to the nation.

1.3. Problem Statement

Smart Grid, which has been classified as critical infrastructure, comprises infrastructure and devices spread over a large geographical area. The central

control of the Smart Grid systems is governed through SCADA. The Smart Grid SCADA systems are connected to the internet to support geographical remote access. Many vendors use TCP/IP to transport SCADA messages. Such exposes the Smart Grid SCADA system to TCP/IP-based cyberattacks, such as password sniffing, traffic redirection, authentication, as well as DoS attacks. The protection of Smart Grid SCADA devices communicating over the network remains a major concern. Failure to protect this communication can lead to a cyberattack and a loss of critical infrastructure. A successful cyberattack on the Smart Grid SCADA system can result in the attacker causing cascading failures, load-shedding or a complete blackout (Ashraf et al., 2021; Feng et al., 2020).

Cybersecurity is one of the key concerns for Smart Grid. Thus for the country's critical infrastructure, this research study proposes an ECS algorithm that protects the grid, and prevent malicious users from gaining unauthorized access to the Smart Grid network during data transmission. To successfully protect the Smart Grid SCADA system from cyberattacks, three cybersecurity objectives must be achieved: availability, integrity, and confidentiality (NIST US Departments, 2012). Previous studies addressed these objectives separately; however, this study will be addressing all cybersecurity objectives, respectively.

Furthermore, control system malwares such as Stuxnet, Aurora, Maroochy, and BlackEnergy are used to attack the vulnerable Smart Grid SCADA systems. If cyber security is not correctly implemented, it places the critical infrastructure at risk. If an adversary manages to infiltrate the Smart Grid SCADA system, they can take control of the entire system operations and stop the supply of electricity. Such will cause damage to the entire country as it will affect our healthcare systems: people could die in hospitals. This situation will affect our country's security; it will cripple businesses, and result in financial loss to our economy. Therefore, it is important to protect the Smart Grid SCADA system from cyberattacks − we rely on electricity, and need it to operate as a country (Das, 2021; Mera et al., 2020).

1.4. Research Examination/Questions

The main question of this study: How does one develop an enhanced cybersecurity algorithm to improve and strengthen cybersecurity for the Smart Grid SCADA system?

The following sub-questions were used to provide in-depth understanding of various designed cybersecurity algorithms. Below are the sub-questions:

1. What are the existing cybersecurity algorithms used to protect the Smart Grid SCADA system?
2. How can the proposed ECS algorithm for protecting the Smart Grid SCADA system be designed by integrating the NTRU and the Toom-Cook algorithms to achieve secure end-to-end authentication, data integrity, confidentiality, and availability, while reducing complexity?
3. How can the proposed ECS algorithm be implemented to achieve secure end-to-end authentication, data integrity, confidentiality, and availability while reducing complexity?
4. How will the effectiveness of the ECS algorithm for protecting the Smart Grid SCADA system be measured?

1.5. Research Aim and Objectives

The main aim of the study: The main aim of the study is to develop an enhanced cybersecurity algorithm that will improve and strengthen cybersecurity for the Smart Grid SCADA system. The following are the sub-objectives of this study:

1. To identify existing cybersecurity algorithms used to protect the Smart Grid SCADA system.
2. To design an ECS algorithm for the Smart Grid SCADA system by integrating the NTRU and the Toom-Cook algorithms to achieve secure end-to-end authentication, data integrity, confidentiality, and availability, while reducing complexity.

3. To implement the proposed ECS algorithm in order to achieve secure end-to-end authentication, data integrity, confidentiality, and availability while reducing complexity.
4. To measure the effectiveness of the proposed ECS algorithm for protecting the Smart Grid SCADA system.

1.6. Significance and Benefits of the Study

The study will benefit the country as well as utility service providers and researchers who are interested in developing cybersecurity algorithms for the Smart Grid SCADA system.
The four (4) areas of benefit in this research study are:

1. To protect critical infrastructure by designing an ECS algorithm that prevents malicious users from gaining unauthorised access to the Smart Grid SCADA network.
2. To prevent DoS attacks on the Smart Grid system targeting availability which can lead to a blackout.
3. The study will also benefit utility service providers who are interested in evolving or are currently using the Smart Grid, as it can assist in efficiently and correctly implementing cybersecurity requirements and objectives for the Smart Grid.
4. The study can also be used as a learning curve for people interested in designing cybersecurity algorithms for the Smart Grid SCADA system.

1.7. Research Methodology

The study seeks to develop an enhanced cybersecurity algorithm to protect the Smart Grid. To provide answers to the research questions, an experimental methodology was applied, with the following methods discussed below:

1.7.1 Literature review

The data collected will help us understand the views of various scholars and authors in the field of the Smart Grid SCADA system, the importance of secure communication during data transmission, as well as cybersecurity algorithms and methodologies followed when solving the identified problem. Journals, conference papers, technical reviews, tutorials, and other internet sources will also be used as sources for the review of literature.

1.7.2 Modelling

The conceptual model consists of a set of components: the objectives, inputs, outputs, content, assumptions, and simplifications of the model. Therefore, the ECS algorithm will be designed and developed using a conceptual model. This will be achieved by effectively integrating existing algorithms.

1.7.3 Implementation

After the proposed ECS algorithm has been designed, a code/programme will be written so that the performance and effectiveness of the proposed solution can be evaluated.

1.7.4 Experimentation/Simulation

The effectiveness of the proposed solution was measured using the network simulator version 2 (NS-2) tool. NS-2 is a powerful simulation tool used for various aspects such as to test, analyse, and evaluate the performance of a new algorithm or new protocol, comparing the new algorithm with the existing algorithms.

Table I: Research Questions, Research Objectives, and Research Methodologies

Research Questions	**Research Objectives**	**Research Methodology**
What are the existing cybersecurity algorithms used for the Smart Grid?	To identify existing cybersecurity algorithms used for the Smart Grid.	Literature Review
How can the proposed ECS algorithm for protecting the Smart Grid SCADA system be designed by integrating the NTRU with the Toom-Cook algorithm to achieve secure end-to-end authentication, data integrity, confidentiality, and availability while reducing complexity?	To design an ECS algorithm for the Smart Grid SCADA system by integrating the NTRU with the Toom-Cook algorithm to achieve secure end-to-end authentication, data integrity, confidentiality, and availability, while reducing complexity.	Modelling
How can the proposed ECS algorithm be implemented to achieve secure end-to-end authentication, data integrity, confidentiality, and availability while reducing complexity?	To implement the proposed ECS algorithm in order to achieve secure end-to-end authentication, data integrity, confidentiality, and availability, while reducing complexity.	Implementation
How does one measure the effectiveness of the enhanced cybersecurity algorithm for protecting the Smart Grid?	To measure the effectiveness of the enhanced cybersecurity algorithm for protecting the Smart Grid.	Simulation

1.8 Expected Results

The expected results of the study include the following:

1. An ECS algorithm was designed by integrating the NTRU algorithm with the Toom-Cook algorithm to improve and strengthen cybersecurity for the Smart Grid SCADA System.
2. Publications, i.e., in conference proceedings and journals.
3. A compiled summary of the report in the form of a thesis.

1.9 Contributions of the Study

The contributions of the study are:

1. The proposed ECS algorithm ensures that the cybersecurity objectives for the Smart Grid which are confidentiality, integrity, and availability, are correctly implemented and achieved.
2. The integration of the NTRU algorithm with the Toom-Cook algorithm ensured that the proposed ECS algorithm provided secure end-to-end authentication and reduced complexity by improving the efficiency of the encryption and decryption techniques.
3. The proposed ECS algorithm is sufficient and quick to detect malicious activities within the network, as a result, preventing cyberattackers from modification attacks, data-integrity attacks, and from gaining unauthorized access to the Smart Grid SCADA network.

1.10 Organization of the Thesis

The remainder of this thesis is organized as follows: In Chapter 2, the research study presents the review of literature and an overview of the Smart Grid, SCADA, cybersecurity requirements, and a brief understanding of the various types of attack on the SCADA networks, as well as a worldwide history of major hacking attacks on the electric power grid. Furthermore, the study presents related works of various existing cybersecurity algorithms used to

protect and secure the Smart Grid. In Chapter 3, the research study describes and presents the design of the proposed enhanced cybersecurity algorithm. In Chapter 4, the system implementation of the enhanced cybersecurity algorithm is presented. Furthermore, the chapter also outlines the experimental set-up and the technologies used to implement the proposed cybersecurity algorithm. In Chapter 5, the research study presents the evaluated results. Lastly, in Chapter 6, the research study provides a conclusion and suggestions for future work.

1.11 Summary

In this chapter, the background of the Smart Grid is explained as well as how the evolution from the traditional power grid and dependence on SCADA introduces the Smart Grid to new cyber risks and cyberattacks. Furthermore, examples of the power grid that have been successfully attacked are highlighted to emphasise the importance of protecting critical infrastructure. To support the proposed enhanced cybersecurity algorithm, a set of four research questions has been identified and defined, which the dissertation answers as per the objectives. An experimental methodology was applied to achieve the set of four research objectives. The next chapter presents the literature review and related work of the research study.

Chapter 2: Literature Review

2.1. Introduction

Smart Grid systems are heavily dependent on Information and Communication Technologies. For that reason Smart Grids are more prone to cyberattacks, unlike traditional power grid automation systems isolated from the corporate networks. Furthermore, Smart Grid relies on SCADA systems for the automated control and monitoring of the Smart Grid. The usage of public networks, cloud computing, wireless communication, and social engineering on SCADA networks increases the vulnerability of the Smart Grid to cyber-risks, cyber-threats, and cyberattacks. These risks and threats have prompted research studies focusing on various privacy and cybersecurity issues. Methods, models, and techniques have been developed to improve Smart Grid security and resilience by reducing the cybersecurity risks and threats (Caldereo et al., 2016). Moreover, the continuous and repeated cyberattacks on the critical infrastructure demonstrate a need for improved cybersecurity for the Smart Grid.

Chapter 2 is structured as follows: In Section 2.2 the research provides an overview of cybersecurity, together with the objectives that must be met when implementing cybersecurity for the Smart Grid. The chapter lists South Africa's Information Security Acts and Regulations and a number of Smart Grid standards to be followed during the design and implementation of a secure Smart Grid. Section 2.3 provides an overview of a Smart Grid, including the logical architecture of the Smart Grid, definitions of the various actors within the Smart Grid domain, as well as network components used within the Smart Grid. Section 2.4 provides an overview of SCADA. The chapter elaborates the importance of integrating SCADA into the Smart Grid; and how that integration increases cybersecurity vulnerabilities for the Smart Grid. The main focus is still on the SCADA system. The research paper furthermore outlines the SCADA technical components, showing how that equipment is connected and operated on the Smart Grid. Furthermore, it discusses how their interconnection to the public network exposes the Smart Grid to cyberattacks.

Section 2.5 identifies the various types of Smart Grid SCADA attacks. Section 2.6 illustrates and demonstrates a broader underlining of the growing trends of cyberattacks on the critical infrastructure. The chapter provides a history of major attacks across the world, and a recently reported cyberattack in South Africa in the form of ransomware. Section 2.7 discusses the existing cybersecurity algorithm used for protecting the Smart Grid SCADA system, which is one of the objectives of this paper. Section 2.8 then outlines the related work, thereafter the gaps found in these existing solutions.

2.2 Overview of Cybersecurity

Cybersecurity refers to the technique of protecting computers, networks, programmes, and data from unauthorized access or attack aimed at malicious intent. According to NISTIR (2014), each organization's cybersecurity requirements should evolve as technology advances, threats to the Smart Grid inevitably multiplying and diversifying. The traditional grid has evolved to a Smart Grid: continuous research must therefore be conducted to develop solutions that will meet all three (3) cybersecurity objectives.

2.2.1 Cybersecurity objectives

In order to identify cybersecurity objectives, we use a CIA triad model which stands for: confidentiality, integrity, and availability. The CIA triad model is a widely used model that guides organization's efforts toward securing its data. The priority level differs slightly when it comes to security for operational technology (OT) versus Information Technology (IT) security. In a Smart Grid network, availability is most critical for power system reliability, while confidentiality is the least necessary for power system reliability. The table below illustrates the various priority levels for OT and IT networks (NIST, 2012).

Table II: CIA Triad Model Cybersecurity Priority Levels for OT vs IT (NIST, 2012)

Priority	**OT**	**IT**
1	Availability	Confidentiality

2	Integrity	Integrity
3	Confidentiality	Availability

2.2.1.1 Availability

Availability implies that information should be consistently and readily accessible to authorized parties. It also refers to ensuring timely and reliable access to and use of information. Data availability involves preventing DoS attacks that lead to blackouts. Some cybersecurity measures for mitigating threats to data availability as identified by Smart Eye Technology (2020) include:

a) off-site backups
b) disaster recovery
c) redundancy
d) failover
e) proper monitoring
f) environmental controls
g) virtualization
h) server clustering
i) continuity of operations planning

2.2.1.2 Integrity

Integrity refers to data that has not been changed, destroyed, or lost in a malicious or accidental manner. Some cybersecurity controls designed to maintain the integrity of information as identified by Smart Eye Technology, (2020) include:

a) user access controls
b) version control
c) backup and recovery procedures
d) error-detection software

2.2.1.3 Confidentiality

Confidentiality is the protection of data or information from unauthorized access, preserving authorized restrictions on information access and disclosure, including means of protecting personal privacy and proprietary information. Some cybersecurity control to keep your data confidential as identified by Smart Eye Technology, (2020) include:

a) encryption

b) password

c) two-factor authentication

d) biometric verification

2.2.2 Cybersecurity standards and guidelines

Cybersecurity standards are a collection of best practices created by experts to protect organizations from cyber-threats and to improve their cybersecurity stance. Some of the cybersecurity standards/regulations that can be implemented within organizations as guidance and best practices in securing the Smart Grid include:

a) International Organization for Standardization (ISO) ISO/IEC27001

ISO/IEC27001 is an international standard that has been prepared to provide requirements for establishing, implementing, maintaining, and continually improving on an information security-management system. The adoption of such a system is a strategic decision for any organization. The establishment and implementation of an organization's information security management system is influenced by the organization's needs and objectives, security requirements, the organizational processes used, and the size and structure of the organization. All of these influencing factors are expected to change over time. The information-security management system preserves the confidentiality, integrity, and availability of information by applying a risk-management process; affording confidence to interested parties that risks are being adequately managed (ISO/IEC27001, 2013).

b) NIST (National Institute of Standards and Technology Interagency Report) 7628 Revision 1 - Guidelines for Smart Grid Cybersecurity

The initial version and this revision of the guidelines for smart grid cybersecurity were developed as a consensus document by the cyber security working group (CSWG) of the Smart Grid Interoperability Panel (SGIP), a public-private partnership launched by the NIST in November 2009. This three-volume report, Guidelines for Smart Grid Cybersecurity, presents an analytical framework that organizations can use to develop effective cybersecurity strategies tailored to their particular combinations of smart grid-related characteristics, risks, and vulnerabilities. Organizations in the diverse community of smart grid stakeholders from utilities to providers of energy-management services to manufacturers of electric vehicles and charging stations can use the methods and supporting information presented in this report. Information is offered as guidance for assessing risk and identifying and applying appropriate security requirements. This approach recognizes that the electric grid is changing from a closed system to a complex, highly interconnected environment (NISTIR, 2014).

c) ANSI/ISA-99.02.01–2009 Security for Industrial Automation and Control According to ANSI/ISA–99.02.01–2009: this standard defines the elements necessary for establishing a cybersecurity management system (CSMS) for industrial automation and control systems (IACS), providing guidance on how to develop those elements. According to the International Society of Information (ISI), this standard is part of a multipart series that addresses the issue of security for industrial automation and control systems. It has been developed by Working Group 2 of the ISA99 committee. The standard also describes the elements contained in a cybersecurity management system for use in the industrial automation and control systems environment. The standard provides guidance on how to meet the requirements described for each element. This standard has been developed in large part from a previous technical report produced by the ISA99 committee, ISA –

TR99.00.02–2004, Integrating Electronic Security into the Manufacturing and Control Systems Environment.

d) Cybercrime Act 19 of 2020 – South African Government

The Government Gazette Republic of South Africa, 44651 (2021) states that in South Africa, the Cybercrimes Act 19 of 2020 aims to criminalise and penalise cybercrimes. The Act has created twenty cybercrime offences including illegal access to a computer or data-storage device, unlawful acquisition of data, online forgery, extortion, or fraud and theft of incorporeal property. The Act is the overarching legal authority on the regulation, investigation, and criminalisation of cybercrimes. The new Act also prescribes penalties related to cybercrime. The Act gives the South African Police Service the authority not only to investigate, search, access, and seize, but to also cooperate with foreign states in investigating cybercrimes.

Cybersecurity concerns and challenges that emanate from the evolution of the traditional electric grid to a Smart Grid are of great concern, the Smart Grid having been classified a critical infrastructure. It is therefore imperative that any country protect its critical infrastructure. At present, cybersecurity concerns are evident in all nations, the exact nature of the threats differing from country to country, region to region. Therefore, there is a need to assess the threats and impacts for specific countries that have implemented best practices. Such practices will safeguard its critical infrastructure most securely; in this case, by means of the Smart Grid.

2.3 Overview of the Smart Grid

A Smart Grid is an electricity network that uses digital and other advanced technologies to monitor and manage the transporting of electricity from all generation sources to meet the varying electricity demands of end users.

2.3.1 Logical architecture of the Smart Grid

The architecture and interface of a smart grid provide a logical understanding of the ways in which different domains interact within the Smart Grid. The NIST identifies the seven domains within the Smart Grid as: service providers,

customers, transmission, distribution, bulk generation, markets, and operations. Below is a diagram that presents the logical reference model of the Smart Grid.

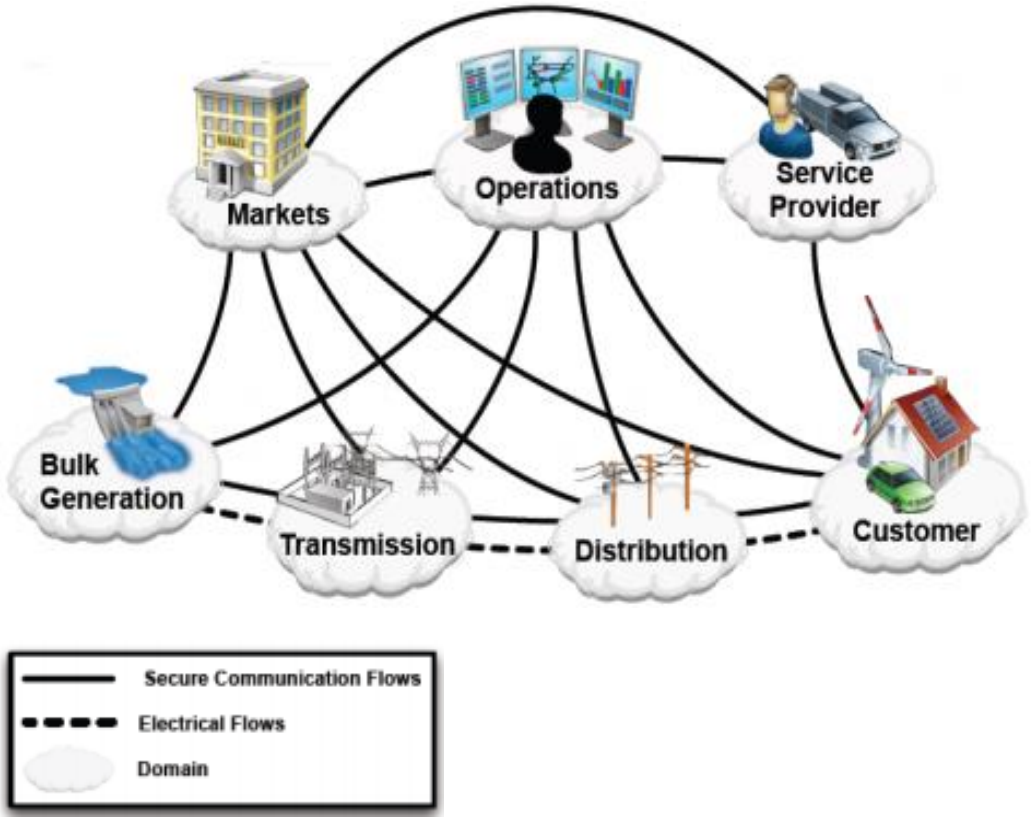

Figure 2.1: Interaction of actors in the various smart grid domains through secure communication flow (NIST US Departments, 2012).

Table III below provides a composite high-level definition for the various actors interacting within the Smart Grid.

Table III: Actors within each of the smart grid domains (NIST US Departments, 2012)

Actors in the Domain	**Definition of Actors in the Domain**
Operations	The proper operation of the power system is monitored – these are managers of the flow of electricity.
Service Provider	This is an organization that provides services pertaining to the

Actors in the Domain	Definition of Actors in the Domain
	establishment and secure operations of smart grids, as per the requirements of the consumer and utilities.
Customer	This is where the electricity is consumed by the end users. The sub-category includes both domestic and large consumers, such as commercial and industrial loads. Actors can generate, manage, and store the electricity.
Distribution	Here distributed generation, distributed storage, transmission, and consumers interact. Actors are entities that distribute electricity to and from customers.
Transmission	This is where the bulk power is transferred from generation centres to distribution. Actors are the carriers of electricity, and may also generate and store electricity.
Bulk Generation	Here the delivery of bulk electricity to consumers starts; actors are the generators of electricity in bulk quantities; energy can also be restored for later distribution.
Markets	Here the assets are exchanged. The operator and the participants are the

Actors in the Domain	Definition of Actors in the Domain
	actors in the electricity markets.

2.3.2 Smart Grid network components

Smart Grid has incorporated two types of network, namely, the home area network (HAN) and the wide area network (WAN), as exemplified in Figure 2.2.

a) A HAN connects all the home's in-house smart devices to the smart meter. The HAN can communicate using Zigbee, wired or wireless Ethernet, or Bluetooth. HANs are also used in residential homes, business area networks (BANs), while industrial area networks (IANs) are used within business offices and industrial sites, respectively (Aloul et al., 2015).

b) A WAN, on the other hand, is a larger network that connects smart meters, service providers, and electric utilities. The WAN can communicate using WiMAX, 3G/GSM/LTE, or fibre optics. The smart meter acts as a gateway between the in-house devices and the external parties to provide the needed information. The electric utility manages the power distribution within the smart grid, collects sub-hourly power usage from smart meters, and sends notifications to smart meters once required. The smart meter receives messages from devices within HAN and sends them to the appropriate service provider, respectively (Aloul et al., 2015).

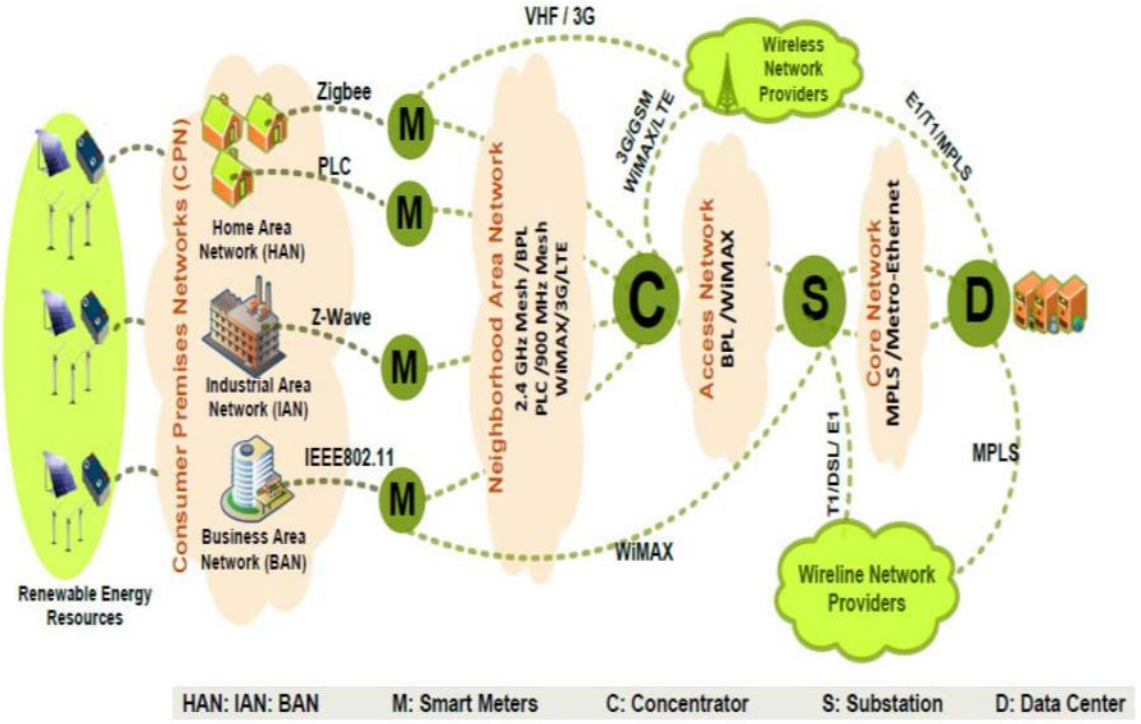

Figure 2.2: Smart Grid basic network architecture (Aloul et al., 2015).

Some of the benefits of such a modernized electricity network include the ability to reduce power consumption on the consumer side during peak hours. This is known as demand-side management; enabling grid connection of distributed generation power (with photovoltaic arrays, small wind turbines, micro-hydro, or even combined heat power generators in buildings); incorporating grid energy storage for distributed generation load balancing; and eliminating failures such as widespread power grid cascading failures (Vijayapriya et al., 2011).

Furthermore, Sayed et al. (2017) indicate that one of the considerations in designing the capabilities of the Smart Grid is the integration of SCADA systems to allow the utility to remotely monitor, supervise, and control the electric network equipments as a means of fulfilling reliability and desire efficiencies for the whole utility. Given the ability of these systems to control the flow of electricity throughout the network, additional planning and forethought are required to ensure that all measures for preventing compromise are considered.

2.4 Importance of the SCADA System to the Smart Grid

The SCADA system is a crucial component for automated control and monitoring of the Smart Grid. According to Wang (2012), without a secure SCADA system it is impossible to deploy the intelligent Smart Grid system because control systems are computer-based systems used within many critical systems to monitor and control sensitive processes and physical functions. In order to deploy the Smart Grid system, there is a trend towards interconnecting SCADA systems and data networks (e.g., the Intranet). Furthermore, the SCADA empowers the consumer by interconnecting energy-management systems to enable the customer to manage their own energy use and to control costs. Use of the SCADA allows the grid to be self-healing by responding automatically and instantly to outages, power quality issues, and system problems (see Figure 2.3) (Cardwell et al., 2013).

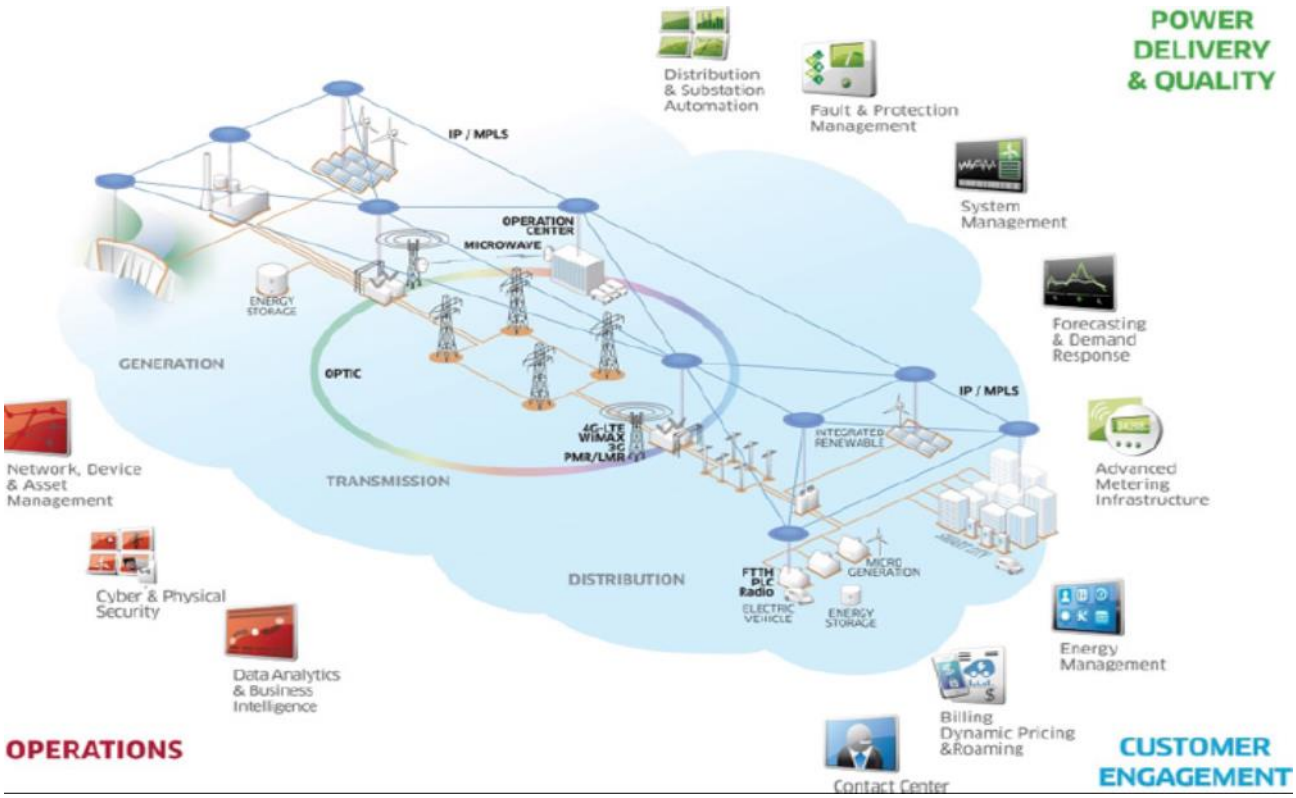

Figure 2.3: SCADA/Smart Grid integration (Source: http://www2.alcatel-lucent.com)

2.4.1 Technical Components of SCADA

Gervasi (2010) described SCADA systems by means of the following components:

2.4.1.1 Operating equipment: this includes pumps, valves, conveyors and substation breakers that can be controlled by energizing actuators or relays.

2.4.1.2 Local processors: this includes the programmable logic controller (PLC), remote terminal unit (RTU), intelligent electronic device (IED), and process automation controller (PAC).

a) Programmable Logic Controller (PLC)

   The PLC is a small industrial computer originally designed to perform the logic functions executed by electrical hardware (relays, drum switches, and mechanical timers/counters). PLCs have evolved into controllers capable of controlling complex processes; and therefore are used in SCADA systems and DCSs. Other controllers used at the field level are process controllers and RTUs; these provide the same control as PLCs but are designed for specific control applications. In SCADA environments, PLCs are often used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs (Falco et al., 2006).

b) Remote Terminal Unit (RTU)

   The RTU, also called a remote telemetry unit, is a special-purpose data-acquisition and control unit designed to support SCADA remote stations. RTUs are field devices often equipped with wireless radio interfaces to support remote situations when wire-based communications are unavailable. Sometimes PLCs are implemented as field devices to serve as RTUs (Falco et al., 2016).

c) Intelligent Electronic Device (IED)

An IED is a “smart” sensor/actuator containing the intelligence required to acquire data, communicate with other devices, and perform local processing and control. An IED could combine an analogue input sensor, analogue output, low-level control capabilities, a communication system, and programme memory in one device. The use of IEDs in the SCADA and DCS systems allows for automatic control at the local level (Falco et al., 2006).

d) Process automation controller (PAC)

2.4.1.3 Instruments: in the field or in a facility that senses conditions such as pH, temperature, pressure, power level, and flow rate

2.4.1.4 Communication devices: this includes both long-range and short-range communication.

a) Short-range communications are installed between local RTUs, instruments, and operating equipment. These short-distance cables or wireless connections carry digital and analogue signals using electrical properties such as voltage and current; or using other settled industrial communications protocols.

b) Long-range communications are installed between local processors RTU/PLC and host servers. This communication typically uses methods such as leased telephone lines, microwaves, satellites, frame relay networks, and cellular packet data.

2.4.1.5 Host computers: act as the central point of monitoring and control. Using a host computer a human operator can supervise the process, while receiving alarms, reviewing data, and exercising control.

Shahzad et al. (2014) describe the SCADA system as a combination of hardware components and software programmes in which hardware includes a RTU, “Master Terminal Unit (MTU)”, actuators and sensors; and software

includes “Human Machine Interface (HMI)”, a central database (Historian) and other user software.

a) Master Terminal Unit (MTU): The master terminal unit or master station unit (MTU/MSU) is the control centre of a SCADA network. Sub-MSU or Sub-MTU acts as a sub-control centre (Ghosh et al., 2019).

b) Actuators and sensors: Sensors and actuators often work in tandem; however, they are devices functioning contrarily. A sensor monitors conditions, signalling when changes occur. An actuator receives a signal and performs an action, often in the form of a movement in a mechanical machine. Another key difference is their location within the system.

c) Human Machine Interface (HMI): The HMI is a user interface that connects a person to a device. It is used to visualize data, and monitor production time, machine inputs, and outputs (Ghosh et al., 2019).

d) A central database (Historian): The data historian is a centralized database for logging all process information within an ICS. Information stored in this database can be accessed to support various analyses, from statistical process control to enterprise-level planning (Falco et al., 2006).

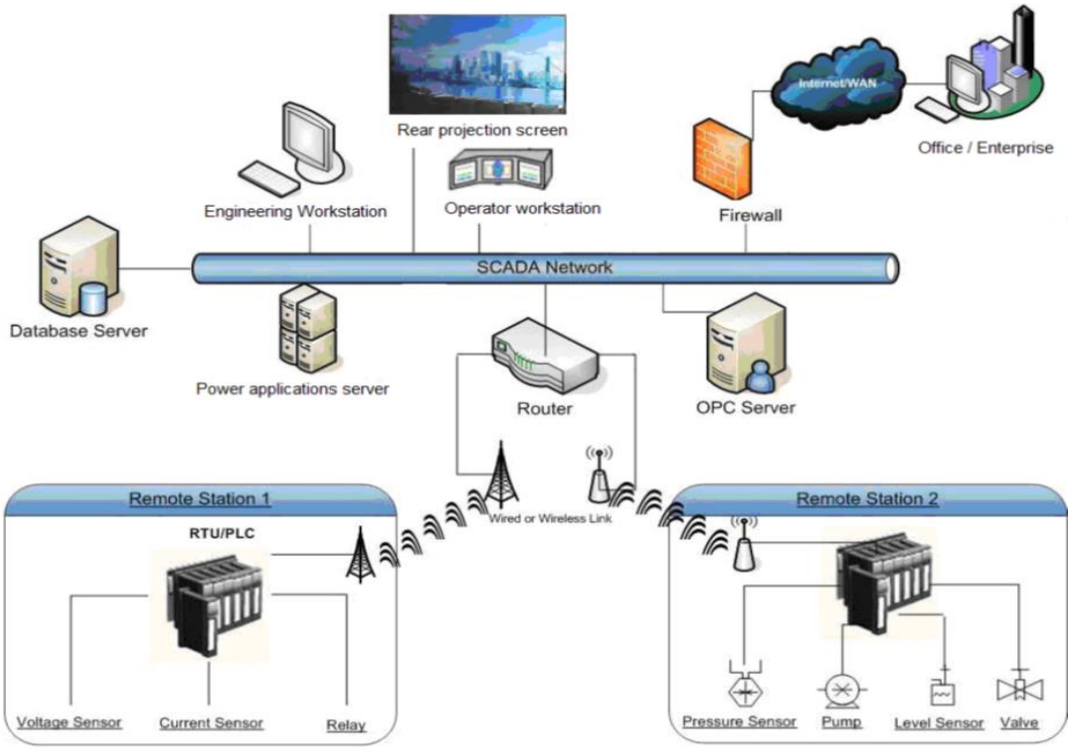

Figure 2.4: SCADA system network (Sayed et al., 2017)

In order to understand the relations between the devices, Yadava et al. (2022) explain that:

a) this user software provides a communication interface between hardware and software.

b) the physical environment is directly connected to the actuators and sensors. The sensors and actuators forward the collected data to RTUs. RTUs gather the data and information from the sensors, forwarding telemetry data to the MTU for monitoring and for controlling the SCADA framework. The MTU data is visualized on the HMI interface. Based on the analysis of data, appropriate actions are transmitted to actuators along the reverse path.

2.5 Types of Attack in the Smart Grid SCADA System

Table IV: Standard Attacks on Smart Grid SCADA N etworks (Ghosh et al., 2019)

Attack	Description of attack	How the attack can be launched	Some tools that can be engaged to launch the attack
Eavesdrop	These are of two types: passive eavesdropping & active eavesdropping	The communication network can be either wired or wireless. By accessing the network between the MTU and sub-MTUSs or RTU, the invader can instal eavesdropping equipment in the network	Wireshark, tcpdump and dsniff
MITM	This occurs when the attacker is in between two units, fetching the private information. The most common MITM attacks are the following: session hijacking network server, IP spoofing and replay attacks.	In an MiM attack, the intruder monitors the traffic and injects abnormal data during transmission, sending it to the receiver. In the case of a successful session hijacking and IP spoofing, the intruder takes over the session and maintains the connection. The spoofing helps the attacker to go undetected.	Ettercap, SSLStrip and Evilgrade
Masquerade	The attacker uses a fake identity, pretending to be a legitimate user and stealing	By launching IP spoofing and a brute force password attack, the malicious user can use the stolen password and can	Ettercap, Arpspoof, and Brutus

Attack	Description of attack	How the attack can be launched	Some tools that can be engaged to launch the attack
	information from the system or network	login to gain unauthorized access to a system or network.	
Virus and worms	Virus and worms are types of malware. A malware is a malicious software or programme that corrupts the data stored in the computer. Such can also lead to distributed denial of service attack	The intruder can send a file containing the malicious code to the MTU after launching an MITM or masquerade attack. For example, the virus or worm can spread through sending email attachments, web links, and peer-to-peer file-sharing networks.	Any malicious code which is self-replicable and attached to an .exe file in the device
Trojan horse	A type of malicious programme disguised as a harmless file. However, unlike a virus, a Trojan horse is not self-replicable. Therefore, hackers use social engineering tactics to transfer this type of virus	After launching IP spoofing or social engineering, the intruder can inject innocent-looking malicious and executable code and send it as a web link or a free download to the target system. Thus, the hacker can gain access to the control system, hacking it.	Social engineering. For example, Web links offering a free software download
Denial of	DoS attacks the	An RTU infected by virus	Slowloris,

Attack	Description of attack	How the attack can be launched	Some tools that can be engaged to launch the attack
Service (DoS)	availability requirement of a network. This is the type of attack in which a legitimate user is denied access to a resource	or worm can send random IP packets to the MTU and thus consume network bandwidth. This may further lead to resource starvation.	GoldenEye for an operating system, Kali Linux Low Orbit Ion Cannon (LOIC)
Fragmentation	A type of DoS attack that leads to the unavailability of resources	This involves sending over-sized datagrams. In this type of attack, the sizes of the sent datagrams are greater than the network's maximum transmission unit.	Tools used to launch DoS attacks can be used to launch fragmentation attacks.
Cinderella	The objective of this attack is to cause the security software license to expire	The hacker disguises their ID as a legitimate user and gains access to the system by using a brute-force attack. Then the internal network clock is changed to cause the security software to expire prematurely, thus increasing the network vulnerability. Attackers can use tools to launch masquerade and brute-force attacks	For example: - Ettercap for Masquerade attacks - Ncrack, Hydra, and Hashcat for Brute-force attack

Attack	Description of attack	How the attack can be launched	Some tools that can be engaged to launch the attack
Doorknob rattling	This is the type of attack in which the failed attempts of a brute-force remain hidden from the detection system of the network	At first, the attackers will launch a masquerade attack. Then they will repeatedly attempt a random combination of username and password on different devices to gain access. This leads to a few failed attempts. Should the failed attempts go undetected, this kind of attack can be successful.	- Ettercap for Masquerade attacks - Ncrack, Hydra, and Hashcat for Brute-force attack

2.5.1 Types of attack in the Smart Grid SCADA wireless networks

The usage of internet connectivity, cloud computing, wireless communications, and social engineering on the SCADA networks has made its architecture vulnerable (Kang et al., 2009). One of the main reasons for the vulnerabilities in the SCADA is the lack of strong encryption and real-time monitoring. Attacks can occur at all layers from the supervisory level to the field instrumentation level. Zhu (2011) identifies these attacks as follows:

a) Attack on hardware:

This is a scenario in which the hacker gains unauthenticated access to the units, and tampers with them or their functions. The primary challenge in securing hardware is access control, for example, the doorknob-rattling attack (Zhu et al., 2011). Furthermore, Yadav et al. (2022) attest to most components of the SCADA systems, i.e., HMI, PLC, network, RTU, and MTU, being proprietary. Data communication in SCADA systems uses various communication protocols, i.e.,

Modbus, DNP3, Profibus, etc. CVE-2014-2343, CVE-2014-2342, CVE-2017-9963, CVE-2017-7969, and many more CVE are reported in the communication network. Most of the vulnerabilities can be easily exploited via the remote network.

1. Approximately 83 % of the vulnerabilities are published on the network, which raises the alarm for network security.
2. Approximately 76 vulnerabilities were reported specific to HMI. In PLCs/ MTUs/ RTUs, legacy systems have mostly been used until now, applying unencrypted message passing. However, operating systems installed on PLCs/ MTUs/ and RTUs are not capable of implanting IDSs, firewalls, and antivirus tools which identify and prevent snooping on the network.
3. Approximately 65 vulnerabilities in the system firmware have been reported. Programmers usually do not consider security parameters while programming, which leaves many of SCADA's security entities vulnerable.

b) Attack on software

The SCADA system utilizes a variety of software to enhance its efficiency by fulfilling functional demands. However, owing to poor implementation, the system is vulnerable to SQL injection, the Trojan horse, and buffer overflow. These are a few examples of attacks on software (Zhu et al., 2011). Furthermore, Ralston et al. (2007) remind that SCADA systems are operated on commercial Windows PCs, the primary target for attackers due to substantial vulnerabilities in their operating systems. Yadav et al. (2022) insist that the reported vulnerable components belong to seventy-seven (77) different vendors and manufacturers; with the largest reported vulnerability belonging to Siemens− fifty-five (55), and Schneider-electric − fifty-three (53). These vulnerabilities are also widely diversified. In short, the SCADA systems are more prone to vulnerabilities and attacks after being evolved to integrate with an internet-connected system. Most of the vulnerabilities

are targeted to HMI and communication networks, these systems being directly connected to the internet.

c) Attack on a network connection:

The attack on the communication stack can be either on the network layer, the transport layer, or the application layer. Figure 2.5 gives a classification of attacks based on the layers of the open systems interconnection (OSI) model, mapping them to the violation of security goals, namely, confidentiality, integrity, availability, and non-repudiation (Zhu et al., 2011). Furthermore, Yadav et al. (2022) indicate that most of the vulnerabilities are exploited via remote access. Network monitoring agents, which come configured by default access phrases that are available publicly, give easy access to the systems. The attacks on these systems are very sophisticated and complex. In Stuxnet, the attacker attacked the nuclear centrifuges via an air-gapped network. In the Maroochy attack, the attacker used the stolen wireless radio to control the SCADA systems. The major concern for the SCADA systems is external attacks. Approximately 89% of the vulnerabilities of the SCADA are exploited via the networks.

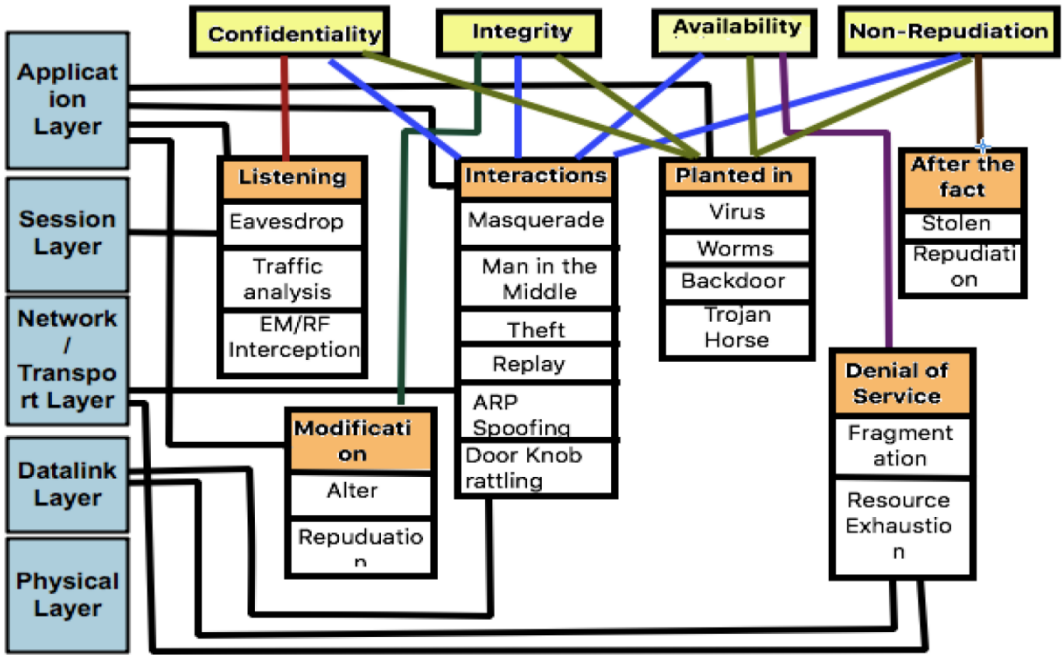

Figure 2.5: Classification of SCADA attacks in terms of security requirements and OSI layers (Ghosh et al., 2019)

According to Wang (2012), when moving the current energy distribution infrastructure towards a smart grid, we have to overcome the challenges of integrating network-based security solutions with automation systems. Such usually requires a combination of new and legacy components, and may not have sufficient reserved resources to perform security functionalities (Wang, 2012).

2.6 History of Major Hacking Attacks on the Electric Power Grid Worldwide

Cybersecurity is an emerging challenge for organizations across the world. The numerous cyberattacks on critical infrastructure have become a growing trend (see Figure 2.6).

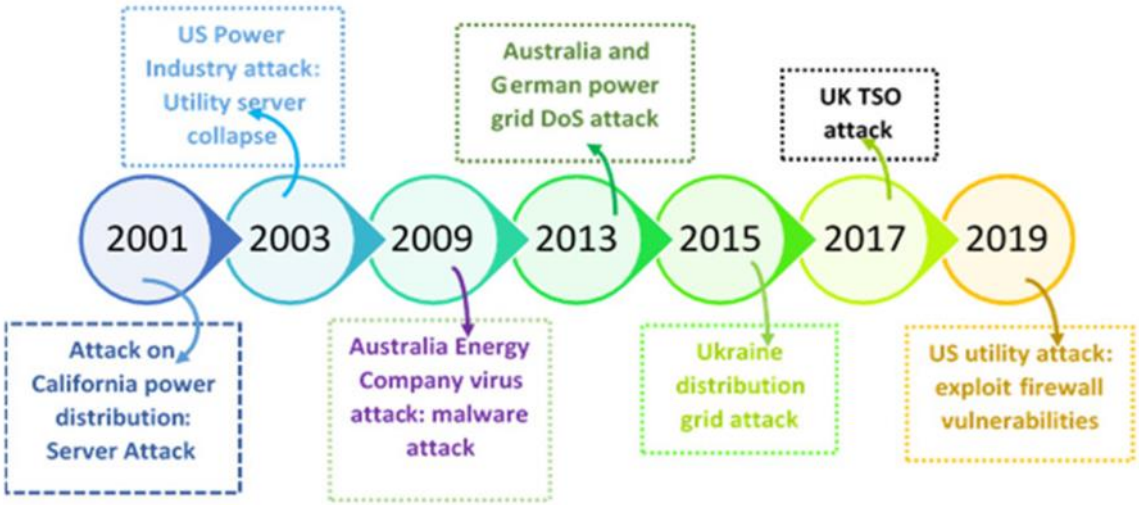

Figure 2.6: Major cyberattacks on the electric power grid (Ashraf et al., 2021)

In May 2014 in South Africa, it was reported that a public-sector cyberattack had occurred targeting state infrastructure in South Africa. Personal details of an estimated 16 000 whistle-blowers in the South African Police Services were hacked by a suspected member of the hacktivist group. The hackers then went on to post details online; stating that the attack was in response to the Marika shooting, in which miners were killed by the police during a strike (Roane, 2013).

On 09 September 2021, one of the most recent cyberattacks on the South African critical infrastructure was reported by News24. The Department of

Justice and Constitutional Development announced that its information technology system had been interrupted due to a security breach. The breach was achieved through ransomware. As a result, all electronic services provided by the department were affected, including issuing of letters of authority, bail services, emails, and the departmental website (News24, 2021).

2.7 Existing Cybersecurity Algorithm used for protecting the Smart Grid SCADA System

There are two types of cryptography algorithms, namely, the symmetric and the asymmetric algorithms. Symmetric algorithms include advanced encryption standard (AES), data encryption standard (DES), triple DES (3DES), and so forth. On the other hand, asymmetric algorithms include NTRU, RSA, ECC, Diffie–Hellman (DH), ELGAMAL algorithms, etc. According to Jamel et al. (2017), the major issue when implementing a symmetric key cryptography (SKC) in any type of network is the secure exchange of the various symmetric keys (*n* nodes require *n* (*n* - 1) / 2 keys). However, public key cryptography (PKC) overcomes this weakness because it provides a robust security model. The PKC can ensure secure authentication, confidentiality, integrity, and availability.

Table V: Comparison of Symmetric and Asymmetric Cryptosystems (Premnath, 2013)

Comparison Feature	Symmetric Cryptosystem	Asymmetric Cryptosystem
Key Management	Symmetric encryption uses only one key that all parties to the message exchange must know, so the key is the same on either side of the transmission. This complicates key management as it requires secure	Asymmetric encryption uses both a public and a private key. The owner holds the private key and never shares it with anyone. The public key is available to anyone to decrypt a message from the owner;

Comparison Feature	Symmetric Cryptosystem	Asymmetric Cryptosystem
	exchange and update of secret keys among the communication SCADA systems/devices	only the owner's private key can encrypt the message
Speed	Faster due to the simplicity of the algorithm	Relatively slower than symmetric algorithms
Key Length Requirement	Faster due to the simplicity of the algorithm	Requires longer key lengths to achieve a given level of security
Security risk	Risk is the disclosure of a key shared with an unauthorized entity	Less risky since the private key is not shared with anyone
Resource utilization	Requires constant computational resources regardless of key size	Requires more computational resources for long key size
Approved algorithm for SCADA system	AES, DES, 3DES	RSA, ECC, NTRU, DH

The only requirement for this study is to select the best public key cryptography scheme, and the optimak public key cryptosystem (PKCS) algorithm that will ensure secure end-to-end authentication, achieving the three (3) cybersecurity objectives, while reducing complexity.

A cryptosystem can be considered a suite of three algorithms applied for key generation, encryption, and decryption (Premnath, 2013). The two primary

cryptosystems used are symmetric and asymmetric, depending upon the nature of the keys used to encrypt a message. A study conducted by Jamel et al. (2017) and Rezai et al. (2017) proposed various PKCSs used for securing the Smart Grid SCADA system. Of all the various proposed algorithms, a study conducted by Feng et al. (2020), Loriya et al. (2017), Miri et al. (2017), Nitaj (2015), and Premnath (2013), proved that the three (3) best known algorithms used to protect the Smart Grid SACAD system are the RSA, the ECC, and the NTRU algorithms.

2.7.1 Public key cryptosystems

a) RSA algorithm

RSA is the first public key cryptosystem. The RSA algorithm comprises the initials of the surnames of developers Ron Rivest, Adi Shamir, and Leonard Adleman. Abood et al. (2018) assert that the RSA relies on numeral synthesis and employs two basic numbers to present both the public and private keys. Furthermore, according to Abood et al. (2018), the RSA provides excellent security and low speed; however, it is not flexible.

b) ECC algorithm

The ECC was developed by Neal Koblitz and Victor Miller. This algorithm provides the same level of security, but with smaller key sizes than the RSA. Abood et al. (2018) assure that the main advantage of ECC is that it utilizes small key lengths which results in quick encoding while consuming minimal energy. According to Abood et al. (2018), ECC provides excellent security and high speed; another added advantage is that is flexible.

c) NTRU algorithm

NTRU cryptosystems were developed by Joseph H. Silverman, Jeffrey Hoffstein, Jill Pipher, and Daniel Lieman. The NTRU algorithm is a combination of two (2) algorithms, NTRUEncrypt and NTRUSign. In 2009, the NTRU cryptosystem was approved for standardization by the Institute of Electrical and Electronics

Engineers (IEEE). The NTRU is one of the strongest and fastest public cryptosystems. It is also resistant to classic and quantum attacks (Nitaj, 2015).

2.7.2 RSA, ECC, NTRU with their mathematical problems

Cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. In PKC, *sk* and *pk* keys are mathematically related to the complex function *f*. It is very hard to gain a private key from the public key. In order to recover the *sk* to decrypt information, a mathematical problem P related to complex function f must be solved. The security of PKCS depends on the hardy of solving P. Table V shows the various mathematical complexity problems for RSA, ECC, and NTRU.

The PKCSs RSA and ECC are based on the complexity of number theoretic problems; their security is highly reliable in the distribution of prime numbers or based on the discrete logarithm problem on finite fields. The NTRU cryptosystem is based on geometrical problems (Jamel et al., 2017).

Table VI RSA, ECC, NTRU and their Mathematical Problems (Loriya et al., 2017).

Crypto system	Mathematical Problem	Description	Running times
RSA	Integer factorization	Given a number n, find its prime factors	Sub-exponential
ECC	Elliptic curve discrete logarithm	Given an elliptic curve E and points P and Q on E, find x such that Q = x.P	Sub-exponential
NTRU	Short vector	Based on hardness	Sub-exponential

	problem (geometrical problem)	of lattice problems	

Table V shows the sub-exponential complexity of the problem on which the RSA is considered hard to solve but not as hard as fully exponential solutions, such as ECC and NTRU. Because of this, ECC and NTRU can offer security levels similar to other PKCSs, but using shorter length keys, which require less space for key storage, and for time-saving when keys are transmitted. These characteristics make the ECC and the NTRU the best choice for securing devices with constrained resources (Loriya et al., 2017).

2.7.4 Advantage of using the NTRU over the RSA and ECC

The benefits of using the NTRU are listed below, demonstrating that it is the right choice for application in the SCADA environment (Premnath, 2013). The NTRU:

a) has been observed to be multiple times faster than both the RSA and the ECC.

b) consumes minimal resources including CPU and battery.

c) significantly reduces server resource utilization for large-scale deployments.

d) improves the data throughput (over RSA) when integrated with SSL

e) is ideal for low-power or hard-to-access environments, for embedded devices in which code size is a major limitation.

f) Resistant to quantum computing attacks.

2.8 Related Work

There has been a wide interest in the secure design and implementation of the Smart Grid. Thus, over the past years, several studies have been conducted on various protocols, security algorithms, and key management schemes to protect the Smart Grid. In this section, the previously proposed solutions are

discussed. The research study further outlines the gaps in these previously proposed solutions.

Das (2021) presents the following applicable algorithms to securing SCADA systems: the symmetric key, which includes AES, the triple data encryption algorithm (TDEA), or triple data encryption standard (TDES). The asymmetric key includes the digital signature standard (DSS), the digital signature algorithm (DSA), the RSA digital signature algorithm, and the elliptic curve digital signature algorithm (ECDSA). Lastly, the following standards were included: the secure hash algorithm (SHA) and the message digest algorithm. Because a smart grid network involves power generation, transmission, distribution, monitoring, and control, multicast provides the means for smart delivery of mass messages such as those needing delivery of power to a certain targeted load, or fast operation of a circuit breaker. Das (2021) furthermore presents the multicast application authentication methods as follows: secret-info asymmetry, time asymmetry, hybrid asymmetry, key management, public-key infrastructure (PKI), and symmetric key management. This is for authentication requirements to be met. Furthermore, the study compares the presented symmetric keys with asymmetric keys. The results obtained from the performance analyses prove that the asymmetric key algorithm uses lower power consumption and less computation. However, the limitation of these approved SCADA algorithms is that they only satisfy authentication: they do not guarantee data availability and confidentiality of the cybersecurity requirements.

Rezai et al. (2017) presented a review of the existing key-management schemes that have been used for securing SCADA networks. The key-management schemes presented are the symmetric and the asymmetric key-management schemes. The parameters used to evaluate the performance of these management schemes include storage cost, which relates to the number of required keys to be stored as well as total delay time, which denotes the sum of the message encryption/decryption time, group key set-up time, certificate verification time, and data transmission time. The obtained results proved that neither asymmetric nor symmetric key management alone

is sufficient for securing the SCADA network. Asymmetric key management alone is unsuitable in that some RTUs and IEDs lack the ability to utilize the PKC. Therefore, extensive research is still required to develop efficient hybrid asymmetric and symmetric key-management schemes/architectures. In addition to that, according to Rezai et al. (2017), other issues that still require extensive research efforts include: public-key infrastructures, cryptographic authority, and certificate management in the SCADA key-management scheme, finding vulnerabilities of the SCADA networks, distributed security mechanisms which meet the resource limitations of the SCADA networks, application of cloud security in the SCADA networks, lightweight cryptographic algorithms and protocols, and even some new hardware specifically designed for the SCADA networks, intrusion-detection systems (IDSs), access control, protocol vulnerability assessment, and firewalls.

Feng et al. (2020) proposed a new privacy protection scheme of NILM data based on a hybrid cipher algorithm to protect against threats of eavesdropping, tampering, and falsification of electro-data. In order to prevent hacker attacks, to protect the information security of data, and to maintain the interests and privacy of electricity consumers, the cryptography technology is widely used. This ensures that, even should the information be hijacked, useful information cannot be obtained by the hacker. To achieve this, three kinds of encryption algorithms, the AES, the RSA, and the HMAC-SHA1, were used in this scheme. The RSA algorithm protects the key of the AES algorithm; and the AES algorithm encrypts the users' large data. This it can not only realize the safe and convenient key management, but it can also ensure the speed of data encryption. In order to close the loopholes in key management of RSA, the public key being public to the outsider, the hash algorithm HMAC-SHA1 was introduced to guarantee the integrity of data transmission and the identity authentication of the sender. A test platform was established to test the various cryptography scenarios. The test platform was composed of a PC host computer and an MCU lower-machine hardware platform. The interface of the PC host computer was developed by Visual Studio 2017 and Qt5 tools, whose function was sending commands and receiving feedback information from the lower machine through the serial port.

The sending of commands included the following: a) encryption algorithm type; b) length of key; and c) electricity data. The received information was the required test performance of various algorithm modes running in MCU under the set conditions. The computing cost of RSA decryption and signature determined the computing cost of the total scheme (Feng et al., 2020). The effectiveness and efficiency of the hybrid cipher algorithm scheme was tested. The results obtained from the performance analysis proved that the requirements of data security and confidentiality were met. However, the security requirement of availability was not met.

Alese et al. (2012) prepared a comparative analysis of RSA, ECC encryption, and Menezes Vanstone Elliptic Curve Encryption (MVEC) algorithms. The test was performed on the Intel Pentium dual core 1.6GHZ machine running 512MB of RAM, the operating system being Windows Vista Home Basic. The study independently tested key generation, encryption, and decryption time. The parameters of the operations tested included: the size of the applied key; and the size and content of the key. Each operation for every test parameter was run 20 times. The performance results showed that the ECC has proved to involve much lower overheads than the RSA. The comparison revealed that ECC outperforms RSA at all key lengths and it can also create private/public keys pairs at a superior speed to the RSA. However, the study concluded that, although ECC has shown many advantages due to its ability to provide the same level of security as RSA using shorter keys, its drawback is its lack of maturity. Mathematicians believe that research has not yet been completed on ECDLP. Therefore, it was concluded in the study that the RSA is better than the ECC; being more reliable, its security more trustworthy.

Dawson et al. (2006) proposed the SKMA for secure SCADA communications. The architecture includes a proposed key-management protocol (SKMP). SKMA specifies the keys and mechanisms required to secure SCADA communications. The SKMP uses a series of existing security techniques to provide secure key management which only utilizes a symmetric cryptosystem for securing SCADA communication, thus simplifying implementation, and minimising overheads. Furthermore, the study compares the SKMA with the

SKE. The results obtained from the performance analyses prove that the SKMA has the following advantages over the SKE: firstly, the SKMA only uses symmetric techniques; thus simplifying implementation, and minimising overheads. Secondly, the SKMA only requires that long-term keys be stored on the node to which the key belongs, and to one other party, the key-distribution centre (KDC). This decreases the number of copies of each long-term key, minimising the risk of exposure, and simplifying recovery from the compromise of a master station. The SCADA systems mostly use broadcast communication. However, the protocol presented by Dawson et al. (2006) cannot provide such a mechanism; nor does it satisfy the confidentiality and integrity security requirements of a Smart Grid as regulated by the NIST.

Lim (2011) proposed an ID-based key management architecture taking its cue from a pairing algorithm based on elliptic curves. Bilinear pairings such as weil pairing and tate paring defined on elliptic curves have been used to construct efficient ID-based cryptosystems. The ID-KMA addresses the issues of public key cryptography per a digital signature. According to Lim (2011), the advantages of the ID-KMA include removal of the concept of the digital certificate, minimizing the overheads, fast session-key establishment and encryption, and efficient secret-key recovery. The ID-based key-management architecture uses four main keys − the emergency key (EK), the long-term key (LTK), the update key (UK), and the session key (SK). However, a study conducted by Castellanos (2017) indicates that all the aforementioned key-management protocols are based on traditional cryptography schemes which are vulnerable to quantum attacks. Furthermore, public-key algorithms tend to increase the computational and time costs (Premnath, 2013).

Shahzad et al. (2014) proposed a SCADA security mechanism, a security solution based on asymmetric and symmetric cryptography algorithms. The proposed security solution is for preventing and detecting SCADA communication attacks over the internet. Cryptography algorithms such as AES and RSA were deployed to secure the SCADA/DNP3 communication against authentication and confidentially attacks. The SHA-2 hashing algorithm was then deployed to secure SCADA/DNP3 against integrity attacks.

In addition to that, the “digital signature” function based on hashing (using SHA-2) and RSA algorithm was generated to provide security against non-repudiation attacks. To test the performance of the proposed solution, the distributed network protocol (DNP3) prototype was developed based on “application layer, pseudo-transport layer and data link layer” of the DNP3 protocol. Furthermore, a testbed setup was established including seven RTUs: RTU1, RTU2, RTU3, RTU4, RTU5, RTU6 and RTU7 connected with the MTU in Station1 and Station 2. Security attacks related to security services such as shared-key guessing, brute force, cracking key, man-in-the-middle, data injection, packet replay and deletion were simulated, using attacker built-in tools. The proposed solution was measured based on system behaviour; and the result proved that their proposed solution provides higher security (including authentication, data integrity, confidentiality and non-repudiation) than other end-to-end security solutions. However, the algorithm presented by Shahzad et al. (2014) is only based on the SCADA’s DNP3 protocol. The SCADA is not only limited to the DNP3 protocol, it may use various protocols such as Modbus, Fieldbus, Profibus, etc. These protocols were also designed without any security concerns. Therefore, there is a need to implement security mechanisms/solutions in other SCADA protocols.

Mera et al. (2020) proposed the Toom-Cook algorithm for encoding and decoding of the keys in cryptographic algorithms, to reduce complexity. The algorithm is also used in McEliece cryptosystems to overcome the drawbacks in terms of the size of the encrypted key and transmission rate. There are only a few algorithms that advance efficiency through large integer multiplication. The Toom-Cook algorithm, the Toom-Cook-4-way, and Karatsuba are well-known techniques that help improve efficiency in cryptosystems. To increase the efficiency of the Toom-Cook-based polynomial multiplications, the research study conducted by Mera et al. (2020) furthermore introduced a technique namely ‘lazy interpolation’ which, along with precomputation, can reduce the overheads of evaluation and interpolation. Two (2) scenarios were used to evaluate the performance of the proposed algorithm. The first scenario involved calculating the sum of two or more polynomial multiplications. The second scenario was identified when multiple polynomial multiplications have

to be calculated and one operand stays the same. The algorithm was then applied to Saber. Saber is one of the post-quantum key-encapsulation mechanisms (KEMs) candidates considered in the second round of the ongoing NIST's post-quantum standardization procedure. The simulation results proved that the algorithm could augment the efficiency of the computationally costly matrix-vector multiplication by 12 − 37% compared with previous methods on their respective platforms. Therefore, the Toom-Cook algorithm is still one of the best techniques for multiplying big integers.

Premnath (2013) proposed the use of a light-weight and faster NTRU asymmetric cryptosystem into the SCADA systems for use in encryption and digital signature of the SCADA networks to address the issues of security and performance complexities, existing cryptographic algorithms being time- and power-consuming. The NRTU is a public-key scheme for lattice-based cryptography. The scheme has two sub-algorithms, namely, the NTRU Encrypt which is used for encryption, and the NTRU Sign which is used for generating a digital signature. The encryption and decryption processes use polynomial operations which make the system faster. An experimental case study with a number of scenarios was conducted to compare the performance of the NTRU, the RSA, and the ECC with respect to their key generation, encryption, decryption, and digital signature speeds on 700 MHz Raspberry Pi running Linux and Intel(R) Core (TM) i3 CPU @ 2.27GHz. The results indicated that the RSA key generation is 20 to 25 times slower than the corresponding NTRU key-generation operation for the same level of security. The second test was observed by implementing the algorithms for computation using the open-source Bouncy Castle 1.47 Java library, comparing the RSA, NTRU, and ECC experimental run times. Their encryption, decryption, and key-generation speeds were compared. The performance evaluation shows that cryptographic operations of NTRU are indeed faster than those of the RSA & ECC for the same level of security (around 2 to 10 times faster). The third experimental case was conducted based on the encryption and decryption runtimes on Raspberry Pi of the NTRU and the RSA. The performance results proved that the total time taken

for both encryption and decryption by RSA is 18 to 33 times longer than that of the NTRU for the same level of security. The test results proved that the NTRU had better processing speed than the RSA and ECC and is suitable for real-time requirements of the SCADA security. The proposed algorithm, the NTRU-based encryption, and authentication schemes were able to address the data-integrity, confidentiality, authentication, and non-repudiation issues.

However, all the schemes are based on arithmetical operations. This means that by launching a brute-force attack using Shor's or Grover's algorithms, these schemes can be broken. Therefore, there is still a research gap in securing the SCADA networks from quantum attacks.

To support the study conducted by Premnath (2013), a study by Nitaj (2015) asserts that the NTRU public key cryptosystem is one of the fastest known public-key cryptosystems. It was first introduced in 1996 by (Hoffstein et al.,1996). The NTRU is resistant to quantum attacks and is categorized as a post-quantum cryptosystem. The NTRU is more efficient than the current and most widely used public-key cryptosystems, such as the RSA which was proposed by Rivest et al. (1978), the ECC proposed by Koblitz (1985), and the El Gamal proposed by Gamal (1985). The security of RSA, ECC, and El Gamal are based on the hardy of factoring large composite integers or computing discrete logarithms. Shor (1997) showed that quantum computers can be used to factor integers and to compute discrete logarithms in polynomial time. As a consequence, the RSA, ECC, and El Gamal will be easily breakable using a quantum computer (Nitaj, 2015). Hence, some public key cryptosystems have been developed that are believed to be resistant to quantum-computing-based attacks, such as the NTRU cryptosystem.

Miri et al. (2017) proposed the NTRU cryptosystem as the best solution for securing data and communications in the ad-hoc ultra-wide band impulse radio (UWB-IR) networks. The research study evaluated and compared the performance of three PKCSs: the RSA, ECC, and the NTRU. The parameters used to evaluate the performance of the PKCSs included: the key size, security level, and speed of encryption and decryption operations. The results obtained from the comparison of the NTRU and ECC algorithms proved that

the NTRU is faster than the ECC with all levels of security; and that the performance speed of encryption and decryption for the NTRU is superior to those of the ECC. The results obtained from the comparison of the NTRU and the RSA algorithms proved that the NTRU encrypts and decrypts more messages than the RSA. Therefore the NTRU provides more high-speed encryption and decryption than does the RSA. According to Miri et al. (2017), the NTRU cryptosystem advantages include easy key generation, high-speed encryption and decryption, small key size, and very low computational power. In addition to that, the operation speed of the NTRU is very high, more efficient, and it consumes less space (Miri et al., 2017).

Compared with all other proposed key-management protocols and cybersecurity algorithms for securing the SCADA networks, the NTRU is the best algorithm to be implemented. It meets all the objective's main security requirements: confidentiality, integrity, and authentication. The scheme is believed to be resistant to quantum-computing-based attacks. However, the future is never predictable, and a quantum computer may be able to crack the NTRU algorithm in the future.

2.9 Summary

Given the importance of protecting the critical infrastructure, a security gap was identified in the Smart Grid SCADA System. This research study evaluates the existing cybersecurity algorithms used to protect the Smart Grid SCADA system. This chapter has discussed the cybersecurity requirements, the overview of Smart Grid, the importance of SCADA in Smart Grid, as well as studies conducted by other researchers. Researchers have attempted to discover and propose cybersecurity algorithms as well as a security scheme that improves the security of the Smart Grid SCADA system. Many vendors use the TCP/IP to transport the SCADA messages. This has made the system more vulnerable to cyberattacks. The protection of the Smart Grid SCADA devices communicating over the network remains a major concern; failure to protect this communication can lead to a cyberattack and a loss of critical infrastructure. The Smart Grid SCADA system must be protected at all costs to avoid an intruder gaining unauthorised access to the network, taking control of

operations which could lead to power cuts or complete blackouts. Therefore, this challenge results in a high demand for both security and authentication.

Chapter 3: System Design and Architecture

3.1 Introduction

The main objective of this research study was to design an ECS algorithm that will improve and strengthen cybersecurity for the Smart Grid SCADA system. This chapter demonstrates the end-to-end communication of Smart Grid SCADA devices; showing how data flows from a client sender to a client receiver using the proposed ECS algorithm to ensure secure authentication. Authentication is a system for certifying the origin of a communication or the process for verifying that an entity or object is who or what it claims to be. Authentication is a crucial identification process of eliminating attacks targeting data integrity. The NTRUEncrypt algorithm was used for encryption and decryption to achieve secure communication between the client sender and a client receiver. In addition to that, the ECS algorithm will be designed in such a way that it achieves the cybersecurity objectives, namely: availability, integrity, and confidentiality. Furthermore, the Toom-Cook algorithm was used to make the encryption and decryption techniques efficient by reducing complexity.

Chapter 3 is structured as follows: Section 3.2 discusses the system architecture. Section 3.3 discusses how the proposed ECS algorithm was designed to achieve secure end-to-end authentication, confidentiality, integrity, and availability, while reducing complexity. The security of deploying the proposed cybersecurity algorithm within the SCADA systems by integrating the NTRU and Toom-Cook algorithms is also focused on. Furthermore, the section enlightens how the ECS algorithm improves and enhances the security of the Smart Grid SCADA system. A flowchart diagram is also provided to assist researchers in this research study to design and develop an effective cybersecurity algorithm for the Smart Grid SCADA system. Lastly, Section 3.4 provides the chapter summary.

3.2 System Architecture

This research study proposed an enhanced cybersecurity algorithm for the Smart Grid SCADA system by integrating the NTRU algorithm (which is a combination of two (2) algorithms, NTRUEncrypt and NTRUSign) with the Toom-Cook algorithm. The reason for using NTRU is that it is one of the

strongest and fastest public cryptosystems: it is also resistant to classic and quantum attacks. An interesting application of this phenomenon is to think of the good basis vectors as a private key, which makes solving closest vector problem (CVP) simple for a given target vector. The bad basis vectors provide a public key, which does not aid in solving CVP, but does provide a way of generating the lattice and placing a target vector in the lattice. This idea has been used to create a number of asymmetrical lattice-based cryptosystems (Zahid, 2017). The NTRUSign was used for authentication; while the NTRUEncrypt algorithm was used for both encryption and decryption. In addition to this, when we want to encrypt a string, we first convert such into a series of long integers, and the encryption keys are stored in the form of long integers. In order to make the encryption and decryption techniques efficient the arithmetic of long integers containing hundreds of digits is used. Hence, the Toom-Cook algorithm is applied for polynomial multiplication to augment the efficiency of the encryption and decryption technique. Such improves and enhances security for the Smart Grid SCADA system. The Toom-Cook-3, Toom-Cook-4-way and Karatsuba are the best known techniques for improving the efficiency in cryptosystems. According to Mera et al. (2020), Toom-Cook is still one of the best techniques for multiplying big integers. The Toom-Cook algorithm is an improved method by a factor of 9/5 compared with the Karatsuba method, in which the number of multiplications has been reduced to 5 from 9.

The various steps start from the initiation phase, Step 1. In this phase the Client Sender A wishes to transmit data or command to Client Sender B. Steps 2, 3, 4, and 5 follow, in which authentication takes place using the NTRUSign algorithm for digital signatures. Digital signature schemes are common authentication mechanisms used in the SCADA. According to Premnath (2013), digital signature schemes are a type of public-key encryption for identifying a sender and preventing data falsification when data is sent from a receiving machine/client to a machine/client. Client Sender A will create a signature data for data desired to be transmitted using the private key of the transmitting client. This then transmits the signature data to Client Sender B, together with the desired data. Client Sender B performs a

verification of the signature data using a public key corresponding to the private key of Client Sender A's apparatus to judge whether the desired data has been falsified. The 4 steps involved in the authentication process are Step 2: signing key; Step 3: verification key; Step 4: digital document; and Step 5: valid signature. Step 6 is the key-generation phase in which Client Sender A begins by generating keys and choosing random polynomials. Step 7 is the encryption process. Step 8 is the decryption process. Lastly, Step 9 is the step in which we perform the arithmetic operation by applying the Toom-Cook algorithm in order to make the encryption and decryption techniques efficient.

3.3 Integrated Cybersecurity Algorithm Design

The algorithm was designed in such a way that when Client Sender A wishes to transmit or send data/command to Client Sender B, Client Sender A goes through the authentication phase. The NTRU is a combination of two algorithms: NTRUEncrypt and NTRUSign. For the authentication phase, NTRUSign algorithm was implemented. The authentication phase comprises different stages, namely, signing key stage, verification stage, digital documents stage, and valid signature stage. All these stages are further explained in the study, while Figure 3.1 illustrates the flow of the processes. Once the user, Client Sender A, has been successfully verified and authenticated, communication between the two (2) devices can be established. The key-generation phase then takes place for the secure exchange and update of public and private keys among the communication SCADA systems/devices. In the key generation under the NTRUSign signature scheme, the private and public keys are generated by using multiple elements in a polynomial ring R with integer coefficients and an ideal of the ring R modulo polynomial XN-1. The next phase is the encryption phase, which is then followed by the decryption phase. The NTRUEncrypt algorithm performs encryption and decryption by polynomial operations that can be implemented at higher speeds; thus by implementing the NTRU encryption in the SCADA we were able to achieve higher speed-processing than conventional public-key encryption.

IEC 62351 is one of the recommended standards by NIST for securing communication between Smart Grid SCADA systems. Table VII shows how the proposed ECS algorithm is designed to achieve secure end-to-end authentication, confidentiality, integrity, and availability, while reducing complexity.

Table VII Cryptographic Solutions for Different Attacks in the Smart Grid SCADA Communication and proposed ECS Solution

Type of Attack	Cryptography Solutions by IEC 62351	Proposed ECS algorithm
Authentication Attack	HMAC, asymmetric digital signature schemes	NTRUSign
Confidentiality Attack	Symmetric and asymmetric encryption algorithms, asymmetric digital signature schemes	NTRUEncrypt
Integrity Attack	Symmetric (AES, DES, TDES) and asymmetric encryption algorithms (RSA, ECC), hashing algorithms (SHA-1, SHA-2, and SHA-256)	NTRUEncrypt
Availability Attack	Asymmetric encryption algorithms, asymmetric digital signature schemes	NTRUEncrypt

Furthermore, the Toom-Cook algorithm was integrated for encoding and decoding of the keys in cryptographic algorithms to reduce complexity.

3.3.1 NTRU algorithm

The study proposes a light-weight and faster NTRU asymmetric cryptosystem integrated into the SCADA systems. The NTRU consists of two (2) algorithms: NTRUEncrypt, which is used for encryption, and NTRUSign, which is used for

digital signatures. The NTRU encryption is proposed as a public-key encryption enabling high-speed processing. The NTRU encryption performs encryption and decryption by polynomial operations that can be implemented at higher speeds than RSA encryption which carries out modulo exponentiation under a certain rule; and ECC that performs scalar multiplication for points on an elliptic curve (Premnath, 2013). NTRUSign is convenient for use in SCADA applications involving real-time constraints.

3.3.2 Integration of the NTRU and Toom-Cook algorithms

NTRU is an open-source public-key cryptosystem that uses lattice-based cryptography both to encrypt and decrypt data. It consists of two algorithms: NTRUEncrypt, which is used for encryption and decryption, and NTRUSign, which is used for digital signatures. The NTRUSign is convenient for use in SCADA applications involving real-time constraints. The NTRU is known as one of the strong and fastest public cryptosystems. The Toom-Cook is still one of the best techniques for multiplying big integers. The integrated cybersecurity algorithm for the Smart Grid SCADA system was intended to provide a secure and faster cryptographic solution. Such would enhance and strengthen the security of the Smart Grid SCADA system using the NTRU lattice-based asymmetric cryptographic and the Toom-Cook algorithms.

A. Initialization phase

Step 1: Client Sender A wishes to transmit data or command to Client Sender B.

B. Authentication Phase

The NTRUSign algorithm will be used for authentication. A digital signature scheme consists of:

- a set of (hashes of) digital documents D
- a set of signatures S
- a set of randomized elements R
- a set K of pairs $K\ sign, and\ K\ verify$ consisting of linked signing and verification keys.

A signing key is a map;

$$K\ sign : D\ x\ R\ \rightarrow S$$

and a verification key is a map.

$$K\ verify : D\ x\ R\ \rightarrow \{\ Yes, No\ \}$$

Sign and verification keys satisfy.

$$K\ verify\ (d, s) = Yes\ \Leftrightarrow\ s\ K\ sign\ (\ d, r) for\ some\ r\ \in R$$

Public Parameters:

Dimension parameter *N*, odd primes *p* and *q*, and norm-bound $B = [\ P2\ N\ /\ 4]$

Step 2: Signing Key

A pair of $(\boldsymbol{f}, \boldsymbol{g})$, vectors with $\boldsymbol{f}$ random mod 3, and g random p

Step 3: Verification Key

$$\boldsymbol{h} = \boldsymbol{f} - \mathbf{1}\ *\ \boldsymbol{g}\ (mod\ q)$$

Step 4: Digital Documents

A document (hash) is a pair of $mod\ p$ vectors $(\boldsymbol{s}p, \boldsymbol{t}p)$

Step 5: Valid Signatures

A signature on $(\boldsymbol{s}p, \boldsymbol{t}p)$ for the signature key h is a pair of vectors ($\boldsymbol{s}, \boldsymbol{t}$) satisfying:

- $t\ \equiv s\ *h\ (mod\ q), i.e., (s, t) \in Lh.$
- $(s, t) \equiv (sp, tp)\ (mod\ p).$
- $||\ s\ ||\ \infty\ and\ ||\ t\ ||\ \infty\ are\ both\ \leq \frac{1}{2} q\ - B.$

<u>NTRUSign Parameters</u>

The following should be practical while providing good security:

N = 661

p = 3

q = 9829081

B = 1487

k = 10

With these parameters, we have:

Pro (Signature is Accepted) ≈ 45%

Key and Signature Size ≈ 15864 bits

Bit Security ≈192 to 256

Algorithm 1: NTRUSign – Signing Algorithm

This algorithm computes the NTRUSign signature on a document $(\boldsymbol{sp}, \boldsymbol{tp})$ using the signing key $(\boldsymbol{f}, \boldsymbol{g})$

1. Choose a random $r\ with\ ||\ r||\ \infty\ \leq\ [\frac{q}{2p} - \frac{1}{2}]$.
2. Set $s0 = sp + pr$.
3. Set $t0 = h\ *s0\ (mod\ q)$.
4. Compute $a =\ \ g - 1\ *(tp - t0)\ (mod\ p)$.
5. Set $s = s0 + a\ *f\ and\ t = t0 + a\ *g$.
6. If $||\ s\ ||\infty\ or\ \ t\ \ \infty\ is\ > \frac{1}{2}q - B, then\ REJECT. Go\ to\ Step\ 1$.
7. Return $(\boldsymbol{s}, \boldsymbol{t})$.

It is easy to check that the $(\boldsymbol{s}, \boldsymbol{t})$ returned by the algorithm has three properties needed as a valid signature for the document (sp, tp)

Figure 3.1 shows the flow of information between two (2) SCADA devices and how the NTRUSign algorithm was applied to validate the transmitter and receiver communicating over the network. This is in order to provide data availability and confidentiality as per the cybersecurity requirements for the Smart Grid.

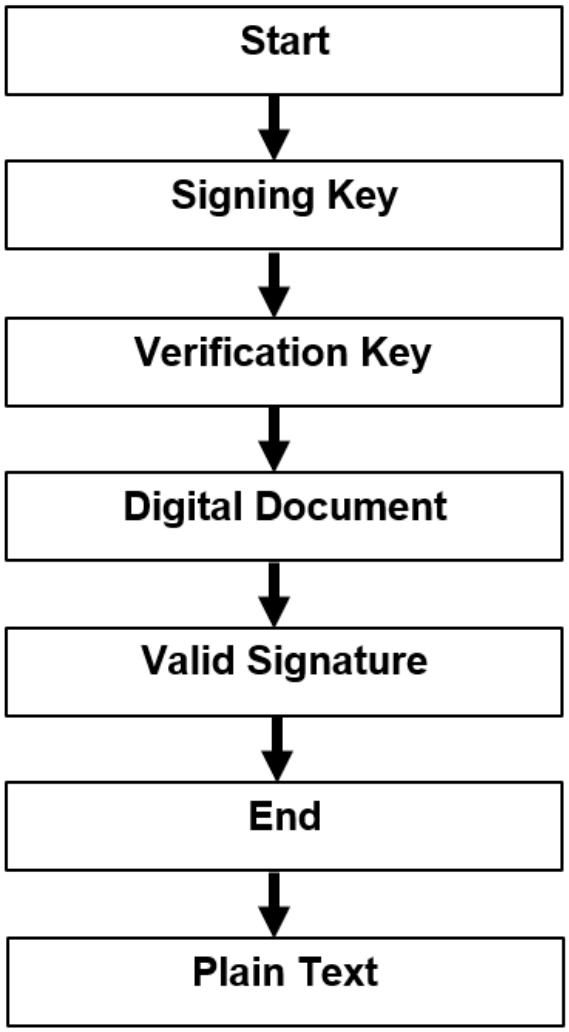

Figure 3.1: Authentication process

C. Key-generation phase

The NTRUEncrypt was used for encrypting and decrypting data being transmitted over the network. NTRUEncrypt uses lattice cryptography. This means that both bases generate the same lattice.

The arithmetic of NTRU depends on three (3) integer parameters (N, *p, q*).
Let $\mathbb{Z}q = \mathbb{Z}/q\mathbb{Z}$ denote the ring of integers modulo *q*. The operations of NTRU took place in the ring of truncated polynomials $\mathcal{P} = \mathbb{Z}q [X]/ (X^N – 1)$. In this ring, a polynomial f is defined by its coefficients in the base $\{1, X, X^2, \ldots X^{N-1}\}$ as presented in Equation (3.1).

$$f = (f_0, f_1, \cdots f_{N-1}) = f_0 + f_1 X + \cdots + f_{N-1} X^{N-1} . \quad (3.1)$$

The addition of two polynomials f and g is defined as pairwise addition of the coefficients of the same degree, as presented in Equation (3.2):

$$f + g = \left(f_0 + g_{0,} f_1 + g_1, \ldots, f_{N-1} + g_{N-1}\right), \quad (3.2)$$

and multiplication denoted " $*$ " is defined as convolution multiplication (see Equation (3.3)):

$$f * g = h = (h_0 + h_1 , \ldots, h_{N-1}), with\ h_k = (x + a)^n = \sum_{i+j \equiv k} f_i\, g_j . \quad (3.3)$$

The Euclidean norm or the length of a polynomial $f = (f_0, f_1, \cdots f_{N-1})$ is defined as in Equation (3.4):

$$||f|| = \sqrt{\sum_{i=0}^{N-1} f_i^2}. \quad (3.4)$$

Let $ß\,(d)$ be the binary set of polynomials defined for a positive integer d as the set of polynomials of R with d coefficients equal to 1 and all the other coefficients equal to 0. The set $ß\,(d)$ can be written as in Equation (3.5):

$$ß(d) = \{\ f(X) \textstyle\sum_{i=0}^{N-1} f_i X^i \in \mathrm{P} \mid f_i \in \{0,1\} \sum_{i=0}^{N-1} f_i = d\ \}. \quad (3.5)$$

Various descriptions of NTRUEncrypt, and various proposed parameter sets, have been in circulation since 1996. The 2005 instantiation of NTRU is set up by six public integers: $N, p, q\ d_f, d_g, d_r$ and four public spaces Lf, Lg, Lm, Lr

- N is prime and sufficiently large to prevent lattice attacks.
- $p\ and\ q$ are prime numbers.
- q is much larger than p.
- $Lf = B('df)$ is a set of small polynomials from which the private keys are selected.
- $Lg = B\,(dg)$ is a similar set of small polynomials from which other private keys are selected.
- $Lm = \mathbb{Z}[X]/\,(Xn - 1)$ is the plaintext space. It is a set of polynomials. $m \in \mathbb{Z}p\frac{[X]}{}\,(Xn - 1)$ that represent encryptable messages.

- $Lr = B\ (dr)$ is a set of polynomials from which the blinding value used during encryption is selected.

Step 6:

The key-generation procedure gains a quadruple of the form (N, p, q, d) that meets all the above-mentioned inputs. In order to obtain a key pair for NTRUEncrypt, the following steps will be taken:

- Randomly choose a polynomial $f \in Lf$ such that f is invertible in P modulo *p* and modulo *q*.
- Compute $fp \equiv f - 1\ (mod\ p)\ and\ fq \equiv f - 1\ (mod\ q)$.
- Randomly choose a polynomial $g \in Lg$.
- Compute $h \equiv g * \text{fq}$ (mod q).
- Publish the key (N, h) and the set of parameters $p, q, Lf, Lg, Lr\ and\ Lm$.
- Keep the private key (f, fp).

The NTRU operates in three (3) polynomial rings $\mathbb{Z}$3 [X] / Φn, $\mathbb{Z}$q [x] / Φn and $\mathbb{Z}$q [x] / (Φ1 . Φn) with Φ1 = (x – 1) and Φn = (xn-1 + x 2-1 + … + 1).

Algorithm 2: NTRU Key Generation

Output: *pk = (h), sk = (f, f_p, h_q)*

8. *f , g* ← Sample *()*

9. f_q ← f^{-1} mod *(q,* Φ_n*)*

10. *h* ← *(3 . g .* f_q*)* mod (q, Φ_1 . Φ_n)

11. h_q ← h^{-1} mod (*q*, Φ_n)

12. f_p ← f^{-1} mod (3, Φ_n)

D. Encryption Phase

The NTRUEncrypt algorithm was used for both encryption and decryption. The version of NTRUEncrypt is described below.

Public Parameters:

N a prime $(250 < N < 2500)$

q large modulus $(250 < q < 2500)$

p small modulus $(say\ p = 3, p\ \aleph q)$

Private Key:

$\boldsymbol{F}, \boldsymbol{G}$ Random ∈ $\{-1, 0, 0\}N$

$\boldsymbol{f}, \boldsymbol{g}$ set $f = 1 + p\boldsymbol{F}\ and\ \boldsymbol{g} = p\boldsymbol{G}$

Public Key:

$\boldsymbol{h} \equiv \boldsymbol{f} - 1 * \boldsymbol{g}\ (mod\ q)$

Encryption:

m plaintext ∈ $\{-1, 0, 0\}N$

r random ∈ $\{-1,0,0\}N$

e $\equiv \boldsymbol{r} * \boldsymbol{h} + \boldsymbol{m}\ (mod\ q)$, ciphertext

Decryption:

$a \equiv \boldsymbol{f} * \boldsymbol{e}\ (mod\ q)$

Lift a to $\mathbb{Z}$n with coefficients | ai | $\leq \frac{1}{2}q$

$\boldsymbol{a}\ (mod\ p) is\ equal\ to\ \boldsymbol{m}$

The encryption function takes an input as the domain parameters, described above, the message M to be encrypted and the public key of the receiving party as input. NTRUEncrypt requires the message to be properly padded and formatted to prevent certain attacks. In order to obtain the ciphertext c (x) of a message M to be encrypted under the public key h(x), the steps shown below will be taken.

Step 7:

- Represent the message as a polynomial $m \in Lm$.
- Randomly choose a polynomial $r \in Lr$.
- Encrypt m with the public key (N, h) using the rule $e \equiv p * r * h + m \pmod{q}$.

Algorithm 3: NTRU Encryption

Input: $m, r, pk = (h)$

Output: c

13. $m' \leftarrow Lift(m)$

14. $c \leftarrow (r \ . \ h + m'$ mod (q, Φ_1 . Φ_n)

E. Decryption Phase

Step 8:

- The receiver computes $a \equiv f * e \pmod{q}$.
- Using a centring procedure, transform a to a polynomial with coefficients in the interval $\left[-\frac{q}{2}, \frac{q}{2}\right]$.
- Compute $m \equiv fp * a \pmod{p}$.

The decryption process is correct if the polynomial $p * r * g + f * m \pmod{q}$ is actually equal to $p * r * g + f * m \in in\ \mathbb{Z}[X]/(Xn - 1)$; that is without using modulo q. We have:

$$a \equiv f * e \pmod{q}$$

$$\equiv f * (p * r * h + m) \pmod{q}$$

$$\equiv f * r * (p * g * fq) + f * m \pmod{q}$$

$$\equiv p * r * g * f + fq + f * m \pmod{q}$$

$$\equiv p * r * g + f * m \pmod{q}$$

Hence, if $a = p * r * g * + f * m \ in\ \mathbb{Z}[X]/(Xn - 1) \pmod{q}$, then

$$a * fp \equiv (p * r * g + f * m) * fp \equiv m \pmod{p}.$$

We note that if the parameters are chosen properly, the decryption process never fails. A sufficient condition for this is to choose q much larger than p.

Algorithm 4: NTRU Decryption

15. Input: Two*integersAandBaregivenwhere0 < A, B, < Xn*
16. *Output:* $AB = c0 + c1xk + c2x2k + c3x3k + c4x4k\ when\ k = n/(k = numbers\ of\ splits$
17. Here $x0 + x1t + x2t2, B = y0 + y1t + y2t2\ heret = Xk$
18. $t = (0,1,2,-1,inf)$
19. $t = 0\ x0 * y0, which\ gives\ w0\ immediately$
20. $t = 1(x2 + x1 + x0) * (y2 + y1 + y0)$
21. $t = -1(x2 - x1 + x0) * (y2 - y1 + y0)$

Figure 3.2 shows the flow of information between two (2) SCADA devices and then how the NTRUEncrypt algorithm was applied to encrypt and decrypt data being transmitted over the network. The algorithm would secure information and provide data integrity as per the cybersecurity requirements for the Smart Grid.

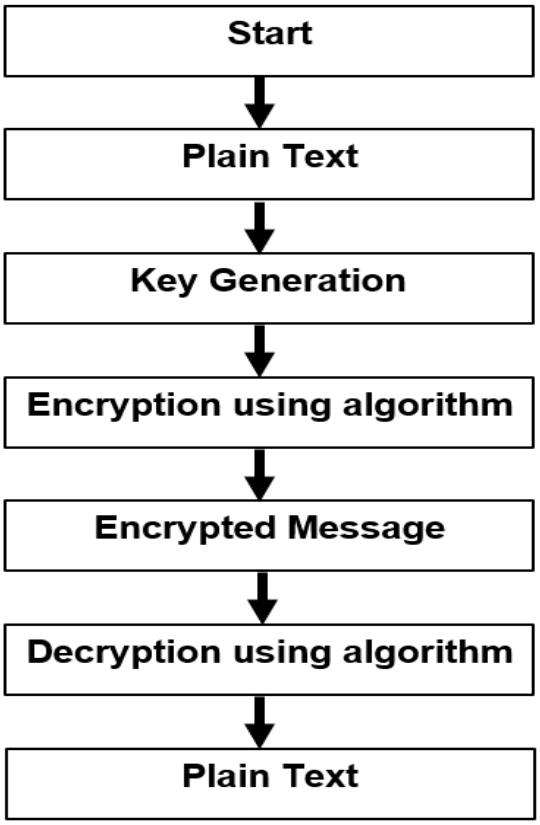

Figure 3.2: Encrypt and decrypt process.

F. Arithmetic Operation Phase

Step 9:

The Toom-Cook algorithm is the advanced approach for splitting the numbers into parts. The Toom Cook-n-way reduces the product to *2*(n)-1* multiplications. Where *n* stands for *3*, let the operands considered be split into *3* pieces of equal length. The parts are written in terms of polynomials (see Equations (3.6) and (3.7)).

$$X\,(t) = (X2)t2 + X1\,(t) + X0 \tag{3.6}$$

$$Y\,(t) = (Y2)t2 + Y1\,(t) + Y0 \tag{3.7}$$

Base B = b is chosen, such that the number of digits of both *x* and *m* in base B is at most k (e.g., 3 in Toom-3). A typical choice for *i* is given by Equation (3.8):

$$i = max\frac{[logbm]}{k}[logbn]\ /k\ ] + 1 \tag{3.8}$$

In our example we'll be choosing the value of

$$B = b2 = 108$$

Then we will separate x and y into base B digits x, y: These 2 equations are multiplied to form $w\ (t) = x(t) * y(t)$

$$W(t) = w4 * t4 + w3 * t3 + w2 * t2 + w1 * t + w0 \qquad (3.9)$$

The final w(t) is calculated through the value of t, although the final step is going to be the addition. Thereafter $x(t)$ and $y(t)$are calculated and multiplied by choosing some set of points, forming $w\ (t)$.

Let the following points be (0,1,2,-1,inf)

$$t = 0\ x0 * y0$$

$$t = 1\ (x2 + x1 + x0) * (y2 + y1 + y0)$$

$$t = -1\ (x2 + x1 + x0) * (y2 + y1 + y0)$$

$$t = 2(4 * x2 + 2 * x1 + x0) * (4 * y2 + 2 * y1 + y0)$$

$$t = inf\ x2 * y2,$$

Then, the value of those combinations is calculated through

$$W(0) = w0$$

$$W(1) = w4 + w3 + w2 + w1 + w0$$

$$W(-1) = w4 - \ w3 + w2 - w1 + w0$$

$$W(2) = 16 * w4 + 8 * w3 + 4 * w2 + 2 * w1 + w0$$

$$W\ (inf\ ) = w4$$

Algorithm 5: Toom-Cook Algorithm

---

22. *Input: TwointegersAandBaregivenwhere0 < A, B, < Xn*
23. *Output:* $AB = c0 + c1xk + c2x2k + c3x3k + c4x4k\ whenk = n/(k = numbers\ of\ splits$
24. Here $x0 + x1t + x2t2, B = y0 + y1t + y2t2\ heret = Xk$
25. $t = (0,1,2,-1,inf)$
26. $t = 0\ x0 * y0, which\ gives\ w0\ immediately$
27. $t = 1(x2 + x1 + x0) * (y2 + y1 + y0)$
28. $t = -1(x2 - x1 + x0) * (y2 - y1 + y0)$

3.5 Summary

The chapter presented the design of the proposed cybersecurity algorithm by integrating the NTRU with the Toom-Cook algorithms. The NTRUEncrypt algorithm was used for encryption and decryption to achieve secure communication between nodes during data transmission. The Toom-Cook algorithm was used to further improve the efficiency of the encryption and decryption techniques which also resulted in achieving higher-speed processing and reducing complexity in encoding and decoding of the keys and transmission rate. The process of the algorithm consists of six (6) phases; namely, the initialization phase, the authentication phase, the key-generation phase, encryption phase, decryption phase, and arithmetic operation phase. To measure the effectiveness of the proposed cybersecurity algorithm, all phases were executed one after another before granting a user access to communicate over the network. The proposed algorithm is expected to improve the efficiency of the encryption and decryption technique and also to provide a secure and more rapid cryptographic solution to enhance cybersecurity for the Smart Grid SCADA system.

Chapter 4: System Implementation

4.1 Introduction

In this chapter, the implementation of the enhanced cybersecurity algorithm for the Smart Grid SCADA system is presented. The algorithm is implemented using network simulator version 2 (NS-2) because NS-2 has the distinct features of a good simulator. One, it provides support for both wired and wireless networks; therefore the study will model the wireless network which will comprise 8 nodes. The nodes will be placed randomly in order also to replicate real-time and/or real-world smart grid scenarios. Two, it is easy to add new protocols on NS-2 (Chhimwal et al., 2013). To add the security functions to the integrated cybersecurity algorithm, a new protocol will be built and added at the network layer – the IP layer. The study will then define a new packet format to represent the new protocols. The new protocol is represented by a class derived from a built-in class in NS-2. This is to ensure secure communication and integrity of data packets during transmission.

The rest of the chapter is structured as follows: In Section 4.2 an overview of the Smart Grid network simulators is presented. In Section 4.3 the study compares various simulators used in the Smart Grid networks, along with their features, key strengths, and weaknesses with the aim of selecting a credible simulator for this study. Section 4.4 describes the parameter setup of the simulator as well as details of how the integrated cybersecurity algorithm for the Smart Grid SCADA system will be simulated. Lastly, Section 4.5 provides the chapter summary.

4.2 Overview of Smart Grid Network Simulators

According to Pujeri et al. (2014), a network simulator is used to test, analyse, and evaluate the performance of a new algorithm or new protocol, comparing the new algorithm with the existing algorithm. However, the result generated by the simulator may not be exact or accurate, which may result in the algorithm failing in real-time. In order to overcome this, it is essential for the researcher to select an appropriate simulating tool that is easy to use, more flexible in model development modification and validation, and which also does appropriate analysis of the output data. A network simulator can also be

used to test the overheads and/or performance of the security solutions in a control system, such as authentication protocols, data secrecy, secure routing, network-based intrusion detection, etc. (Kabir et al., 2014). In addition to this, Wu et al. (2012) state that simulators can be used to test the security designs of the data and/or network in control systems.

Figure 4.1 below illustrates the principle of security simulation. The network security schemes are usually proposed in one or several layers of the reference 7-layer model. The security schemes for end-to-end data are proposed in the upper layer (application layer, presentation layer, and session layer) in the OSI reference network model. On the other hand, the security schemes for end-to-end segments, packets, frames, and bits are proposed in the media layer (transport layer, network layer, data link layer, and physical layer). This security scheme can be based on the basic technologies, such as encryption, integrity check, machine learning, and wireless communication technologies (Wu et al., 2012).

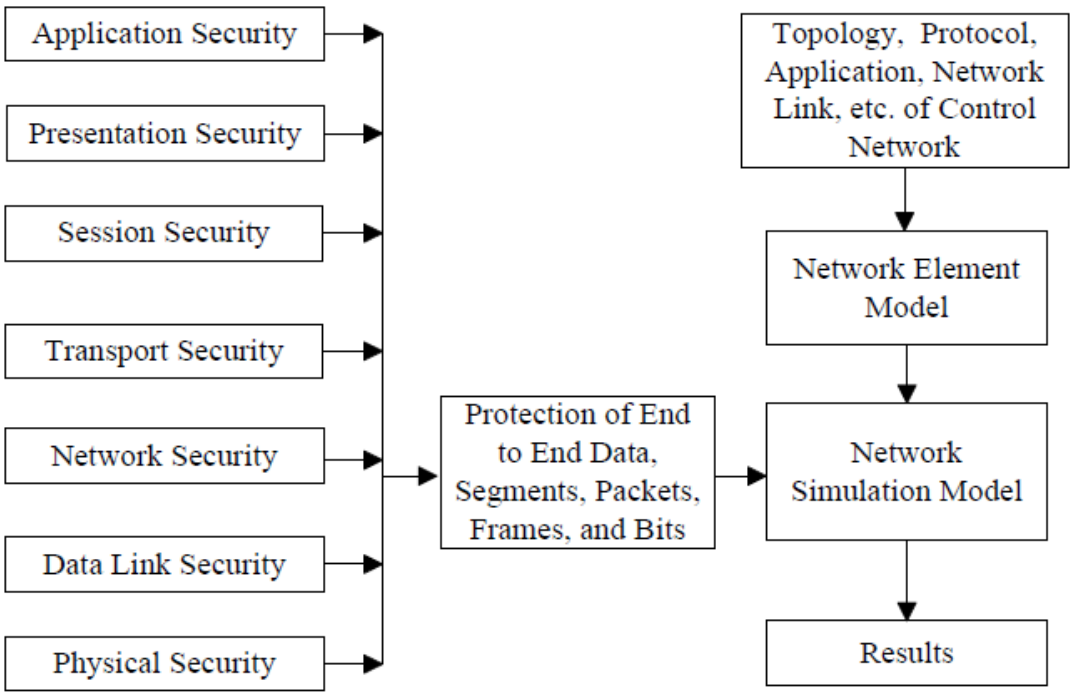

Figure 4.1: Security-simulation-based network simulator (Wu et al., 2012)

4.2.1 Advantages of network simulator

Sharma et al. (2020) identify the advantages of simulation as:

a) Simulation helps in finding or searching for the loopholes in the network or proposed solution design.

b) Simulation modelling is considered the fastest and best way of testing the system before implementing it in the real world.

c) Simulation makes the developer learn more things through implementations. This is a process of learning by implementing. Moreover, predictions about the system can be made to avoid future consequences or challenges by virtually investigating the behaviour of the system.

4.2.2 Smart Grid SCADA system simulator requirements

The three (3) SCADA system simulator requirements identified by Queiroz et al. (2011) are that a SCADA simulator must:

a) Allow plug-n-play for the creation of simulations.

b) Allow connectivity to multiple external hardware and/or software.

c) Support multiple industry-standard protocols (e.g., DNP3, Modbus/TCP, etc.) Therefore, these requirements were taken into consideration when selecting the network simulator.

4.2.3 List of network simulators

There are different types of network simulation tools that are open-source and commercial, including:

a) Network simulator version 2 (NS-2)

b) Network simulator version 3 (NS-3)

c) Global mobile information system (GlomoSim)

d) Network simulator (NetSim)

e) TinyOS simulator (TOSSIM)

f) SensorSim

g) Matrix laboratory (MATLAB)

h) Optimized network engineering tool (OPNET)

i) Objective modular network tested in C++ (OMNET ++)

j) Quality networking (QualNet)

Amongst the list of simulators identified in 4.2.3, the study will only focus on five (5) simulators which are the most used simulators in the Smart Grid SCADA system. The study will then compare those simulators in order to choose the most credible simulator for the integrated cybersecurity algorithm. The five (5) compared simulators are: Matlab, OMNET ++, SCADASim, NS-2, and NS-3.

a) MATLAB

MATLAB is an efficient simulation methodology also referred to as SIMULINK. Simulink is a tool for designing and simulating dynamic and embedded systems. Simulink has collaborated with MATLAB, and is designed by MathWorks. Simulink has the capability of modelling, simulating, and analysing. It is a graphical programming language tool for modelling, implementing, and investigating dynamic systems. It is a simulation tool that provides several toolboxes set to build new network scenarios (Sharma et al., 2020).

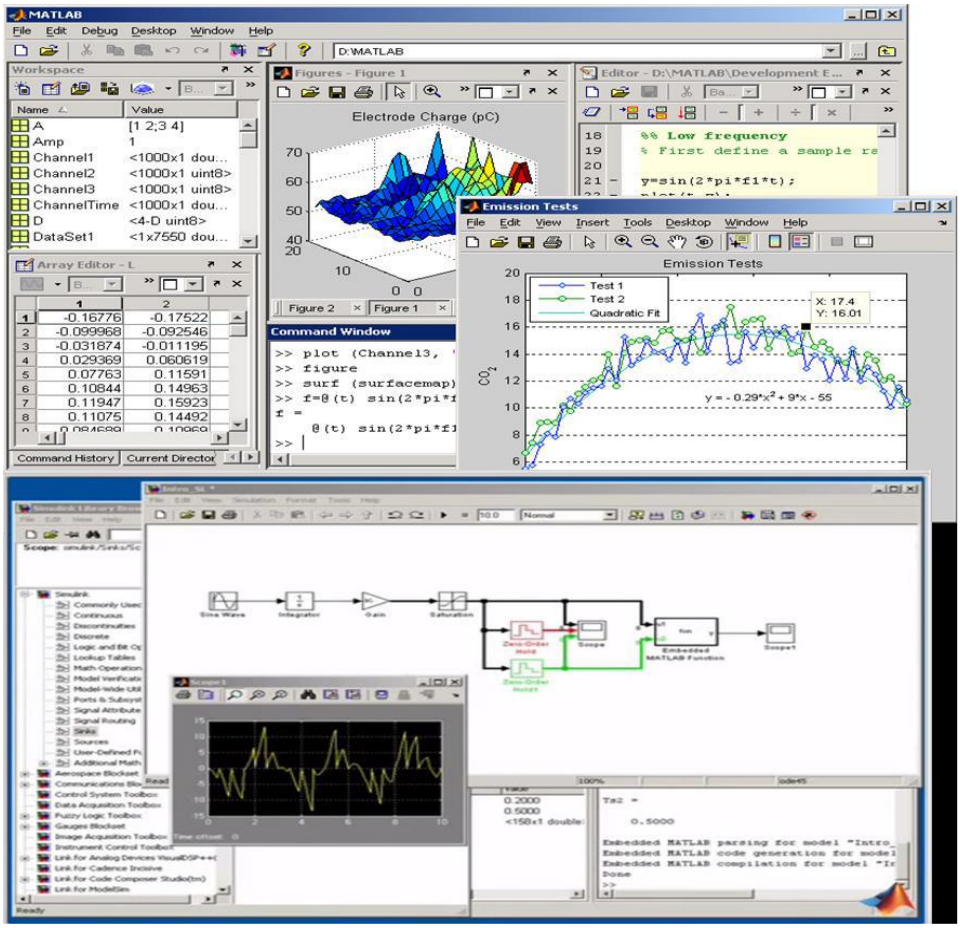

Figure 4.2: MATLAB interface

b) OMNET ++

OMNET++ is a generic simulation engine that allows plug-n-play through its NED WYSIWYG editor; and allows integration into external applications and devices. There are three ways of integrating an OMNET++ simulation with external applications; namely, source code, shared libraries, and sockets (Mayer et al., 2008). According to Wu et al. (2012), a key benefit of such a simulation tool is its ability to test the effects of attacks on a real control process using realistic SCADA protocols (Modbus/TCP). Furthermore, OMNeT++ (Objective Modular Network Tested in C++) is an open-source simulator tool similar to NS-2 and NS-3 to simulate networks both wired and wireless. OMNeT ++ offers an eclipse-based IDE, a graphical runtime environment and a host of other tools. It is a general-purpose simulator capable of simulating any system composed of devices interacting with one another. The support for wire and wireless simulation is incomplete.

OMNeT++ provides a component-based, hierarchical, modular, and extensible architecture. Components and modules are programmed in C++, and then assembled into larger components and models using a high-level language (NED). This provides the reusability of the model free of charge. OMNeT++ has vast GUI support. Due to its modular architecture, the simulation kernel (and models) can easily be embedded into applications. Besides the simulation kernel library, the simulation environment contains a graphical network editor (GNED), a NED compiler, graphical (Tkenv) and command line (Cmdenv) interfaces for simulation (Kabir et al., 2014).

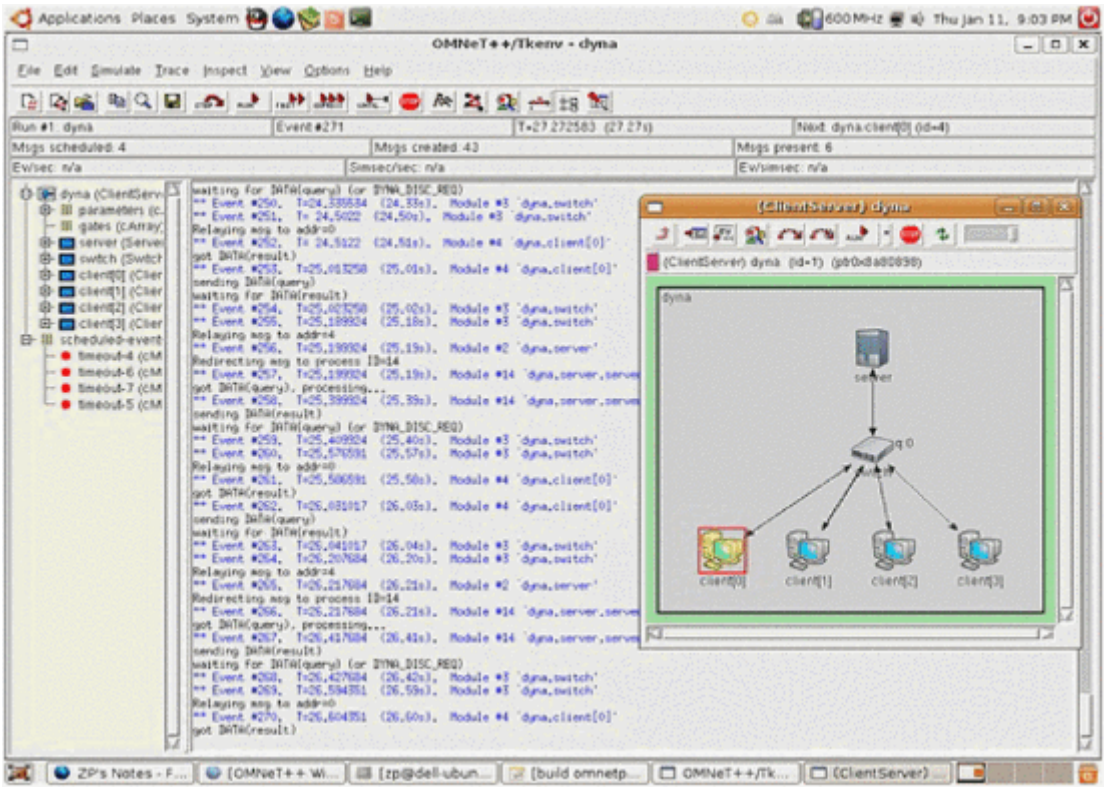

Figure 4.3: OMNET ++ simulator interface (Khan et al., 2012)

c) Scada Simulator (ScadaSim)

The SCADASim aims to provide an environment in which flexible SCADA system simulations can be efficiently built. It allows multiprotocol integration with external devices and applications. SCADASim is built on top of OMNET++. OMNET++ consists of modules that communicate with one another through message passing.

The communication occurs either through input and output gates or through direct messages. Modules can also be combined in a hierarchy of levels making it possible to build complex simulation components. To choose OMNET++ as the simulator engine we evaluated several other engines such as NS-2/NS-3. OMNET++ was chosen because it is a generic simulation engine. It allows plug-n-play through its NED WYSIWYG editor; and it also allows integration into external applications and devices (Queroz et al., 2011).

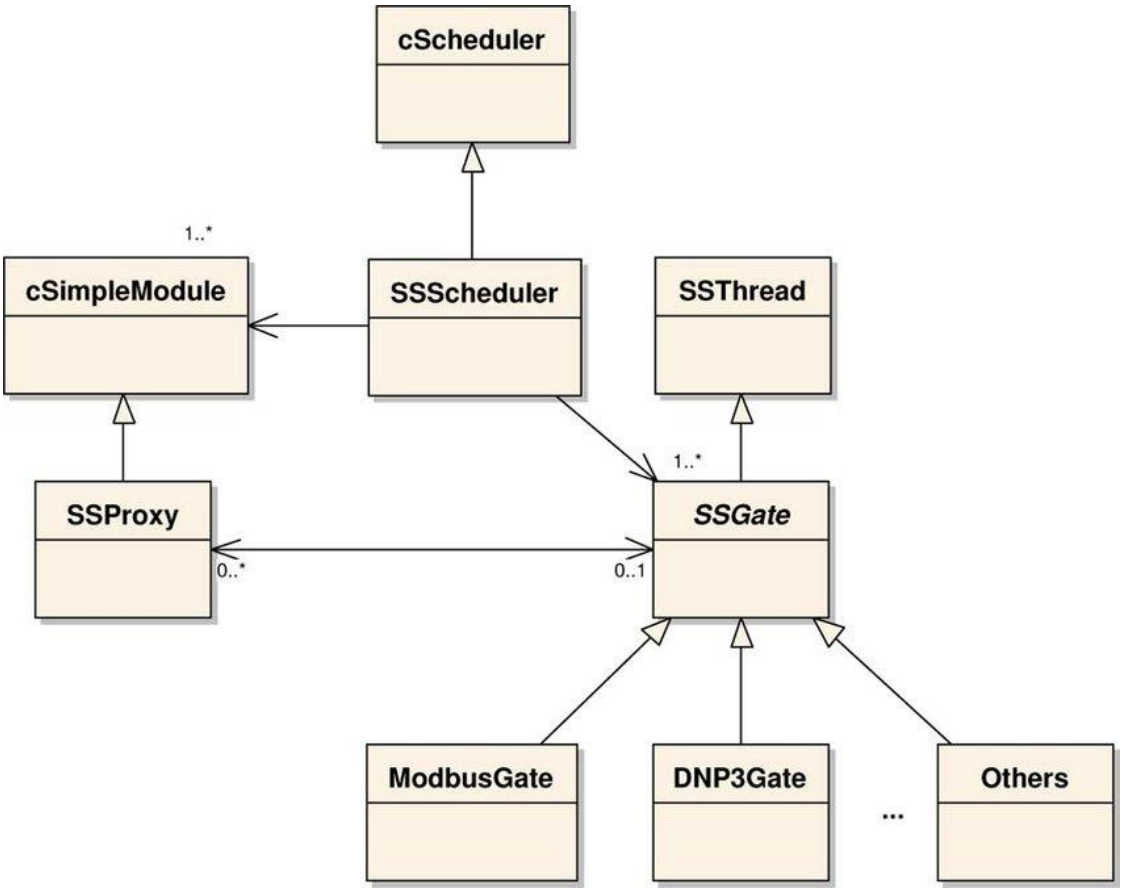

Figure 4.4: SCADASim component architecture (Queroz et al., 2011)

d) Network simulator version 2 (NS-2)

NS-2 (Network Simulator Version-2) is an open-source discrete event simulator designed especially for network research. It provides support for both wired and wireless simulation of functions and protocols such as TCP, UDP, inter alia. NS-2 performs simulations to explore various issues such as protocol interaction, congestion control, the effect of network dynamics, scalability, and more. It runs on the right kind of

scenario which includes, amongst others, the topology size, density distribution, traffic generation, membership distribution, a real-time variance of membership, and network dynamics. (Kabir et al., 2014).

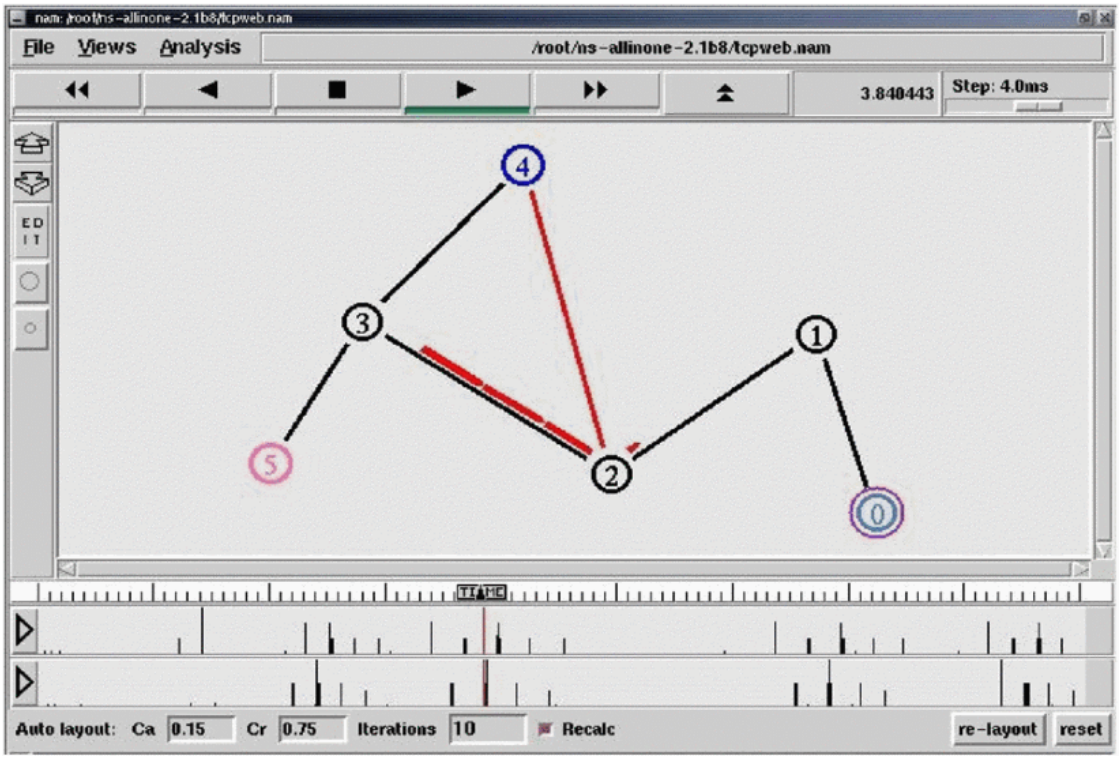

Figure 4.5: NS-2 Simulator interface (Khan et al., 2012)

e) Network simulator version 3 (NS-3)

NS-3 is an open-source and discrete-event network simulator targeted primarily for research and educational use. NS-3 is implemented entirely in C++ and supports python for scripting and visualization. Ns-3 is used to simulate the local area networks (LANs) and wide area networks (WANSs); as well as to simulate wired and wireless networks (Anad et al., 2019). According to Kabir et al. (2014), for wired technology, the NS-3 provides a device model of a simple network of Ethernet which uses CSMA/CD as its protocol scheme with exponentially increasing back-off to contend for the shared transmission medium. NS-3 is not an extension of NS-2. Besides the scalability and performance improvements, simulation nodes have the ability to support multiple radio interfaces and multiple channels. Furthermore, NS-3 supports a real-time schedule that makes it possible to interact

with a real system. For example, a real network device can emit and receive NS-3 generated packets (Saidallah et al., 2017).

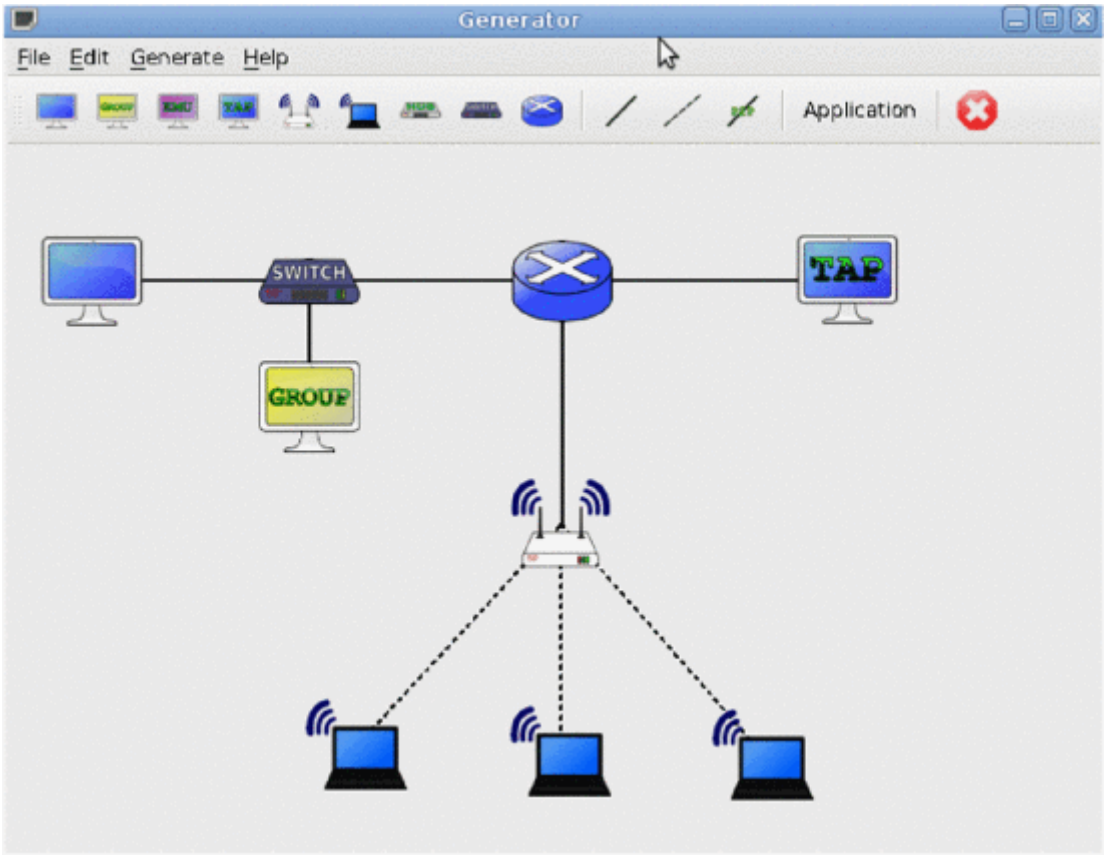

Figure 4.6: NS-3 simulator interface (Khan et al., 2012)

4.3 Comparison of Network Simulators

As indicated above in Section 4.2.3, various open-source and commercial simulators are available, and can be used for testing the cybersecurity of the Smart Grid SCADA system. However, to select a credible simulation tool for this study it is imperative to have the knowledge of various other simulation tools available, along with their features, strengths, and limitations. Therefore, a comparative study is conducted and presented in this study of various open-source simulators, comprising MATLAB, OMNET ++, SCADASim, NS-2, and NS-3. The selection of the five (5) network simulators is also based on their popularity in the Smart Grid SCADA system cybersecurity simulations. Table VIII details the key strengths and limitations of the various network simulators.

Table VIII: Key Strengths and Limitations of Network Simulators

Simulator	Key Strength	Limitations
MATLAB	• Leverages three (3) different simulation technologies to efficiently trade-off simulation detail and speed • Fast discrete event simulation engine • Customizable wireless modelling • Integrated GUI-based debugging and analysis	• Complex GUI operation • It does not allow many nodes within a single connected device • Accuracy of results is limited by the sampling resolution • Simulation is inefficient if nothing happens for long periods
OMNET ++	• Powerful graphical user interface (making tracing and bugging easier) • Simulates power consumption	• Number of protocols is not large enough • Compatibility problem (not portable)
SCADASim	• Provides high scalability while integrating both real hardware and prototype software modules • Integration of existing external components into simulations simplifies the evaluation of components because topologies, traffic patterns, and other parameters can easily be changed within the tool	• Does not provide implementations of all types of attacks into all SCADA protocols. There are more than 150 protocols used by SCADA systems • System can only simulate network-based attacks • Stopped being developed in 2011 • Does not simulate hosts with different behaviours on the

Simulator	Key Strength	Limitations
	• The framework can be extended by the users to add their own protocols; otherwise there are too many protocols	corporate network, such as e-mail servers and databases
NS-2	• Easy to add new protocols • A large number of protocols are available publicly • Availability of a visualization tool	• Supports only two wireless MAC protocols − 802.11, and a single-hop TDMA protocol • Needs to be familiar with a writing scripting language
NS-3	• NS-3 is not an extension of NS-2 is a new simulator • NS-3 is open-source	• Python bindings do not work on Cygwin • Only IPv4 is supported

Table IX describes the various features provided or supported by the simulation tools.

Table IX: Feature Comparison of Network Simulators

Features	MATLAB	OMNET++	SCADASim	NS-2	NS-3
Licence Type	Commercial	Open source (for study and research)	Open source	Open source	Open source
Language used	C and C++	C++	C++ and OMNET ++	C++ and OTCL	C++ and optional Python bindings

Features	MATLAB	OMNET++	SCADASim	NS-2	NS-3
Platform	Windows, Linux, MAC OS X	Linux, Unix, windows, MAC OS	Linux	Linux, Unix, windows, Cygwin	Linux, Unix, Windows
GUI Support	Excellent	Good	Good built on OMNET ++	Poor	Good
Ease of use	Easy	Easy	Easy, built on OMNET ++	Hard	Hard
Time taken for download and installation	Easy	Very easy takes very little time. Readily available	Moderate	Moderate time	Long time to download and instal necessary patches and supporting software

4.3.1 The selected network simulator (NS-2)

The NS-2 simulator suits the choice of simulation for this paper due to its flexibility and ability to test complex scenarios (Kabir et al., 2014). Furthermore, a study conducted by Mohammed (2013) reminds that NS-2 supports a number of algorithms for routing and queuing. This is very helpful because it is costly to verify the viability of new algorithms, test architectures, check topologies, and check data transmission.

Fig 4.6 below shows a detailed description of the NS-2 architecture. The NS-2 provides users with an executable command “ns” which takes one input argument, the name of a Tcl simulation scripting file. In most cases, a simulation trace file is created and is used to plot graphs and/or to create animation (Issariyakul et al., 2011).

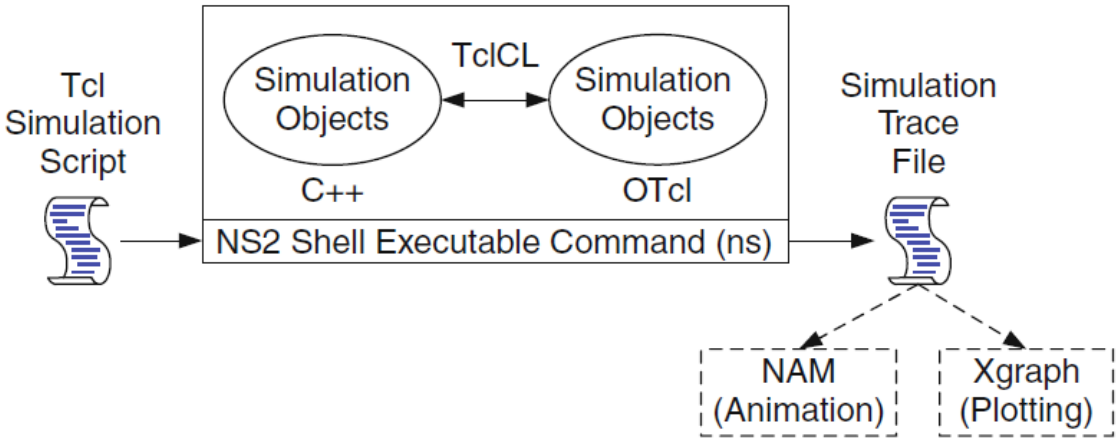

Figure 4.7: NS-2 basic architecture (Issariyakul et al., 2011)

NS-2 consists of two key languages which allow and enable it to be a very powerful simulator: C++ and Object-oriented Tool Command Language (OTcl).

a) C++ defines the internal mechanism (i.e., a backend) of the simulation. The OTcl sets up the simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a frontend). The CCC and the OTcl are linked together using TclCL. Mapped to a C++ object, variables in the OTcl domains are sometimes referred to as handles. Conceptually, a handle is just a string (e.g., "_o10") in the OTcl domain, and does not contain any functionality. Instead, the functionality (e.g., receiving a packet) is defined in the mapped CCC object (e.g., of class connector). In the OTcl domain, a handle acts as a frontend that interacts with users and other OTcl objects. The handle may define its own procedures and variables to facilitate the interaction (Issariyakul et al., 2011).

b) After simulation, NS-2 outputs text-based simulation results. To interpret these results graphically and interactively, tools such as NAM (Network AniMator) and Xgraph are used. To analyse a particular behaviour of the network, there is an in-built tool in NS-2 for graphical-based simulation, namely, NAM. This tool gives a pictorial view of the transfer of packets on the nodes, the position of the nodes, and other simulation details. It also has Xgraph which handles and analysis the simulation end results graphically (Bakare et al., 2019).

4.3.2 NS-2 directory structure

NS-2 directory tools contain various helper classes such as random variable generators. Directory common contains basic modules related to packet forwarding such as the simulator, the scheduler, the connector, the packet, and the directories queue, the TCP and trace containing modules for queue, TCP, and tracing, respectively (Issariyakul et al., 2011).

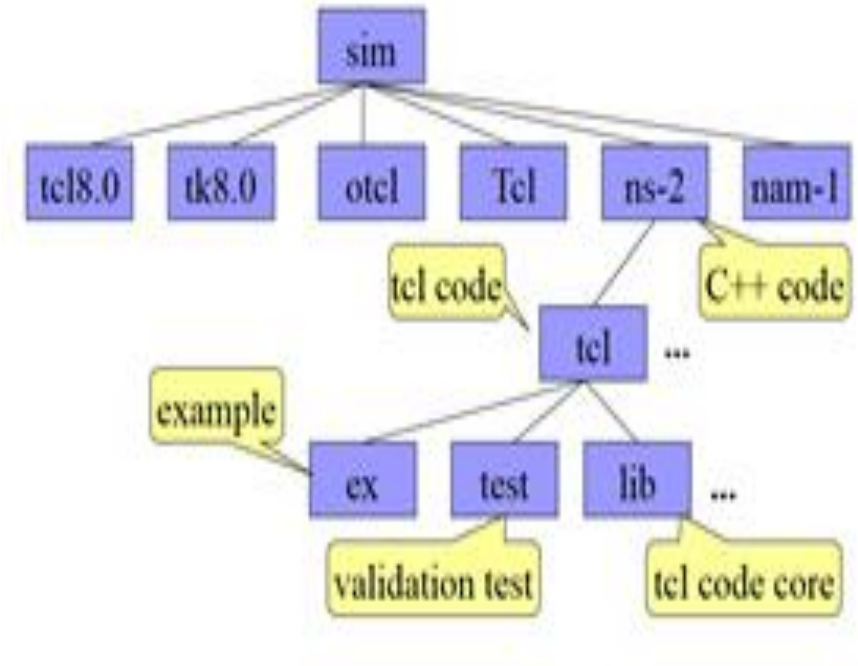

Figure 4.8: NS-2 directory structure (Issariyakul et al., 2011).

4.4 Simulation of the Integrated Cybersecurity Algorithm for the Smart Grid SCADA System

The main purpose of simulating the proposed integrated cybersecurity algorithm is to determine whether the proposed cybersecurity algorithm brings improvement to the Smart Grid SCADA system. The Tcl in NS-2 enables full control over the simulation setup, configuration, and occasional actions (e.g., creating new TCP flows). Therefore, the Tcl language will be used to design the network, which includes setting up parameters, node configurations, topology, connection between nodes, transfer packages, and simulation time. In addition to that, C++ language is used for the security package that entails encryption and decryption functionalities (Mohammed, 2013).

4.4.1 Simulation setup

The integrated cybersecurity algorithm for the Smart Grid SCADA system is implemented using NS-2.35 simulator. The simulation focuses on the DoS attack made on the RTU. When the RTU is affected by a DoS attack, commands initiated from HMI/ MTU may not be able to reach RTU; this may affect critical functionalities such as scheduling, state estimation, and islanding. Furthermore, DoS attacks are considered one of the major threats to the Smart Grid SCADA system targeting availability; and a successful attack on the RTU can lead to a blackout. Simulation of DoS attacks will help in assessing the efficiency and effectiveness of the proposed ECS algorithm against RSA and ECC. Some 8 nodes will be randomly arranged to replicate a real-time Smart Grid SCADA network. The nodes will represent five (5) RTUs: RTU1, RTU2 and RTU3, RTU4, and RTU5, which will be connected with MTU in Substations A and B. In Substation A, RTU1, RTU2, RTU3, RTU4, will be directly connected with MTU using a switch within the LAN. The RTU5 is located at Substation B, a distance away from Substation A with WAN. On the computing platform, a machine running Windows 10 with 8GB memory was used. To simulate the wireless network, the MAC layer protocol will use 802.15.4 and the routing protocol implemented is the Ad hoc On-Demand Distance Vector Routing (AODV) to specify how routing information is propagated to all related nodes.

4.4.2 Implementation of the integrated cybersecurity algorithm for the Smart Grid SCADA system

As mentioned in 4.1 a new protocol, the ECS algorithm will be built and added onto the NS-2 to augment the security functions. This will allow and enable the simulation and performance testing of the enhanced cybersecurity algorithm. Encryption and decryption functions will also be added to the new protocol to ensure secure communication and integrity during data transmission between nodes.

Steps for modifying/adding new packet formats (Hegde et al., 2014)**:**

a) Define a new packet format.

b) Derive a new class from agent class for processing this new packet format.

c) Processing includes:

- Encrypting function
- Decrypting function

Steps involved in adding a new protocol in NS-2 (Hegde et al., 2014):

a) Define a new packet class Security_Packet

b) Add new packet entry into Packet.h file.

c) Add new packet type in ns-default.tcl file.

d) Make an entry into ns-Packet.tcl file.

e) Make an entry into Makefile.info file.

4.2.3 Parameter setup

The cybersecurity algorithm is implemented using version NS-2.35. Table X details the parameters setup for the simulation of the integrated cybersecurity algorithm for the Smart Grid SCADA system:

Table X: System Parameters

Parameters	Value
Simulator	NS-2
Type of Network Interface	Wireless
Internet Protocol	TCP
MAC Protocol	IEEE 802.15.4

Routing Protocol	AODV
Antenna Model	Omnidirectional
Terrain Size	500 X 500 m
Number of Nodes	8
Node Placement	Random
Packet Size	10 B
Intervals	10 µs
Transmission Speed	5 Mbps
Security Algorithm	Integrated cybersecurity algorithm for the Smart Grid SCADA system

This research study chose to use the IEEE 802.15.4 protocol because of the security features it offers; and also because the MAC protocol IEEE 802.15.4 is used as a data link layer for various network protocols. AODV was chosen as the routing protocol because it minimizes the number of required broadcasts by creating routes only on an on-demand basis; and it has been declared the best routing protocol because it is loop-free (Sarao, 2019).

4.5 Summary

The chapter presented the simulation setup for the proposed integrated cybersecurity for the Smart Grid SCADA system; illustrating how the algorithm will be implemented. The chapter provided a review and comparison of the Smart Grid SCADA system network simulators, their features, key strengths, and weaknesses. A detailed explanation of the NS-2 simulator was also provided, including the features that made it suitable and credible for use in this research study.

Chapter 5: Results and Discussions

5.1 Introduction

Cybersecurity is one of the key concerns for the Smart Grid. Testing new solutions is crucial work for researchers because it allows them to test and analyse the results of the proposed solution design before implementation. Simulation recreates real-world scenarios using computer programmes; one of the advantages of simulation identified by Arvind (2016) is that it also saves a great deal of time, and money and makes the implementations easy. According to Pujeri et al. (2014), a network simulator is used to test, analyse, evaluate the performance of a new algorithm or new protocol, and compare the new algorithm with the existing algorithm. The simulator can be modified to achieve better results for the required analysis. This chapter presents and analyses the performance results using the NS-2 simulator to measure the effectiveness of the integrated cybersecurity for the Smart Grid SCADA system. The NAM was used to analyse the behaviour of the network. The NAM also provided a pictorial view of the transfer of packets on the nodes, the position of the nodes, and other simulation details. Xgraph was used to handle, analyse and present the simulation end results graphically. Simulation results were obtained from 10 simulations.

This chapter is structured as follows: In Section 5.2 the study presents the experimental evaluation of the proposed cybersecurity algorithm, NTRUEncrypt and NTRUSign algorithms, and the Toom-Cook algorithm. The section also offers the cryptographic techniques that help in improving the efficiency of cryptosystems. Such is accomplished by reducing complexity in encoding and decoding of the keys and transmission rate through large integer multiplication. In Section 5.3 the study presents simulation results and analysis and the chapter is concluded in Section 5.4.

5.2 Experimental Evaluation

A simulation experiment was conducted using the NS-2.35 simulator to measure the effectiveness of the integrated cybersecurity algorithm for the Smart Grid SCADA system. To simulate the wireless network, the MAC layer protocol 802.15.4 was used; and for the routing protocol, the Ad hoc On-

Demand Distance Vector Routing (AODV) was implemented to specify how routing information should be propagated to all related nodes. The NTRUEncrypt and NTRUSign algorithms were used for the authentication, encryption, and decryption processes, in order to achieve secure communication during data transmission, while protecting information from unauthorized users. The Toom-Cook algorithm was used to make the encryption and decryption techniques more efficient, by reducing complexity in encoding and decoding of the keys and transmission rate.

5.3 Simulation Results

A simulation scenario was applied, as explained in Section 4.4.1, to monitor the performance of the integrated cybersecurity algorithm along with various other PKCSs: the RSA and ECC algorithms. The simulation results presented in this study have been gathered from an average of ten (10) simulations. The performance of public key cryptosystems is evaluated and compared on the key size, security level, speed of encryption and decryption operations, and packet loss:

1. Key size: Key length is an important security parameter. Key length refers to the number of bits in a key used by a cryptographic algorithm to encrypt a message. Key management is vital for encryption and authentication in securing the Smart Grid. To encode and decode the key is essential; this is because the length of the key determines the degree of safety. Thus, the longer the key size, the higher the security (Abood et al., 2018).
2. Security level: This refers to the measure of the strength that a cryptographic primitive such as a cipher or hash function achieves. The security level is usually expressed as several “bits of security” (also security strength), in which *n*-bit security means that the attacker would have to perform 2^n operations to break it.
3. Speed of encryption and decryption operations: The encryption speed measures the time taken to process the ordinary text into encrypted text. The decryption speed measures the period of decoding the decrypted message into readable text.

4. Packet Loss: This occurs when data packets responsible for transporting the information fail to reach their destination after being transmitted over the network.

This research study compared and analysed the performance and the security of the proposed ECS with best-known algorithms RSA and ECC used to protect the Smart Grid SCADA system. The objective is to demonstrate the best-chosen algorithm to be implemented within the Smart Grid SCADA system.

1. The study implemented, evaluated, and compared the performances of cryptographic algorithms RSA and ECC with the proposed algorithm NTRU. The study chose cryptographic algorithms because these are designed around computational hardness assumptions, making these algorithms difficult to break by any intruder/adversary (Jamel et al., 2017). RSA and ECC are approved algorithms for securing the Smart Grid SCADA system and are also known as PKCSs. Cryptosystems are considered a suite of three algorithms used for key generation, encryption, and decryption (Premnath, 2013). The concept of asymmetric key cryptography was introduced by Whitfield Diffie and Martin Hellman. The encryption process uses a public and a private key. The public key (pk) is known to all and is used to encrypt data; however, only the person who has the corresponding private key (sk) can decrypt the data. The challenge with implementing these existing cryptosystems in the Smart Grid for authorization, authentication, encryption, and decryption is that they require more bandwidth, processing power, and memory. Therefore, to overcome this issue, this study proposed the use of a faster and more lightweight cryptographic algorithm known as the NTRU.
2. The NTRU algorithm was proposed to significantly reduce computational and memory overheads. The NTRU cryptosystem is made up of two algorithms: NTRUEncrypt, which is used for encryption, and NTRUSign, used for digital signatures. The NTRU encryption performs encryption and decryption by polynomial operations that can

be implemented at higher speeds than can RSA encryption, which carries out modulo exponentiation under a certain rule, and ECC, which performs scalar multiplication for points on an elliptic curve. Therefore, when compared, the NTRU provides easy key generation, high-speed encryption and decryption and very low computational power, making it a faster and more lightweight algorithm. However, the proposed algorithm strongly considered encryption and decryption of data and the authentication of the user by integrating the NTRU and the Toom-Cook algorithms. Such integration ensures that encryption and decryption for the Smart Grid is efficient and secure. Another reason for choosing NTRU is that it has been categorized as a post-quantum cryptosystem, meaning it is resistant to quantum attacks.

3. There are only a few algorithms that advance efficiency through large integer multiplication. The Toom-Cook-3, Toom-Cook-4-way and Karatsuba are well-known techniques that help in improving the efficiency of cryptosystems. These techniques are used in cryptographic algorithms for reducing the complexity in encoding and decoding of the keys such as ElGamal, RSA, Elliptical Curve-cryptosystems, and the Diffie Hellman key-exchange protocol. This method is also used in McEliece Cryptosystems to overcome the drawbacks in terms of the size of the encrypted key and transmission rate. The Toom-Cook algorithm was chosen to be integrated with the NTRU because it is faster than the Toom-Cook-4-way and Karatsuba methods. Furthermore, a study conducted by Mera et al. (2020) demonstrated that the Toom-Cook algorithm is an improved method by a factor of 9/5 compared with the Karatsuba methods in which the number of multiplications has been reduced to 5 from 9. The study compared various cybersecurity algorithms and well-known techniques that help improve efficiency in cryptosystems. As a result, the study proposed an integrated cybersecurity algorithm for the Smart Grid SCADA system by integrating the NTRU with the Toom-Cook algorithm. This integration assisted in achieving higher processing speed. Such

improved the efficiency of encryption and decryption techniques, which ensured secure communication over the network.

5.4 Effects Studies of Topology

This section presents the performance comparison and security analysis of the public-key cryptosystems; and evaluation of the effects of the key size, security level, and speed of encryption and decryption operations.

5.4.1 Effects of key size and security level

A key is a bit string that is used to transform data. The size in bits of the key is an important security parameter in cryptographic algorithms. Table XI shows the public-key algorithm sizes of the RSA, ECC, and NTRU algorithms, along with equivalent security levels (Jamel et al., 2017).

Table XI: Key sizes of Cryptographic Algorithms in Bits

Security Level	n	RSA key sizes (bits)	ECC Key sizes (bits)	NTRU key sizes (bits)	Protection Life
80	251	1024	160	2008	Until 2010
112	347	2048	224	3033	Until 2030
128	397	3072	256	3501	Beyond 2030
192	587	7680	384	5193	Beyond 2030
256	787	15360	512	7690	--

The public-key size of a cryptosystem gives valuable insight into the bandwidth usage if the cryptosystem is intended to be used in key-exchange schemes (Loriya et al., 2017). Table XI gives corresponding NTRU, ECC, and RSA key sizes for equivalent security levels (k) of 80 bits, 112 bits, and 128 bits, 192 bits, and 256 bits.

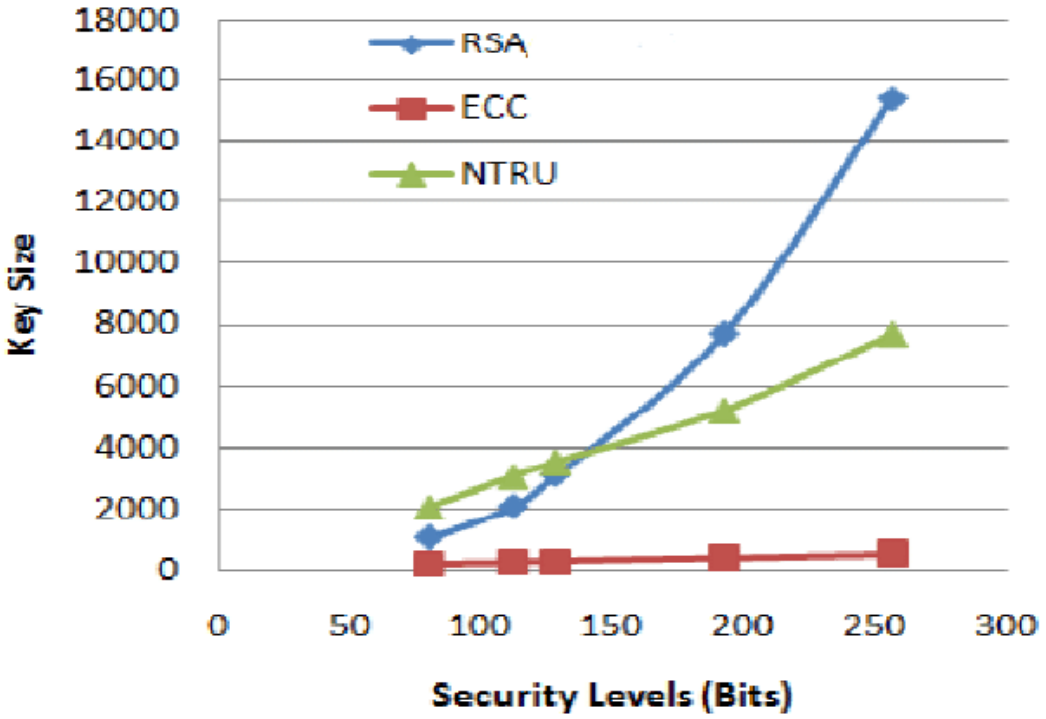

Figure 5.1: Security level vs key size

The security of the RSA and ECC is based on the difficulty of factoring large composite integers or computing discrete logarithms; while the security of the NTRU is related to a very difficult problem in lattice reduction, called the shortest vector problem (SVP). These algorithms were designed around computational hardness assumptions, making them difficult to break in practice by any adversary. However, a study conducted by Shor (1997) showed that quantum computers can be used to factor integers and compute discrete logarithms in polynomial time. As a result, RSA, and ECC will be easily breakable using a quantum computer. This is unlike the NTRU which is not vulnerable to quantum-computer-based attacks. To support this, a study conducted by Silverman (2015) insists that there are no quantum algorithms that solve general cases of SVP or closest vector problem (CVP) in polynomial or subexponential time; thus, the NTRU is a very strong and powerful algorithm.

The results obtained from the simulation show that, when the symmetric key size increases, the key size for RSA increases more rapidly than does the ECC. The ECC algorithm can offer better security per bit increase in key sizes compared with the RSA and NTRU. The ECC has the smallest key size, which makes it the best to use in terms of bandwidth. The NTRU's bandwidth usage becomes more efficient with respect to RSA as the security level increases.

5.4.2 Performance comparison of the RSA, ECC and ECS algorithms in terms of key generation, encryption, and decryption

The performance comparison of the RSA, ECC, and ECS algorithms in terms of key generation, encryption, and decryption is shown in Table IX.

Table Xll: Comparison of Key Generation, Encryption and Decryption Speed of RSA, ECC and ECS Algorithms

	RSA- 1024	**ECC-168**	**ECS - 263**
Public-key size (bits)	1024	168	1841
Key generation (ms)	1432	65	17.6
Encryption (ms)	4.32	140	1.4
Decryption (ms)	48.5	67	2.9

Key length is an important security parameter. Key length refers to the number of bits in a key used by a cryptographic algorithm to encrypt a message. Table XII provides the corresponding NTRU, ECC, and RSA key sizes.

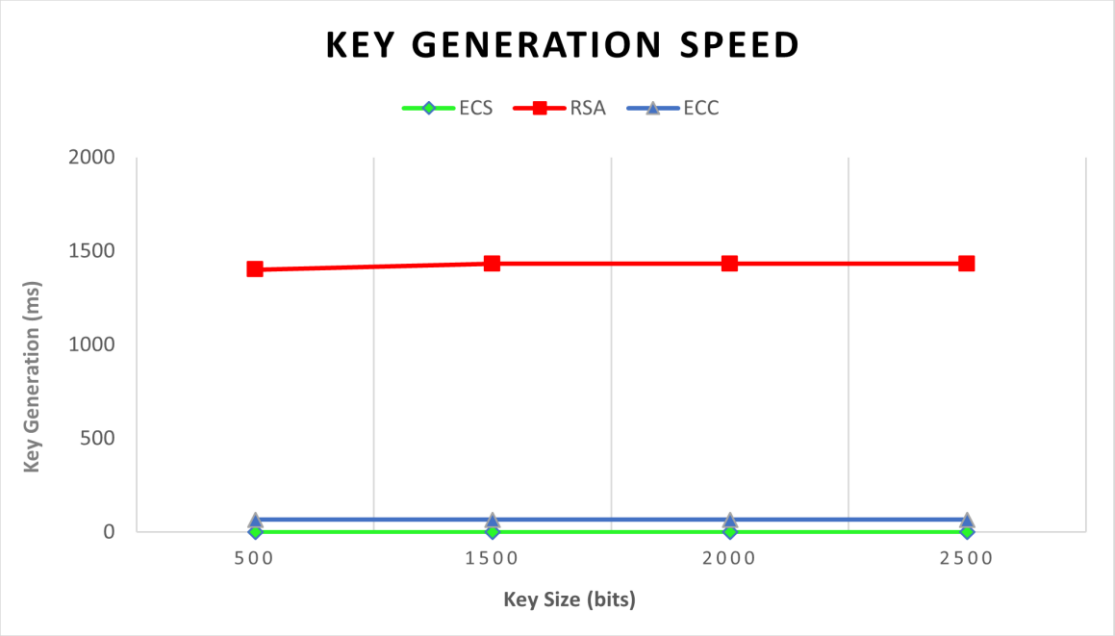

Figure 5.2: Comparison of key-generation speed for RSA, ECC, and ECS algorithms

The speed of key generation for the three (3) algorithms was monitored and compared. We can conclude that the performance of the ECS algorithm offers a more high-speed key generation than do the ECC and the RSA. The results indicate that the ECS algorithm is about three (3) times faster; with a key-generation speed of 19.8ms. However, it has also been noted that ECC is faster than RSA. According to Premnath (2013), current security standards for Smart Grid SCADA System communication specify the use of algorithms such as the RSA or ECC for securing communication. However, there are certain performance issues with cryptographic solutions of these specifications when applied to the Smart Grid SCADA system, with real-time constraints and hardware limitations. Based on this analysis and evaluation, it is evident that the ECS consumes minimal CPU power and battery resources which makes it suitable for constrained devices in which code size is a major limitation. The use of the ECS algorithm significantly reduces computational and memory overheads, making it suitable for SCADA systems with real-time constraints and hardware limitations.

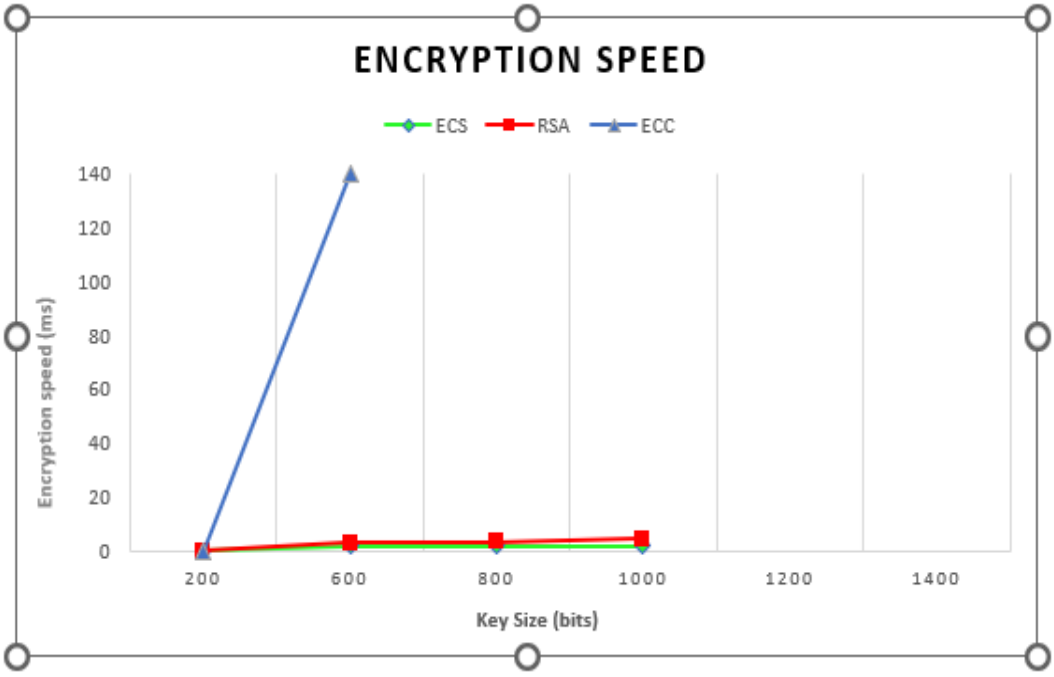

Figure 5.3: Comparison of encryption speed for RSA, ECC, and ECS algorithms

Encryption is the conversion of data into a form, called a cipher text, which cannot easily be understood by unauthorized people. The design and choice of the encryption scheme is the essential mechanism for protecting data confidentiality and integrity in any Smart Grid SCADA system (Premnath, 2013). The test was conducted for a randomly generated message of size 32 bytes. The performance of the NTRU is superior to that of the ECC. The results indicate that ECS block encryption is almost 73 times faster than the ECC block encryption. The ECS encrypts data at 1.4ms whereas ECC encryption speed is 140ms and RSA 4.32ms, respectively. In this case, as opposed to the key-generation speed, RSA outperforms the ECC algorithm. ECS uses the NTRUEncrypt which performs encryption and decryption by polynomial operations. Such can be implemented at higher speeds than for RSA encryption. The NTRUEncrypt carries out modulo exponentiation under a certain rule, and the ECC performs scalar multiplication for points on an elliptic curve (Premnath, 2013). The test results clearly prove that the ECS algorithm encryption achieves higher-speed processing than do both the RSA and ECC algorithms at the same security level.

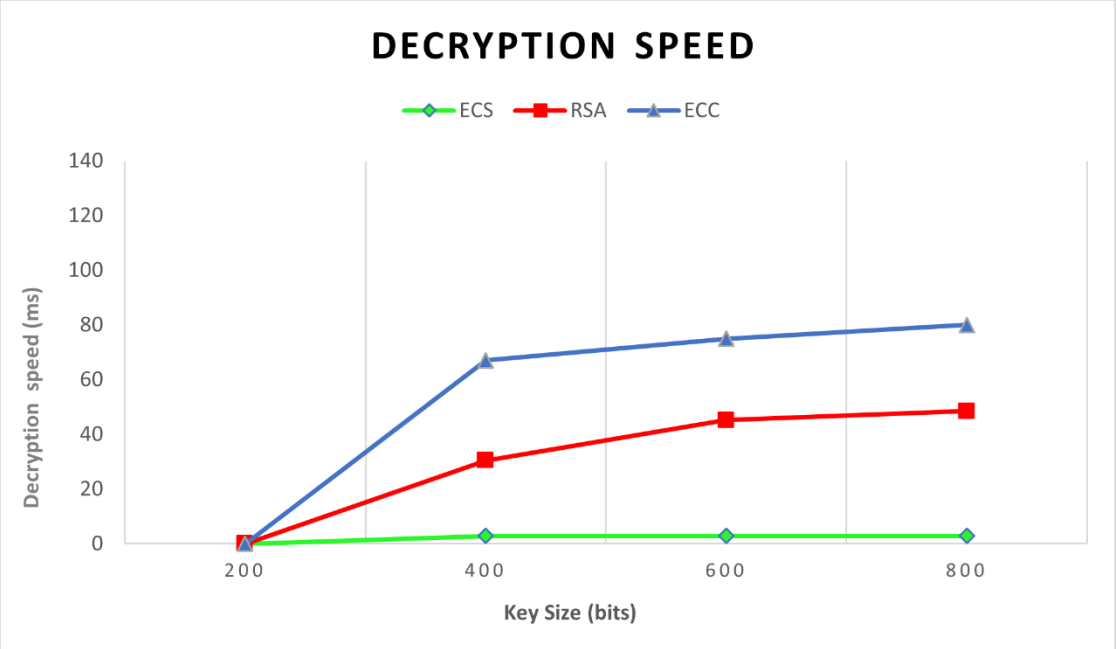

Figure 5.4: Comparison of decryption speed for RSA, ECC, and ECS algorithms

Encryption and decryptions are cryptographic methods used to achieve secure communication and information. Decryption is the process of converting encrypted data back into its original form, so that it can be understood by the intended recipient. Figure 5.3 presents the decryption speed results. The decryption speed parameter is responsible for the amount of time the algorithm takes to decrypt the key. The test was conducted for a randomly generated message of size 32 bytes. Observed results show that the total time taken for ECS decryption is 2.9ms. The ECS algorithm uses the NTRUEncrypt which is known to be the strongest, lightest-weight, and fastest known public-key cryptosystem. Conversely, the RSA resulted in 48.5ms and ECC at 67ms. The RSA decryption is expensive because it involves modular exponentiation of huge numbers.

5.4.3 Performance comparison of the RSA, ECC and ECS algorithms in terms of the amount of packet loss

The parameter measures the probability of packet loss during data transmission and communication between MTU and RTUs. Section 4.2.3 provides details of the simulation setup. The MTU initiates the communication

and then sends data (bytes) to RTU. Random bytes (data) have been transmitted between the MTU and RTU several times. The data/information has been sent and received several times between the MTU and RTU with a bandwidth of up to 5 Mbps. This allows the researcher to monitor and gather information about the amount of packet loss in amount sent and received during data transmission and communication.

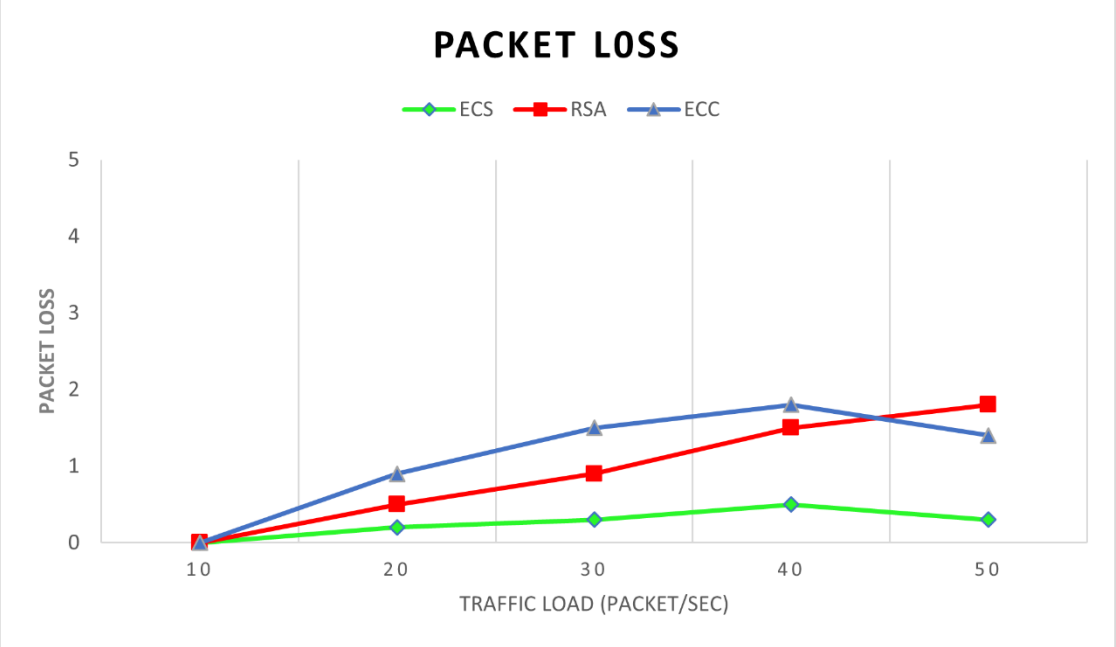

Figure 5.5: Comparison of packet loss for RSA, ECC, and ECS algorithms

The experiment was run several times; performance results were observed in both normal and abnormal communication/traffic. The test results show that similarly, the RSA and the ECC produced 1.8% of packet loss; while the proposed ECS algorithm reached a maximum of 0.5% of packet loss during a DoS attack. The goal of a DoS attack is to disrupt some legitimate activities, such as preventing RTUs from communicating with one another. When the RTU is affected due to a DoS attack, commands initiated from HMI/ MTU may not be able to reach the RTU. An attacker can make unauthorized changes to programmed instructions/status values in RTUs, resulting in damage to equipment, premature shutdown of processes, or even disabling of control equipment that could lead to a blackout. The performance evaluation clearly shows improvement in terms of availability attack. As mentioned in Section 2.2.1, in terms of the cybersecurity objectives, availability is priority one (1) for

the Smart Grid SCADA system. DoS targets availability. Therefore, packet loss becomes a vital parameter for testing to ensure that intended programmed instructions/status from the MTU do reach the RTUs without any malicious interruptions.

5.5 Summary

The chapter presented the results of the simulation scenario discussed in Section 4.1. Furthermore, the study discussed the effectiveness of the proposed ECS algorithm for the Smart Grid SCADA system. The analysed results were presented based on the following network parameters: key size, security level, speed of encryption and decryption operations, and packet loss. The NS-2 simulation tool was used to analyse results and compare the behaviour of the three cryptosystem algorithms: NTRU, RSA, and ECC; and the cryptographic techniques that help in improving the efficiency of cryptosystems through large integer multiplication.

Chapter 6: Conclusion and Future Work

6.1 Introduction

In this research study, an ECS algorithm for the Smart Grid SCADA system was designed by integrating the NTRU and Toom-Cook algorithms in order to improve the security of the Smart Grid SCADA system. The NTRU is one of the strongest, most lightweight and fastest known public-key cryptosystems. TheToom-Cook algorithm is a well-known best technique that helps improve the efficiency in cryptosystems. This integration was necessary because it provided a secure and speedier real-time critical application in the Smart Grid SCADA system by achieving higher encryption and decryption speed with the use of minimal computing power. Simultaneously, such ensured secure authentication during data transmission, and provided end-to-end secure communication. Furthermore, the proposed cybersecurity algorithm is resistant to quantum computing attacks and secure against transcript attacks.

Chapter 6 is structured as follows: A discussion is provided in Section 6.2 on how technical objectives were achieved. Section 6.3 provides an overall summary of the research. In Section 6.4 challenges met during this study are discussed. In Section 6.5 future work is presented; and in Section 6.6, the chapter is concluded.

6.2 Achievements of Objectives

All objectives defined in Section 1.5 of Chapter 1 have been achieved.

1. **To identify existing cybersecurity algorithms used to protect the Smart Grid SCADA System.**

In Section 2.6, the existing cybersecurity algorithms for protecting the Smart Grid SCADA system were identified and discussed. A detailed comparison of symmetric and asymmetric public-key cryptosystems was also provided. The drawback discovered in using symmetric cryptosystems was that the encryption only uses one key that all parties exchanging a message must know; therefore the key is the same on either side of the transmission. This poses a security risk and makes symmetric cryptosystems less secure than asymmetric public-key cryptosystems. Furthermore, it complicates the key-

management process as it requires secure exchange and update of secret keys amongst the communicating Smart Grid systems/devices. Therefore, this study concluded that it is much more secure to use asymmetric public-key cryptosystems due to the high level of security provided. The RSA and the ECC algorithms were identified in a study conducted by Jamel et al. (2017) as approved and best asymmetric algorithms used for protecting the Smart Grid SCADA system. Contrast and comparison of RSA, ECC, and NTRU (which is also a well-known public-key cryptosystem) was conducted in order to select the best-performing algorithm for this study − the NTRU was chosen. It was proved by Premnath (2013) and Jamel et al. (2017) that the NTRU is the best cybersecurity algorithm for protecting the Smart Grid SCADA system because it provides high-level security, and it is lightweight. In addition, it performs encryption and decryption at a higher speed with the use of minimal computing power; it is also resistant to quantum computing attacks. Moreover, in 2009, the NTRU cryptosystem was approved for standardization by the Institute of Electrical and Electronics Engineers (IEEE).

2. **To design an ECS algorithm for the Smart Grid SCADA system by integrating the NTRU and Toom-Cook algorithms to achieve secure end-to-end authentication, data integrity, confidentiality, and availability while reducing complexity.**

In Chapter 3, the study discussed how the ECS algorithm for the Smart Grid SCADA system was designed. Two (2) algorithms, namely, the NTRU and the Toom-Cook algorithms were integrated to ensure secure authentication and communication during data transmission. The NTRU was selected mainly because it is one of the strongest, most lightweight, and fastest known public key cryptosystems (Nitaj, 2015). It has two sub-algorithms, namely, the NTRUEncrypt and the NTRUSign. The NTRU is also a lattice-based cryptography and is also based on embedding messages in a polynomial ring, R, which sets it apart from other existing public-key cryptosystems, making it a very powerful algorithm. Another interesting and intriguing advantage of using NTRU which benefited this research study is that the NTRU algorithm, unlike other best-known algorithms such as the RSA and the ECC is resistant to quantum computing attacks. Integrating the Toom-Cook algorithm played a

huge role in this research study in improving the efficiency of encryption and decryption techniques to reduce complexity. According to Mera et al. (2020), the Toom-Cook algorithm is still one of the best techniques for multiplying big integers. The Toom-Cook algorithm also helped in overcoming the drawbacks in terms of the size of the encrypted key and the transmission rate. The integration of the NTRU and Toom-Cook algorithms was necessary for supporting a secure and faster real-time critical application in the Smart Grid SCADA systems. The encryption and decryption process achieved higher speed with the use of minimal computing power. A flowchart, as shown in Figures 3.1 and 3.2 was added to illustrate the authentication process and the flow of information between two Smart Grid SCADA devices; and how the NTRUEncrypt algorithm was applied to encrypt and decrypt data being transmitted over the network. The algorithm secured information and provided data integrity, confidentiality, and availability as per the cybersecurity objectives for the Smart Grid.

3. **To implement the proposed ECS algorithm in order to achieve secure end-to-end authentication, data integrity, confidentiality and availability, while reducing complexity.**

In Chapter 4, the ECS algorithm was implemented using NS-2.35. simulator software. The NS-2 simulator was used because it suits the choice of simulation for this study due to its flexibility and ability to test complex scenarios (Kabir et al., 2014). In addition, it supports a number of algorithms for routing; it is easy to add to it new protocols; and also, it has the distinct features of a good simulator. A new protocol was built and added to the NS-2.35. to enhance the security functions. This is the ECS algorithm. To achieve the availability of the cybersecurity objective, the simulation focused on the DoS attack made on the RTU. DoS attacks are considered one of the major threats against the Smart Grid SCADA system targeting availability. A successful attack on the RTU can lead to a blackout. To achieve confidentiality and integrity of the cybersecurity objectives the NTRUEncrypt and NTRUSign algorithms were implemented to ensure secure end-to-end authentication and data integrity during data transmission between nodes. The Toom-Cook was integrated with the NTRU algorithm to reduce complexity. The integration of

the Toom-Cook played a huge role in this research study, in creating high-speed encryption and decryption and very low computational power. Section 4.2.3 provides a detailed parameter setup for the implementation of the proposed ECS algorithm.

4. **To measure the effectiveness of the proposed ECS for protecting the Smart Grid SCADA system**

The performance of the proposed ECS algorithm for the Smart Grid SCADA system was evaluated based on the key size, security level, speed of encryption and decryption, and packet loss. To interpret the results graphically and interactively, NAM and Xgraph were used. Analysed results were displayed graphically using Xgraph, in which the behaviour of RSA, ECC, and ECS algorithms was shown. In Figure 5.2 the performance of key generation for RSA, ECC and ECS was compared and analysed. Results show that it took 17.6ms, which was 3 times faster than the RSA and ECC. In Figures 5.3 and 5.4, the performance of encryption and decryption for RSA, ECC, and ECS was compared and analysed. The results obtained from the simulation showed that the ECS is faster and superior to ECC on all levels of security in both encryption and decryption speed. Furthermore, the ECS encrypts and decrypts more messages than the RSA with the same key sizes; and the ECS provides more high-speed encryption and decryption than does the RSA.

In Figure 5.5 the performance of packet loss for the RSA, ECC, and ECS was compared and analysed. The results obtained from the simulation showed that the ECS had a packet loss of 0.5% which was less than for the RSA and the ECC. Therefore, the proposed ECS for the Smart Grid SCADA system is more efficient than the RSA and ECC because it produces less packet loss; and it performed key generation, encryption, and decryption at a higher speed with the use of minimal computing power; it also provided high-level security.

6.3 Summary of Research

The cybersecurity algorithm proposed in this research study improved the security of the Smart Grid SCADA system by reducing the complexity of encoding and decoding of the keys in cryptographic algorithms, thus improving the efficiency of the encryption and decryption operations. The proposed

algorithm was designed and then implemented using the NS-2 simulation software. The study introduced a NTRU and Toom-Cook algorithm to enhance and improve the cybersecurity of the Smart Grid SCADA system by ensuring secure authentication and communication during data transmission and by improving the efficiency of the encryption and decryption operation. Simulation results showed that the proposed ECS algorithm achieved high-speed encryption and decryption with the use of minimal computing power. Furthermore, the proposed cybersecurity algorithm also provided high-level security.

6.4 Encountered Challenges

The Smart Grid SCADA system incorporates very complex networks with interconnected and interdependent systems; and it also consists of infrastructure and devices spread over large geographical areas operating in real-time. Hence, the integration of the algorithms without any loopholes, and having to simulate the designed proposed ECS algorithm was a challenging task. Furthermore, the other challenge faced was learning the NS-2 language and the need for being familiar with writing scripting language.

6.5 Future Work

In this research study, it is assumed that the network throughput during the authentication process and data transmission was not monitored. The experimental evaluation also only focuses on the DoS attack on the RTU. Therefore, in the future, the network throughput and various simulation scenarios of DoS attacks on the network layer and transport layer can be conducted. Such would ensure that all aspects of protecting the Smart Grid SCADA system are covered and maintained. Furthermore, an in-depth analysis of the NTRUSign for authentication will be provided.

6.6 Summary

In this chapter, it was concluded that the proposed cybersecurity algorithm for protecting the Smart Grid SCADA system was able to improve the security of the Smart Grid SCADA system by ensuring secure authentication and communication during data transmission. In addition, the encryption and

decryption processes achieved high speeds with the use of minimal computing power. Furthermore, data integrity, confidentiality, and availability as per the cybersecurity objectives was achieved. The proposed ECS algorithm provided better performance than the RSA and the ECC in terms of key size, security level, and speed of encryption and decryption. Having achieved all the defined goals, it is considered that the ultimate purpose of this research study has been successfully achieved.

Bibliography

ABOOD, OG. & GUIRGUIS, SK. 2018. A Survey on Cryptography Algorithms. International Journal of Scientific and Research Publications (IJSRP), Vol. 8, Issue. 7, pp. 495-516.

ALOULA, F., AL-ALIA, A.R., AL-DALKYA, R., AL-MARDINIA, M. & EL-HAJJB, W. 2016. Smart grid cyber security: Challenges and solutions. International Journal of Smart Grid and Clean Energy, pp. 1-7.

ALSALEEM, MA., YASEEN, DS. & AZIZ, S. 2019. Efficiency comparison of Network Simulators. International Journal of Advanced Science and Technology, Vol. 28, Issue. 6, pp. 45-50.

AMIN, BMR., TAGHIZADEH, S., RAHMAN, S., HOSSAIN, J., VARADHARAJAN, V. & CHEN, Z. 2020. Cyberattacks in smart grid – dynamic impacts, analyses and recommendations. The Institution of Engineering and Technology (IET) 2020, Vol. 5, Issue. 4, pp. 321-329.

BLACKFOG. 2020. The State of Ransomware in 2020. [Online] Available from: https://www.blackfog.com/the-state-of-ransomware-in-2020/ [Accessed: 25/07/2020].

CASTELLANOS, S. 2017. Nascent Quantum Computing Poses Threat to Cybersecurity. CIO Journal. WSJ. Accessed, pp. 1-30.

CHHIMWAL. P., RAI, DS. & RAWAT, D. 2013. Comparison between Different Wireless Sensor Simulation Tools. IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834, p- ISSN: 2278-8735. Vol. 5, Issue. 2, pp. 54-60.

CYBEREDGE GROUP. 2021. Cyberthreat Défense Report. [Online] Available from: https://cyber-edge.com/wp-content/uploads/2021/04/CyberEdge-2021-CDR-Report-v1.1-1.pdf [Accessed: 08/10/2022].

CYBER EDU. 2018. What is OT Security? OT Security Defined, Explained, and explored. [Online] Available from: https://www.forcepoint.com/cyber-edu/ot-operational-technology-security [Accessed: 14/11/2018].

DAS, A. 2021. Cryptographic and Key Management Approach for Cybersecurity in Smart Grid. International Journal of Engineering Research & Technology (IJERT), Vol. 10, Issue. 7, pp. 63-72.

FENG, R., WANG, Z., LI, Z., MA, H., CHEN, R., PU, Z., CHEN, Z. & ZENG, X. 2020. A Hybrid Cryptography Scheme for NILM Data Security. Electronics. 9. 1128. 10.3390/electronics9071128, pp. 1-18.

GE Digital Energy Lentronics. Utility Telecomms Management: Foundation for Critical Utility Networks, Vol. 12.8.10, Issue. 1 [Online] Available from: https://www.gegridsolutions.com/newsletter/feb_2011/Product_News/UTIM_JMUX_v3.pdf [Accessed: 16/11/2018]

GHOSH, S. & SAMPALLI, S. 2019. Survey of Security in SCADA Networks: Current Issues and Future Challenges. IEEE Access, pp. 135812-135831.

ALESE, BK., PHILEMON, ED. & FALAKI, SO. 2012. Comparative Analysis of Public-Key Encryption Schemes. International Journal of Engineering and Technology, Vol. 2, Issue. 9, pp. 1552-1568.

GUO, Z., JIANG, W., SANG, N., & Ma, W. 2011. Energy Measurement and Analysis of Security Algorithms for Embedded Systems. School of Computer Science and Engineering University of Electronic Science and Technology of China Chengdu, China, pp. 54312-54328.

JAMEL. M., NSIRI, B. & BOUALLEGUE, R. 2017. Certificateless Scheme Based NTRU Cryptosystem for Ad-Hoc UWB-IR Network. International Journal of Wireless & Mobile Networks (IJWMN) Vol. 9, Issue. 6, pp. 53-69.

JANG, H., KIM, S., YANG, H. 2012. Optimized Security Algorithm for IEC 61850 based Power Utility System. Journal of Electrical Engineering & Technology. Vol. 7. [Online] Available from: https://www.idc-online.com/technical_references/pdfs/electrical_engineering/Optimized%20Security.pdf [Accessed: 20/09/2017]

KABIR, MH., ISLAM, S., HOSSAIN, J. & HOSSAIN, S. 2014. Detail Comparison of Network Simulators. International Journal of Scientific & Engineering Research, Vol. 5, Issue. 10, pp. 204-218.

LATEST HACKING NEWS. 2020. [Online] Available from: https://latesthackingnews.com/2020/02/17/south-african-nedbank-suffered-data-breach-affecting-1-7-million-customers/ [Accessed: 25/07/2020].

LINARDOPOULOU, T. 2020. Implementation and Analysis of the NTRU Algorithm in Java. Bachelor of Science Computer Science & Systems University of Washington Tacoma, pp. 1-33.

LORIYA, HT., KULSHRESHTA, A. & KELARIYA, DR. 2017. Security Analysis of Various Public Key Cryptosystems for Authentication and Key Agreement in Wireless Communication Network. International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 6, Issue. 2, pp. 267-274.

MERA, J.M.B., KARMAKAR, A. & VERBAUWHEDE, I. 2020. Time-memory trade-off in Toom-Cook multiplication: an application to module-lattice based cryptography. The International Association for Cryptologic Research (IACR), pp. 1-23.

NISTIR 7628 REVISION 1. Guidelines for Smart Grid Cybersecurity. Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements, pp. 1-66.

NITAJ. A. 2015. The Mathematics of the NTRU Public Key Cryptosystem, pp. 1-16.

PREMNATH, AP. 2013. Application of NTRU Cryptographic Algorithm for securing SCADA communication. UNLV Theses, Dissertations, Professional Papers, and Capstones, pp. 1-54.

REZAI, A., PARVIZ., KESHAVARZI, P. & MORAVEJ, A. 2017. Key management issue in SCADA networks: A review. Engineering Science and Technology, pp. 354-362.

SAIDALLAH, M., FERGOUGUI, A.EL. & ELALAOUI, A.E. 2017. A Survey and Comparative Study of Open-Source Wireless Sensor Network Simulators. International Journal of Advanced Research in Computer Science (IJARCS), Vol. 7, Issue. 3, pp. 1-7.

SAYED, K. & GABBAR, HA. 2017. SCADA and smart energy grid control automation. In book: Smart Energy Grid Engineering, pp. 481-514.

SEEMMA, PS., NANDHINI, S. & SOWMIYA, M. 2018. Overview of Cyber Security. International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), Vol. 7, Issue. 11, pp. 125-128.

SHAHZAD, A., MUSA, S. & IRFAN, M. 2014. N-Secure Cryptography Solution for SCADA Security Enhancement: Trends in Applied Sciences Research, pp. 381-395.

SHARMA, R., VASHISHT, V. & SINGH, U. 2020. Modelling and simulation frameworks for wireless sensor networks: a comparative study. The Institution of Engineering and Technology 2020, Vol. 10, Issue. 5, pp. 181-197.

VIJAYAPRIYA, T. & KOTHARI, DP. 2011. Smart Grid: An Overview. Scientific Research on Smart Grid and Renewable Energy (SGRE), pp. 306-310.

WANG, Y. 2012. Smart Grid, Automation, and SCADA Systems Security. 2012World Scientific Review, pp. 1-16.

WU, J. & KOBARA, K. 2012. Comparison of Tools and Simulators for Control System Security Studies. Research Institute for Secure System (RISEC) and National Institute of Advanced Industrial Science and Technology (AIST), pp. 1-6

XU, L. & LIU, G. 2012. Analyzing algorithms of information security. International Conference on Computer Science and Electronics Engineering, pp. 1-42.

YADAV, G. & PAUL, K. 2019. Assessment of SCADA System Vulnerabilities. IEEE Access, pp.1737-1744.

YUS, HA., MUSA, A., RAMLI, AQ. & RIDWAN, MI. 2012. Teleprotection Simulation Lab: Understanding the Performance of Telecommunication Aided Protection Systems under Impaired Telecommunication Network Conditions. IEEE International Conference on Power and Energy (PECon), pp. 1156-1183.

ZHE, T., & HUICHENG, X. 2015. Generating Technology Research on Operational Plan by Case-based-reasoning. 8th International Conference on Intelligent Computation Technology and Automation, pp. 304-402.