5-2025

Detection And Mitigation Of Distributed Denial Of Service (Ddos) Attack: Application To Smart Grid Communication Networks

Emmanuel Sunday Kolawole

DETECTION AND MITIGATION OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK: APPLICATION TO SMART GRID COMMUNICATION NETWORKS

A Dissertation

by

EMMANUEL SUNDAY KOLAWOLE

Submitted to the Office of Graduate Studies
of Prairie View A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2025

Major Subject: Electrical Engineering

DETECTION AND MITIGATION OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK: APPLICATION TO SMART GRID COMMUNICATION NETWORKS

A Dissertation

by

EMMANUEL SUNDAY KOLAWOLE

Submitted to the Office of Graduate Studies
Prairie View A&M University
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Approved as to style and content by:

Penrose Cofie Chairman of Committee	Cajetan M. Akujuobi Member
John Fuller Member	Justin Foreman Member
Emmanuel Dada Member	Annamalai Annamalai Head of Department
Pamela H. Obiomon Dean of College	Camille Gibson Interim Dean of Graduate Studies

May 2025

Major Subject: Electrical Engineering

COPYRIGHT PAGE

DETECTION AND MITIGATION OF DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK: APPLICATION TO SMART GRID COMMUNICATION NETWORKS

EMMANUEL SUNDAY KOLAWOLE

ABSTRACT

Detection And Mitigation of Distributed Denial of Service

(DDOS) Attack: Application to Smart Grid Communication Networks

(May 2025)

Emmanuel S Kolawole, B.S., Federal University of Technology, Akure;

M.S., Prairie View A&M University

Chair of Advisory Committee: Dr. Penrose Cofie

The Smart Grid is an improvement on the conventional grid that uses advanced communication methods and new technology for the production, transmission, and distribution of electrical power. The modern Smart Grid 's ability to function successfully depends heavily on its communication infrastructure. Today, the usage of communication technology promotes energy efficiency, coordination amongst all Smart Grid components, from generation to end users, and optimal Smart Grid functioning. The communication network of the Smart Grid exchanges data regarding the condition of its numerous integrated IEDs (intelligent electronic devices); however, there are always chances for attackers to interrupt utility resources, interfere with communication networks, or steal customers' intellectual property and private information due to the different amounts of IEDs connected across Smart Grid Communication Networks.

Additionally, as Distributed Energy Resources (DER) and dynamic loads become more prevalent, phase angle values that are crucial for Phasor Measurement Units (PMUs) change, and real-time control has emerged as a key tool for tracking power system

performance in today's Smart Grid technology. Because of their link to the Smart Grid 's communication network, Phasor Measurement Units devices are now susceptible to cyberattacks. Because of the recent global security incidents and new cyberthreats, this development has created new cyber-security issues for the Smart Grid and is a very worrying issue.

The effects of Distributed Denial of Service (DDOS) assaults on PMU data transfers over Smart Grid communication networks in the form of NetFlows were carefully examined in this study. For the first time in the literature, a combination of the Secure Network Analytics (SNA) tool, Intrusion Detection System, and firewall were used to model the DDOS attack in the Smart Grid 's communication network. Additionally, risk reduction and good security hygiene are enhanced by employing the Secure Network Analytics (SNA) tool to establish a security baseline for the Smart Grid system.

The research findings are in contrast with those found in previous studies. Our findings demonstrated that this research strategy outperformed previous approaches in the literature in terms of mitigating and detecting DDOS attacks.

Index Terms: Detection and mitigation, distributed denial of service (DDOS) attack, distributed energy resources, firewall, intrusion detection and prevention systems, phase measurement units, Smart Grid system.

DEDICATION

This dissertation work is dedicated to my parents, Mrs. and Late (Chief.) Michael Sunday Abere, who always loved me unconditionally and whose good examples taught me to work hard for the things that I aspire to achieve. This work is also dedicated to my lovely wife, Moronkeji, my children, and friends who have been a constant source of support and encouragement during the challenges of graduate school and life. I am thankful for having them in my life. Thank you for all your support along the way.

ACKNOWLEDGMENTS

It gives me an immense amount of pleasure to convey my special thanks to Dr. Penrose Cofie, Dr. Cajetan Akujuobi, and Dr. Warsame Ali for mentoring me with their vast amount of knowledge and enthusiasm, inspiration, persistent encouragement, and moral support throughout this research work. Working with them has been of tremendous help in developing my ability to perform qualitative research.

I also want to thank the other advisory committee members. They are Dr. Justin Foreman, Dr. Emmanuel Dada, and Dr. John Fuller for their pieces of advice on the general layout of the research work. Their consistent and priceless inputs are highly appreciated.

Once again, I wish to express my special thanks to the chair of my committee, Dr. Penrose Cofie and Dr. Warsame Ali, for their unselfish guidance since the very first day of my admission in the Department of Electrical and Computer Engineering.

I am especially grateful to my lovely wife, Moronkeji, my children, my parents, Mrs. and Late (Chief.) Michael Sunday Abere, my siblings, and friends for their encouragement, emotional support, and prayers. Finally, I take this opportunity to thank all the members of staff and the entire students of the Electrical and Computer Engineering Department, who in one way or the other, made my Ph.D. program at Prairie View A&M University worthwhile.

TABLE OF CONTENTS

NOMENCLATURE

US	United States
DDOS	Distributed Denial of Service
DOS	Denial of Service
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
FW	Firewall
SW	StealthWatch
FC	Flow Collector
FS	Flow Sensor
PFS	Flows Per Seconds
SMC	SNA Management Center
WAMS	Wide area Monitoring Systems
VM	Virtual Machines
SG	Smart Grid
WAN	Wide Area Network
NAN	Neighborhood Area Network
HAN	Home Area Network
A&M	Agriculture and Mechanical
PLC	Programmable Logic Controller
GNS3	Graphic Network Simulator Version 3
SNA	Secure Network Analytics
PMUs	Phasor Measurement Units
DER	Distributed Energy Resources
IEDs	Intelligent Electronic Devices
DG	Distributed generation
DCC	Data and Control Center
SCADA	Supervisory Control and Data Acquisition
OMS	Outage Management Systems
DLR	Dynamic Line Rating
FACTS	Flexible AC Transmission Systems
NIST	National Institute of Standards and Technology
RTOs	Regional Transmission Organizations
ISOs	Independent System Operators
IP	Internet Protocol
MPLS	Multiprotocol Label Switching
CCTV	Closed-Circuit Television
QOS	Quality of Service
VOIP	Voice Over Internet Protocol
NSPs	Network Service Providers
AMI	Advanced Metering Infrastructure
DA	Distribution Automation

DS	Distributed Storage
DG	Distributed Generation
EVs	Electric Vehicles
MDMS	Meter Data Management System
DMS	Distribution Management Systems
HEMS	Home Energy Management Systems
GHG	Greenhouse gas
WEMs	Wholesale Energy Markets
RTOs	Regional Transmission Operators
REM	Retail Energy Market
WASA&C	Wide Area Situational Awareness and Control
AI	Artificial Intelligence
IOT	Internet of Things
DOE	Department of Energy
RE	Renewable Energy

LIST OF FIGURES

FIGURE Page

LIST OF TABLES

TABLE Page

1. INTRODUCTION

The integration of communication and computer networks for the gathering of power usage statistics, local energy consumption, and other measured data across the grid system is the result of the development of Smart Grid technology [1]. In addition to controlling and optimizing the production and distribution of storage systems and consumers, the Smart Grid facilitates the two-way flow of power and information. The majority of the grid's vital infrastructure components are now accessible over the internet and function in a digital environment, which leaves them open to assaults.

Meanwhile, thanks to artificial intelligence (AI), cyberattacks are becoming more sophisticated. Because important infrastructures around the world have been the target of cyber-attacks and security events, this development has created new cyber-security concerns and is extremely alarming. The grid's operating technology made it possible to access the grid remotely more and more, which could cause operational disruptions. Because industrial control systems rely on conventional networking protocols, the so-called grid is susceptible to cyberattacks. Similarly, it is vulnerable to consumer Internet of Things (IoT) gadgets that are linked to the grid. The current grid is susceptible to cyberattacks since it relies on GPS to function. Because of the frequent cyberattacks that cause blackouts and intellectual property loss, it is now essential to secure the Smart Grid communication networks. According to research, the Smart Grid 's core communication system is its most important component [2]. Smart Grid computers and communication

---

This dissertation follows the style of the *IEEE*.

system is its most important component [2]. Smart Grid computers and communication networks handle volumes of important data. Therefore, having a safe and dependable Smart Grid communication network infrastructure is crucial [3].

Unidirectional (one-way flow) power flow from primary power plants to the customers via the distribution and transmission networks is the foundation of the conventional grid. Green renewable energy sources like solar and wind energy have the potential to replace fossil fuels due to the world's growing demand for electricity and the effects of global warming [4]- [5]. Significant drawbacks of the old grid include its limited control, lack of automated analysis, delayed reaction to rapidly fluctuating loading, and poor coordination between generated and consumed energy. In recent years, this has led to a number of significant blackouts or power outages. The next generation of electricity distribution grid technology, known as Smart Grid technology, aims to address the issues with the legacy grid [6]- [7]. The Smart Grid provides and enhances better monitoring, optimization, and protection of all grid components, including transmission, generation distribution, and consumers, through the use of two-way communications, sophisticated sensing and processing infrastructure, digital technologies, and software technology. The purpose of the two-way communication is to give energy users fast access to accurate real-time invoices and rates. Real-time data on energy consumption by consumers can be sent to the grid operator [8].

The most serious and devastating online threat to Smart Grid is Distributed Denial-of-Service, or DDoS, which can cause blackouts all around the world. The federal government is doing everything it can to promote the protection of the US power system from cyberattacks. Bloomberg reported that the Biden administration had a strategy to

methodically enhance power providers' ability to protect themselves against cyberattacks from nations including China, Iran, Russia, and North Korea. Additionally, the Department of Energy (DOE) proposed to use more than $20 billion in federal funds to modernize the US electrical infrastructure, with $45 million of those funds designated for improvements in cyberattack mitigation. These enhancements will concentrate on automated techniques for identifying and addressing grid vulnerabilities, such as cyber security and sophisticated software solutions, with $25 million allocated to cyber tools for grid defense. The goal of this research project was to develop methods for accomplishing the aforementioned mitigation effect.

Russian cyberattacks caused the Ukraine power grid to lose electricity in December 2015, 2016, and 2022. As illustrated in Fig. 1, both attacks caused nationwide blackouts. Additionally, as seen in Fig. 2, a cyberattack on the US Power Grid left millions of homes without electricity. Cyberattacks by North Korea, Russia, China, and Iran are allegedly capable of affecting vital infrastructures and causing catastrophic and extensive blackouts in the United States.

Fig. 1. Hackers shut down Ukraine Power Grid [9].

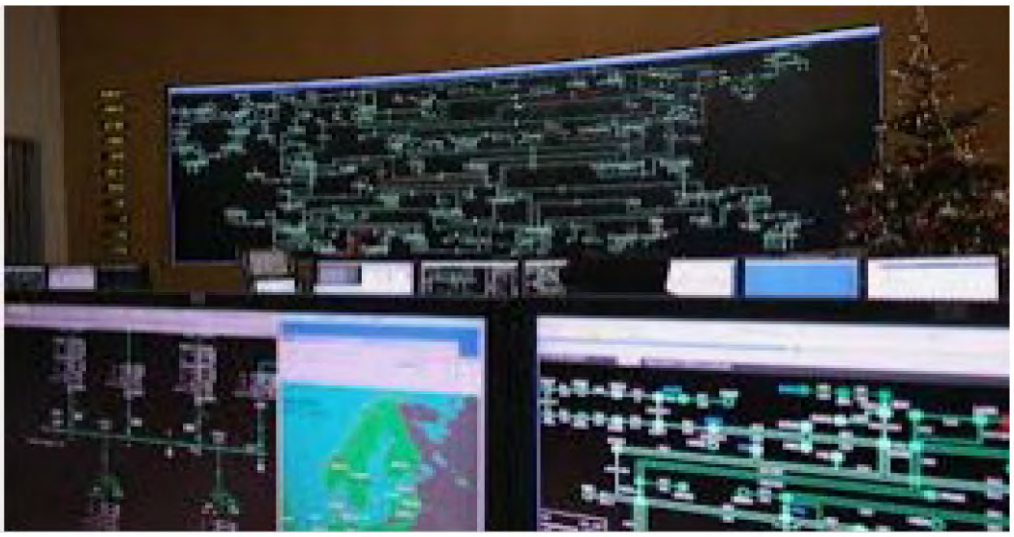


Fig. 2. Major Attack on U.S Power Grid [10].

Adversaries can use network traffic flooding, communication channel jamming, and networking protocol attacks to initiate a DDoS attack on the Smart Grid 's communication channels. The measurement packets supplied from the sensors over this channel will be lost if the attack is successful. Furthermore, a breach of national security and financial losses in the electrical market can also be caused by cyber-security problems. Our simulations show the DDoS attacks that can cause the power systems to become unstable. Studies are carried out in this work to evaluate how DDoS attacks affect the dynamics of communication networks in Smart Grid s.

1.1 Statement of the Problem

The Smart Grid system is an intelligent grid that uses information and communication technologies implemented through smart meters and a control system to manage dispersed generation and surge loading. Smart Grids are susceptible to cyberattacks since they are integrated into open communication infrastructures to facilitate massive data interchange. Cyberattacks on Smart Grids include virus propagation,

distributed control device vulnerabilities, cyber-system failures, and adversaries gaining access to private customer data. The generation, transmission, distribution, and consumers may all be the targets of the threats. Distributed Denial of Service (DDoS) assaults on electric Smart Grid communication networks have become a major global problem in recent years. This has resulted in the loss of numerous material goods and intellectual property Additionally, by creating DDoS attack sequences that jam communication channels, assault networking protocols, and flood network traffic, attackers might cause instability in the power system. Therefore, it is difficult to identify and stop DDOS attacks in Smart Grid communication networks.

1.2 The Dissertation's Purpose

By using an enhanced Secure Network Analytics tool, this study sought to identify and counter Distributed Denial of Service [DDoS] attacks that are applied to Electrical Smart Grid communication networks. With its "Encrypted Traffic Analytics [ETA]" feature, the SNA tool may also identify malware or attacks in encrypted traffic without the need for decryption. When data in the form of NetFlow is exchanged over Smart Grid Communication Networks, it focuses on the practical methods of detecting and mitigating DDoS attacks without causing any harm to internal systems or system shutdowns or blackouts as a result of the attack. The telemetry gathered from the grid environment by the Flow Sensor and Flow Collector is shown on the management console via SNA. In order to prevent the shutdown of all grid systems, the SMC notifies the administrator of any unusual activity, particularly the "DDOS" attack in this use-case, so that it may be addressed right away. Based on the many alarms produced by each dashboard index interpretation, SNA employs baseline methodologies to identify questionable activity in

the environment. Unfortunately, there is currently no technology that can totally prevent hackers from accessing business networks. Assume, in the meanwhile, that a company has the appropriate group of committed individuals, technology, and procedures in place to frequently monitor its surroundings. The security team will then be better prepared to spot and thwart any attack while it is still underway. By doing this, they may steer clear of the expenses and catastrophic outcomes that come with a data breach.

1.3 Communication Networks' Function in Modernizing the Grid

These days, only SCADA and teleprotection software can monitor and regulate the grid. By exploiting the communication between the substations connected by the transmission line, teleprotection, as it is known, is used to remotely detect electrical faults on a transmission line. The faults will then cause the circuit that supplies them to trip. In order to take appropriate grid control action, SCADA systems are utilized to measure currents, voltages, and other characteristics at various places in a substation with the utility Data and Control Center (DCC). Analog and relay-based communication systems are being replaced by digital and mechanical networks, and intelligent electronic devices (IEDs) are replacing outdated electric gadgets.

Additionally, utilities are increasingly using automated meter readings to remotely scan customer meters. Typically, meter measurements are solely utilized to make invoicing easier. Smart Grid accelerated the modernization of the power grid. By using the more recent IEC 61850 set standards, utilities are updating their substation automation from legacy systems, protocols, and networks [11]. Applications between substations are being supported by the implementation of new communication technologies [12].

Upholding power standards and quality is another aspect of modernizing the grid. In general, power quality relates to delivering electricity within permitted voltage and frequency limits. Lastly, as new apps and endpoints are added, the grid's security and dependability must be preserved.

1.4 Domains of the Smart Grid and How They Interconnect

Interconnection between entities, that is, users, systems, and applications- within utility locations and with numerous organizations is supported via Smart Grid communication networks. It is possible to classify these structures into broad "domains," as illustrated in Fig. 3.

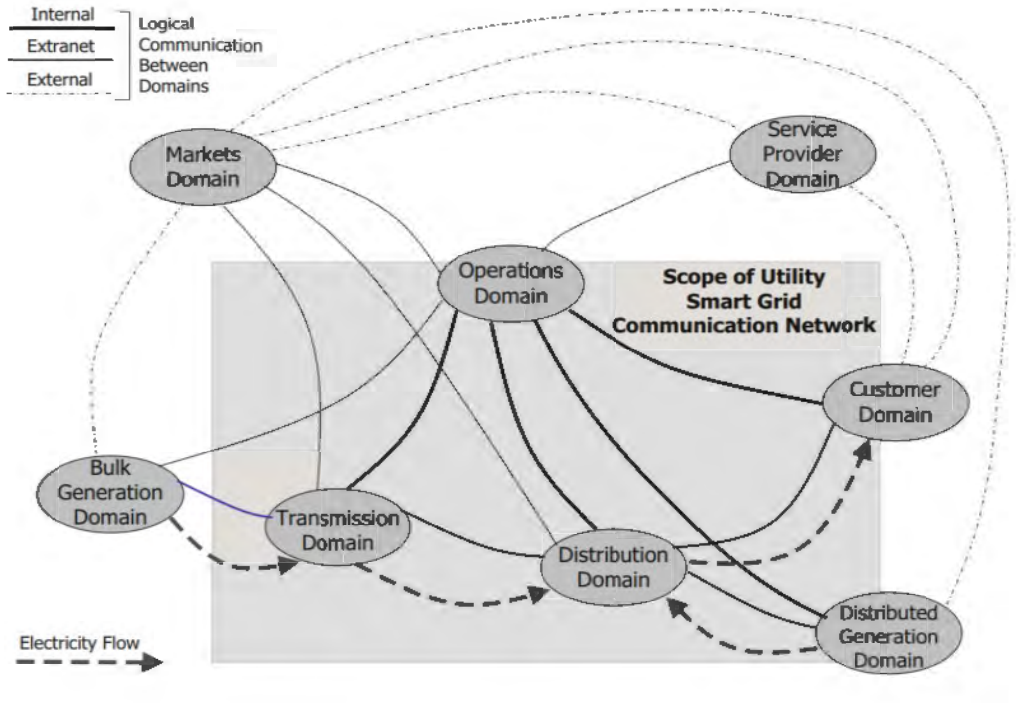


Fig. 3. Smart Grid domains and how they relate to one another.

The National Institute of Standards and Technology (NIST) in the United States served as the model for Fig. 3. Electricity typically travels from bulk generation sources to the transmission system of transmission lines and from transmission substations to the

distribution system. After that, it is sent to the clients who are energy users, via feeders to distribution substations. With the Smart Grid, DG sources that are connected to the distribution grid also produce electricity.

Power grid operations are carried out by a few non-utility entities, such as businesses that oversee the interconnection of several utility networks. These businesses include the Regional Transmission Organizations (RTOs) and Independent System Operators (ISOs), which oversee the interconnection of North American grids. In this way, the operations domain might not be fully included in the boundaries of a utility Smart Grid communication network.

The utility operations area includes grid applications for transmission and distribution system monitoring and control, as well as grid links to consumers and DG. Monitoring of the utility's bulk generation will be necessary for some of these applications since they call for market participation. Lastly, the service provider domain includes communications with service providers outside of the utility.

1.5 The Smart Grid Communication Network's goals

Supporting traffic flow for all applications, including current utility applications and future Smart Grid applications, is the primary goal of the Smart Grid communication network. It is inefficient to build separate networks to support each new application because doing so makes managing many networks and building new ones more difficult. The additional capital and operating expenses required to support new applications are extremely little when using an integrated network. The following sections list some of the goals of the Smart Grid communication networks.

Standards-Based Network: standardized communication networking standards ought to be the foundation of the Smart Grid communication network. This lowers costs by enabling the utilities to purchase compatible network products from several vendors. Reliance on single-vendor solutions, which can become very costly to maintain over time, can be effectively eliminated with multi-vendor goods.

IP or Internet Protocol: the most widely used network protocol for data network transmission nowadays is Internet Protocol (IP). Regardless of the logical or physical connection technologies that provide these connections, IP was created to link network endpoints. Many network devices are offered at cheap prices thanks to IP's general and overall support. Additionally, there has been a group effort to create new techniques, guidelines, and resources to improve IP network operations, engineering, and management performance. Utility SCADA networks have been switching from serial to IP connectivity in recent years. IP communication to utility DCCs is also supported by upcoming Smart Grid technologies like distribution automation and AMI.

MPLS or Multiprotocol Label Switching: additionally advantageous to the network is Multiprotocol Label Switching (MPLS) technology. In addition to integrating network support applications that IP networks are unable to support, MPLS can provide numerous other benefits. Network security is facilitated by MPLS services' support for application endpoints and traffic isolation between "closed user groups" of applications. MPLS offers faster network outage recovery and increased network dependability. Legacy systems, interfaces such as serial interfaces and protocols can all be supported by MPLS services on the same integrated Smart Grid IP communication network. Additionally, by supporting many protocols, including quality of service capabilities which are necessary to

deliver high-priority traffic in a crowded network, it offers quality of service (QoS) capabilities in multiservice networks.

Systems, Applications, and Legacy Protocols Support: in order to save replacement costs, utilities may occasionally be more likely to support legacy systems, applications, and protocols that are not based on IP. Additionally, until their IP-based alternatives have been sufficiently evaluated to satisfy their standard criteria, several utilities may continue to employ conventional systems. For instance, in order to save money on replacing the current systems or devices, the utility company might not want to upgrade a functional SCADA RTU that communicates to the SCADA control system via a serial connection. Since the present IP network is unable to handle the high latency needs of the teleprotection traffic, a utility company will opt to maintain its teleprotection applications from the IP base in a crowded IP-only network. In conclusion, any legacy or conventional protocols, systems, and applications must be supported by the network for a certain amount of time.

Network Performance: in an integrated networking environment, the network must be able to serve the optimal needs of the different separate applications. The end-to-end delay requirements for traffic transported via the conventional network architecture are an example of this. In order to meet each application's end-to-end delay needs during network outages and regular operating situations, network quality of service design must offer the order and delay performance necessary.

Network Reliability: ensuring constant power availability for customers and maintaining high power grid reliability are the key objectives of every utility company's operation. In this regard, communication networks are highly effective since they offer

real-time monitoring and grid control. Thus, it is crucial to maintain high levels of network reliability. Additionally, the assurance requirements for certain mission-critical grid applications are more stringent than those of communication networks that enable voice (VoIP) and corporate data applications.

Network Security: network security protects the entire integrity of the electrical grid in addition to the safety of network operations. There will be severe financial consequences for each outage of electricity brought on by cyberattacks on the equipment that manages and keeps an eye on the electrical grid. As a result, every nation views its electric grid as a vitally important piece of infrastructure. Implementing software security controls and hardware security measures such as firewall access lists, intrusion detection and prevention systems, and security operation policies and procedures should be in line with utility security policies. Additionally, apps may gather private and sensitive consumer information from smart meters and other gadgets. Data privacy is, therefore, seen as a crucial component of network security.

Scalability: the scalability of network design refers to the ability to introduce new Smart Grid applications with minimal changes to the physical network configuration. Usually, when a new application is introduced, the utility simply adds a small number of new endpoints. It should be feasible to add a significant number of application endpoints with careful design and capacity management. A few network configuration adjustments should also be necessary when adding a small number of network endpoints, such as smart meters, several DG locations, and a substation.

Effective Routing and Traffic Aggregation: an integrated IP network has the advantage of having a network architecture that considers the network as a whole. Depending on the amount of traffic generated and the destination locations, traffic is aggregated at multiple places throughout the network to achieve beneficial economies. As a result, connecting the particular pairs of application endpoints via exclusive, expensive, inefficient, and circuit connections is optional. The most efficient way for data to move across a network from its source to its target endpoint is provided by traffic routing. Depending on network circumstances, like a link or element failure, routing protocols may alter these network pathways.

Secure Network-Based Data Management: the latest data management technologies can facilitate secure network-based data management. Implementing safe data management systems that can offer minimal delays when the data is retrieved is necessary due to the increase in the volume of data collected in the Smart Grid for usage by the majority of applications.

Unified Network Management: to accelerate and promote the development of the Smart Grid network, the existing collection of networks must first be combined into an integrated network. Every time new applications and endpoints are added, it will continue to change. Presumably, the network will be built using network components (switches, routers) from several vendors. Additionally, utilities should implement operations support systems (OSSs) that will integrate with various suppliers' element management systems to offer a single end-to-end network management solution for network provisioning, configuration, and troubleshooting.

Well-Ordered Network Transformation: the Smart Grid network transformation process can be made more efficient and less expensive by implementing MPLS services. Since the intelligent grid has not yet been established, the network architecture and first network design should incorporate the current utility assets, for example, fiber plants. Network transformation requires careful planning to reduce network disruptions. It is never a one-step procedure.

Flexibility of Ownership of Network Segments: the communication network architecture must give the utility company the flexibility it needs to determine how NSP networking services and utility-owned networks should interact. The assumed Smart Grid communication network may consist of both utility-owned and NSP-provided network parts, depending on the utility company's existing networking assets.

1.6 An Overview of the Dissertation

This study's remaining sections are arranged as follows: the communication infrastructure, technologies, applications, and literature studies of Smart Grid technology is presented in Chapter 2. Along with giving the foundation knowledge needed to comprehend the remainder of the study, this chapter also describes the fundamental Smart Grid communication protocols. The cyber-security concerns with electrical Smart Grid technology are covered in Chapter 3. This chapter also discusses many security concerns with Electrical Smart Grid technology, including DDOS assaults, new technologies, consumer ignorance, and man-in-the-middle attacks.

The approach and modeling of Smart Grid technology for mitigating DDOS attacks with SNA tools and suitable IP addressing are the main topics of Chapter 4. It describes the encryption capabilities of SNA tools and displays various virtual machines created for

the simulation. The simulation results of the suggested attacker combat techniques are the main topic of Chapter 5. It demonstrates the efficacy of the approach by comparing the outcomes before and after a DDOS assault. The dissertation concludes with a summary and contributions in Chapter 6.

2. A LITERATURE REVIEW

Our houses and businesses are powered by the Smart Grid, a contemporary network system of wires, meters, and transformers. When we plug in our gadgets and flip on the light switch, we establish a connection with the Smart Grid. The 1890s saw the development of the electrical grid, which changed as our technology advanced [13]. More than 9,000 electricity-producing units, more than one million megawatts of generating output, and more than 300,000 transmission links make up the current Smart Grid. The operation network, business network, and consumer network are the three primary networks that make up Smart Grid. There are distinct communication subnetworks for each of these three networks, each with a distinct purpose. To keep the grid functioning, the power providers utilize the first is the operation network. The players in the energy market use the second one, the business network, to efficiently manage the market and supply electrical services to all of the customers [14].

The results of various recent studies and the drawbacks of their approaches to Smart Grid cyberattack mitigation are listed below.

- **Research article**: Asri, S., Pranggono, B. Impact of Distributed Denial-of Service Attack on Advanced Metering Infrastructure; Wireless Personal Communications 83(3), 2211– 2223 (2015).

Limitations: the NeSSi 2 Tool was used for the research, and the findings demonstrated that a sufficiently big DDoS attack may compromise the entire grid. But it wasn't until the server was taken offline that the effect became apparent.

- **Research article**: Fang et al. The contributions of cloud technologies to

Smart Grid. The findings included an overview of how various cloud computing technologies were applied in Smart Grid s, followed by a quick look into cloud security.

Limitations: no specific tool or framework has been utilized or suggested to improve the Smart Grid 's security, and concerns about cloud security were commonly surveyed.

- **Research article**: Abdul Rahman et al. Smart Grid security challenges:

Classification by sources of threat. Journal of Electrical Systems and Information Technology, Vol. 5, No. 3, pp. 468-483, Dec. (2018). The authors extensively categorized and studied the security issues with Smart Grid s according to the sources of threats.

Limitations: the suggested NIST framework needs to be narrowed down to a specific area, such the creation and deployment of Smart Grid s, because it is quite generic and ambiguous. To be honest, the writers had to offer a precise method and resolution for the security issues with Smart Grid s that were discussed in the earlier parts.

- **Research article**: Sgouras et al. (2014) Cyber Attack Impact on Critical Smart Grid Infrastructures. ISGT pp. 1–5. IEEE (2014). The findings demonstrated that the DoS attack on the server resulted in service degradation and a decrease in the quantity of TCP packets sent to smart meters.

Limitations: A DDoS attack on the server apparently reduced connections with about 90% of the smart meters, according to the research, which was carried out using the OMNeT++ Tool. The limitations of the work are comparable to those of Asri's study.

Research article: Yilmaz et al. (2018) Cyber Security in Industrial Control Systems: Analysis of DoS Attacks Against PLCs and the Insider Effect. Smart Grid According to the authors' research on the potential for denial-of-service (DoS) attacks on

PLCs, if a PLC's IP address is known, it can be targeted from both inside and outside of its network.

Limitations: PLC and TIA Portal Management Software Tools were used in the investigation. The findings demonstrated that, even with a small number of disturbances, the network was rapidly degraded. The results are comparable to those of Asri's study as well.

Research article: S. Premkumar. and V. Saminadan., "Impact of Denial of Service (DOS) attack in Smart Distribution Grid Communication Network," *International Journal of Applied Engineering Research,* vol. 12, no. 4, pp. 4443-4447, 2017.

Limitations: The GNS3 Tool was used for the research, and the simulation results unequivocally demonstrate how vulnerable a Smart Grid power system is to DDOS attacks. The destination server was overloaded, unavailable, and shut down after repeated flooding. This was due to the inability of any appropriate and trustworthy tool or mechanism to identify, track, and lessen DDOS attacks. It is evident from the aforementioned talks that the majority of research efforts were unable to prevent the attacks, which resulted in server blackouts and shutdowns. The DDOS attempt was identified, stopped, and confined in the case of our suggested SNA tool without compromising the server or resulting in a shutdown.

2.1 Communication Infrastructure for Smart Grids

Three different network types serve as the foundation for the communication network infrastructure of the Smart Grid: wide area networks (WAN), neighborhood area networks (NAN), and home area networks (HAN). The communication network infrastructure of the Smart Grid is depicted in Fig. 4 below.

A HAN is a kind of network that is set up and run in a constrained space, typically a small home or business. In contrast to the other two networks, the HAN has a modest transmission data rate. A HAN is a wireless or wired broadband Internet connection that is shared by several people. Through a network connection, this improves communication and resource sharing between PCs, mobile devices, and other devices. All smart home appliances that use energy and smart meters can be linked to HAN in a standard Smart Grid deployment. The smart meters receive and process the device's data via HAN. Either Ethernet or ZigBee technologies can be used to create HAN, which enables effective home energy management. HAN is for end users' homes or places of business.

Conversely, NAN is a network type that functions within a hundred-meter radius. Data on the energy consumption of each home can be sent to the NAN network by connecting many HANs to a single NAN. Data analysis for identifying patterns in energy generation-demand and consumer charging depends on this data storage. It can be carried out by cellular, Wi-Fi, and PLC technologies.

WAN, which is made up of numerous NANs and Local Distribution Companies (LDCs), is set up and runs over a wide ten-kilometer radius. It offers channels of communication for information sharing between NANs and utility systems. Furthermore, WAN is used for communication between all of the Smart Grid 's components, including transmission and distribution, operator control centers, and renewable energy production. The WAN has a very high transmission data rate of up to a few Gbps and can be implemented via Ethernet networks, WiMAX, 3G/LTE, and microwave transmission. In conclusion, a wide area network (WAN) facilitates information transfer between the utility systems and NANs by offering interfaces or communication channels. In this instance,

several HANs are connected to the local access points via NAN (Neighborhood Area Network). This communication is for end-user home or business communications in the context of HAN (Home Area Network) [15]. Fig. 5 below shows the general Smart Grid Network Architecture modules or components with various reference points.

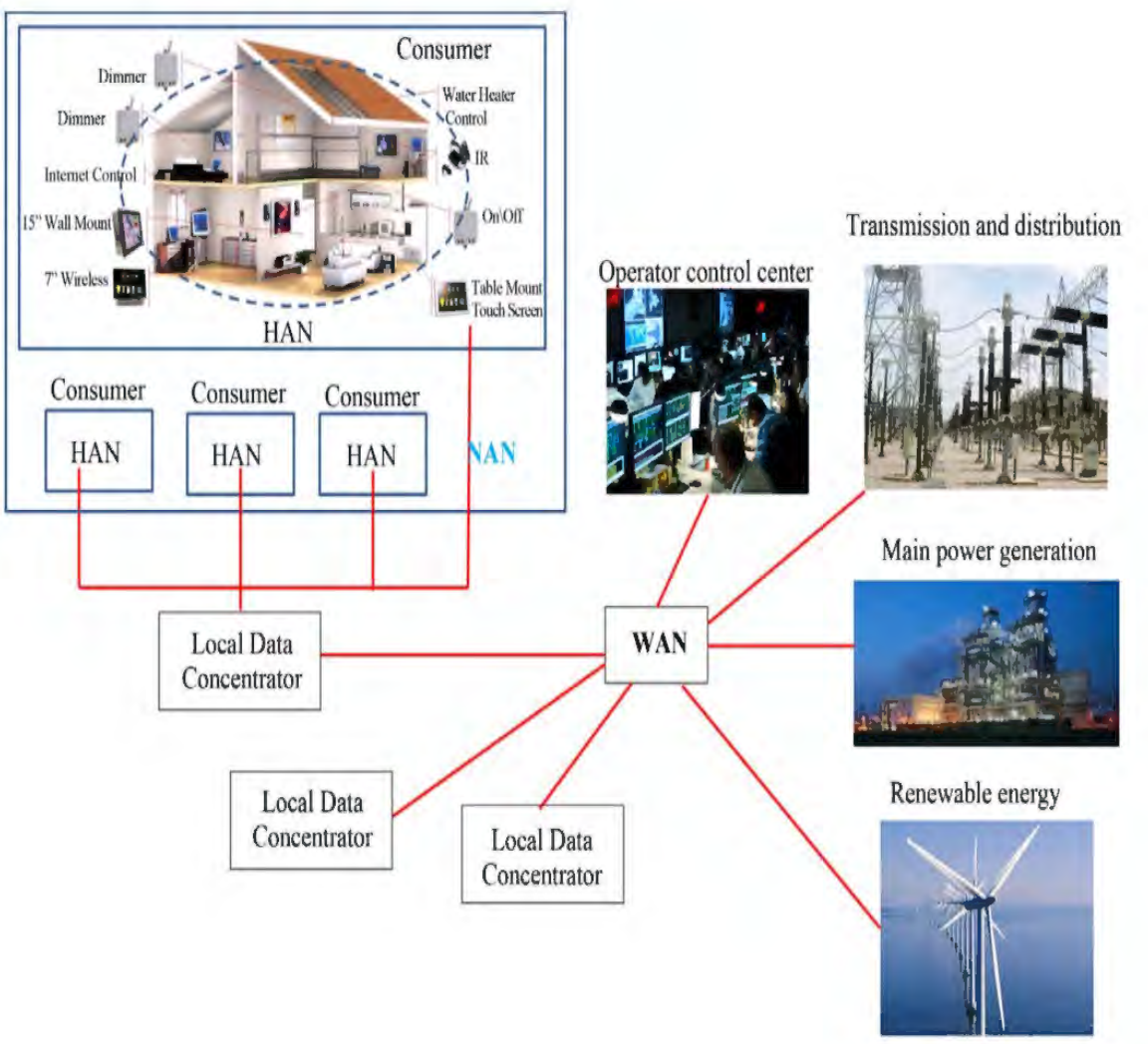


Fig. 4. Infrastructure for Smart Grid Communication Networks [16].

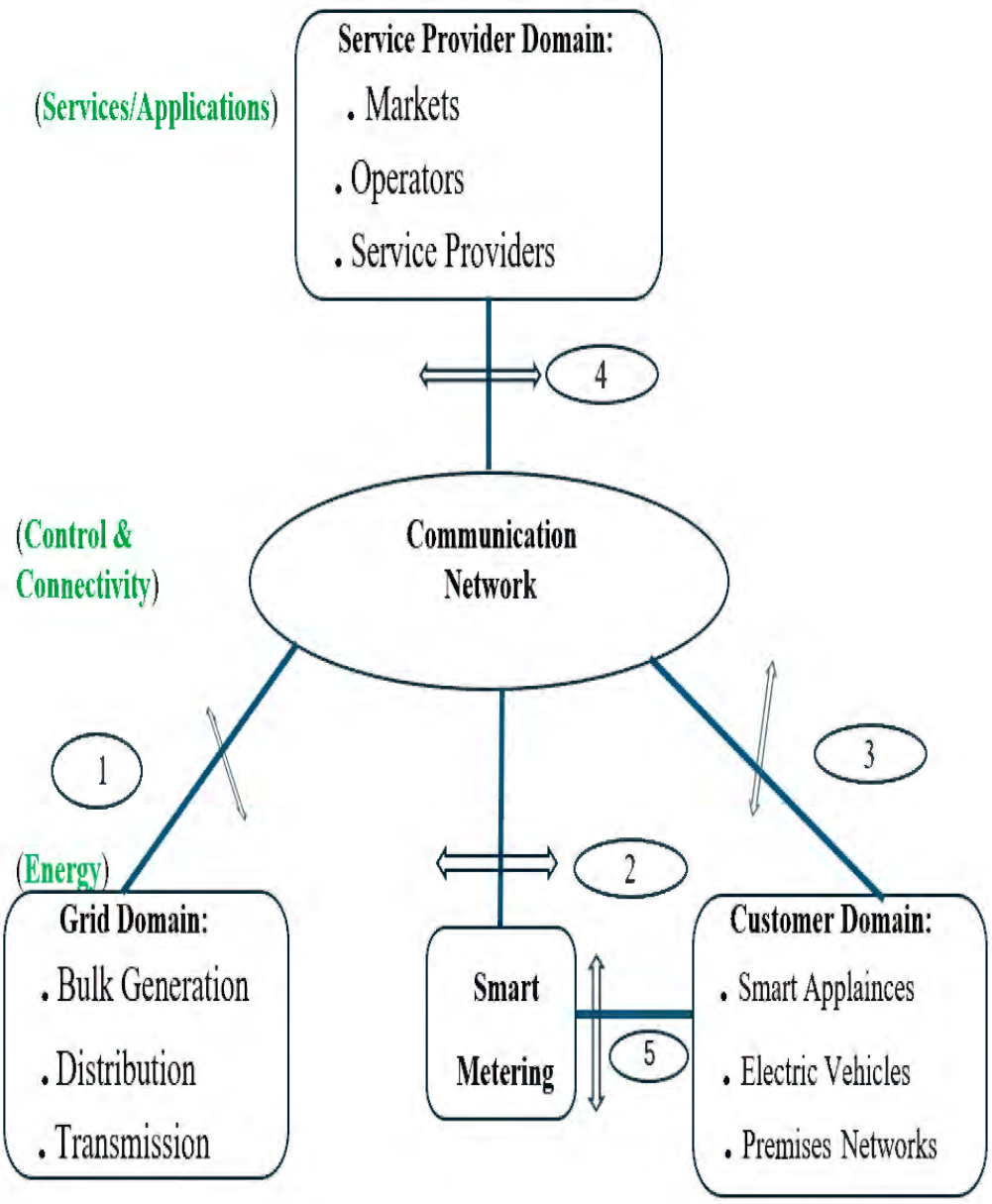


Fig. 5. Components of the Generic Smart Grid Network Architecture [17].

2.2 Technologies for Smart Grid Communication

As explained below, a number of technologies can be used with the smart grid.

The ZigBee

An IEEE 802.15.4 standard terms ZigBee. It is intended for use with digital radios that are tiny and low power. Compared to other wireless personal area networks (WPANs), the technology used in the Zigbee specification was less expensive and simpler. Wireless light switches, medical device data collection, industrial equipment that needs short-range traffic management systems, home automation, and other low-power, low-bandwidth applications are all examples of applications made for small-scale projects that need a wireless connection.

ZigBee's stated rate of up to 250 kb/s, as per its specification, is most suitable for periodic or intermittent data from an input device or sensor. Smart meters can be integrated with other devices and the ZigBee network with the "ZigBee Smart Energy" application [15]. Through this application, smart meters may monitor and operate the integrated devices and receive information from them. Additionally, it enables improved energy consumption and real-time dynamic pricing, which improves the ability of users to view their energy usage in real-time.

Among the benefits of using ZigBee in Smart Grid applications are its affordability, portability, and comparatively low bandwidth. ZigBee's small battery, which shortens its lifespan, little memory, slow processing speed, and limited data rate are drawbacks.

WLAN

A group of local area networks (LANs) or other networks that may communicate with each other is called a wide-area network (WAN). In essence, it is a network of networks, and the largest WAN in the world is the Internet. It uses spread spectrum or orthogonal frequency division multiplexing (OFDM) to connect two or more devices [16]. To enable communication between computers and users in one area and other devices in

other locations, WANs link LANs and other networks. A lot of WANs are private and designed for a single company.

In the meanwhile, built-in ISPs connect a company's local area network (LAN) to the Internet. WLANs operate in the 2.4 GHz to 3.5 GHz frequency range
as normal, and because they are widely used worldwide, they are simple to include into the Smart Grid. IEEE 802.11 standards serve as their foundation. WLAN's low cost, global deployment, and plug-and-play device capabilities are among its benefits. The drawback of WLAN is the increased likelihood of interference from other devices using the same frequencies for communication.

Cellular Systems

Users can make calls, send texts, and access the Internet over cellular networks, also known as mobile networks. Despite being the most widely utilized communication network, they are susceptible to a number of problems. High data rate connections up to 100 Mbps are made possible by cellular networks, which improves the capacity of various Smart Grid components and devices to communicate with one another. WiMAX, GSM, 2G, 3G, GPRS, and 4G are a few of the current cellular communication technologies [17]–[22].

The WiMAX chips are incorporated by smart meters that are deployed through the Smart Grid. The advantages of cellular networks include high data transmission speeds, infrastructure with a wide deployment area, and security techniques that have already been used in cellular communication. The drawback of cellular networks is that they must be shared with other users and must be entirely devoted to Smart Grid communications.

PLC or Power Line Communication PLC

Data transmission over existing electrical power lines is made possible by Power Line Communication (PLC). In essence, it enables network connectivity without the need for new cable by using the same wires that transport electricity to convey communication messages. This is frequently utilized in Smart Grid applications such as building automation systems, smart meters, and home energy management systems. Electrical power lines can be used to transmit data between devices thanks to power line communication. Modified carrier signals are added to the wire system in order for powerline communications systems to function. Powerline uses various radio bands for communication. Power wire circuits can only carry a limited number of higher frequencies because the original design of the power distribution system was to transport AC power at normal frequencies of 50 or 60 Hz. Each sort of powerline communication is said to be limited by the propagation problem. In Smart Grid applications, PLCs are utilized to connect smart meters to a Local Data Concentrator (LDC) via Neighborhood Area Network communication.

The benefit of PLC is that the established infrastructure lowers installation costs. The restricted communication frequency and higher-order harmonics in the power lines that disrupt communication signals are the drawbacks of PLC. Table 1 provides a broad summary.

TABLE I
COMMUNICATION TECHNIQUES FOR THE SMART GRID [18]

Communication Technologies			
Flow between smart meters and sensors or other electrical appliances (inside HAN)		Flow between data centers and smart meters (from HAN to WAN via NAN)	
Wired	**Wireless**	**Wired**	**Wireless**
Power Line Communication (PLC)	ZigBee Smart Energy Profile/ZigBee (SEP)	Power Line Communication	Cellular Technologies (WIMAX, CDMA, 2G, 2.5G, 3G, UMTS LTE, WCDMA)
	6LowPAN	Digital Subscriber Lines (xDSL)	Mesh Networks (802.11s)
	Z-wave	Optical Fiber	

2.3 Communication Infrastructure for Smart Grids

To guarantee the seamless integration of various communication protocols, infrastructures, and smart meters, the Smart Grid communication standard is essential to its deployment. This is accomplished by creating standards that are widely recognized by all organizations and stakeholders engaged in the creation of Smart Grids. The European Committee for Standardization, the International Electrotechnical Commission (IEC), the American National Standards Institute (ANSI), the Institute of Electrical and Electronics Engineers (IEEE), and other authorized organizations are currently engaged in the process

of standardizing Smart Grids. The common standards for Smart Grid communication are listed below.

PLC G3 or G3-PLC

Fast, dependable, and long-range communication via existing power lines is made possible by PLC G3, also known as G3-PLC, a power line communication (PLC) technology. This modern technology makes use of specific frequency bands like FCC and ARIB, as well as CENELEC-A, -B, and -C. G3-PLC offers medium- and low-voltage power grids cost-effective long-range communications. The frequency bands supported by this worldwide ITU standard span from 10 kHz to 490 kHz.

IEEE 2030

Alternative methods and best practices for attaining Smart Grid interoperability are offered by the IEEE 2030 standard. The framework for creating an IEEE international and national body of standards based on cross-cutting technical disciplines in power applications and information control and exchange through communications is provided by this first IEEE standard on Smart Grid interoperability. IEEE 2030's main goal is to provide two-way power flow with control and communication in order to support a more dependable and adaptable electric power system. It offers a knowledge base covering terminology, functional performance and evaluation standards, and characteristics.

IEEE 1901

The foundation for in-home powerline networks and broadband over power lines (BPL) was laid by the IEEE 1901 standard. Broadband over power lines (BPL) is a standard for high-speed communication devices that use electric power lines. This standard specifies physical layer (PHY) and medium access control (MAC) requirements for high speed

(>100 Mb/s at the physical layer). For applications involving universal communications in Smart Grid s, the standard has received respectable recognition.

IEC 62351

A worldwide cybersecurity standard for control and communication systems in Smart Grid s is IEC 62351. While adapting the recommendations to the reality of the industrial world, it seeks to assist grid operators in safeguarding themselves against risks threatening this sector. In order to implement security technologies in the operational environment, it outlines the requirements for cyber security. Role-based access control (RBAC), security event recording, cryptographic key management, and system management objects and networks are all included.

IEC 62056

The IEC 62056 standard, sometimes referred to as COSEM/DLMS (Device Language Message Specification/Companion Specification for Energy Metering), is an international requirement for communication between utility companies and smart meters. Reading and controlling data about gas, electricity, and water usage is its main function. In a "Smart Grid " setting, it outlines a standardized method for facilitating effective remote meter reading, data sharing between meters and data gathering devices, and management.

IEC 60870-5

Telecontrol, which is power system automation applications, supervisory control, and data acquisition, uses the IEC 60870-5 set of standards. Additional Smart Grid communication standards, including IEC 60870-5-101, IEC 60870-5-103, IEC 60870-5-104, and others for electric power systems, were implemented by working group 03 as well.

A typical computer network with five levels [18]—Physical Layer (1), Link Layer (2), Network Layer (3), Transport Layer (4), and Application Layer (7)—is used for Smart Grid communication. This network is based on the ISO/OSI architecture.

TABLE II
SMART GRID COMMUNICATION NETWORK LAYERS, STANDARDS, AND PROTOCOLS

7	Application Layer	IEC 60870-5-104, IEC 60870-5-5, IEC 60870-5-4
4	Transport Layer	TCP (RFC 793)
3	Network Layer	IP (RFC 791)
2	Link Layer	PPP (RFC 1661 & RFC 1662) | Transmission of IP datagrams over Ethernet network (RFC 894)
1	Physical Layer	X.21 | Ethernet (IEEE 802.3)

2.4 Applications of the Smart Grid

The evolution of Smart Grid infrastructures/technologies has altered daily routines and way of life. Here are just a few of the numerous uses for the Smart Grid that exist today.

DA or Distribution Automation

Distribution automation is one use case for the Smart Grid. This is the capacity of the Smart Grid to automate all distribution system operations through the use of data gathered from feeders, substation systems, and meters placed at consumer sites. [19] [20]. It can also be applied to fault isolation, restoration, and detection.

AMI or Advanced Metering Infrastructure

AMI is a communication network, smart meter system, and data management system that enables real-time communication between utilities and customers in order to gather, examine, and store energy usage data. Additionally, it is among the most important Smart Grid applications. The AMI meters are digital meters that gather energy consumption data automatically and send it wirelessly and problem-free to a communication network. The AMI system lowers operational costs, remotely controls meter functionality, detects system defects, and tracks energy consumption in real time.

DG or Distributed Generation

Another essential component of Smart Grid applications is DG. In contrast to centralized generating sources from power plants connected to the utility distribution system, it refers to electricity produced close to the point of use. DG has several advantages, including increased energy efficiency, decreased carbon pollution, and transmission losses.

Automation for Power Systems

The Smart Grid 's ability to identify and quickly address grid faults or interruptions is another use case. This function automatically finds, examines, and fixes associated grid interferences, disturbances, blackouts, and outages.

Distributed Storage

Another crucial component of Smart Grid applications is DS. It describes how well an electrical energy equipment that is connected to the grid can store and release energy at the right times.

EVs, or Electric Vehicles

EVs can incorporate electric car charging into the grid as part of Smart Grid applications, which lowers greenhouse gas emissions and increases productivity and operational efficiency. In practice, EVs are regarded as distributed storage systems as, when they are connected to the grid, the batteries are charged using the grid's power and can then be released back into the grid.

HANs, or Home Area Networks

Another advantage of Smart Grid s is the capability to simplify the management of home energy consumption. Air conditioners, heaters, electronic devices, radios, televisions, lighting, solar panels, and more are examples of household gadgets. These and many other gadgets may communicate with one other without any problems thanks to HAN.

Micro-grids

Microgrids offer still another significant advantage in their use with a Smart Grid. It is a collection of linked loads and dispersed energy resources that function as a single controllable unit. Microgrids that use a variety of power sources, such as solar, diesel, wind, and gas, can also operate in island mode or as grid-connected systems. As illustrated in Fig. 6, it is only a group of individual customers on a campus of buildings or a community that are connected to one another and at least one energy producing source. The term "power grid" refers to this grouping of customers and generation sources. Both the microgrid's energy sources and the utility grid provide energy to microgrid users.

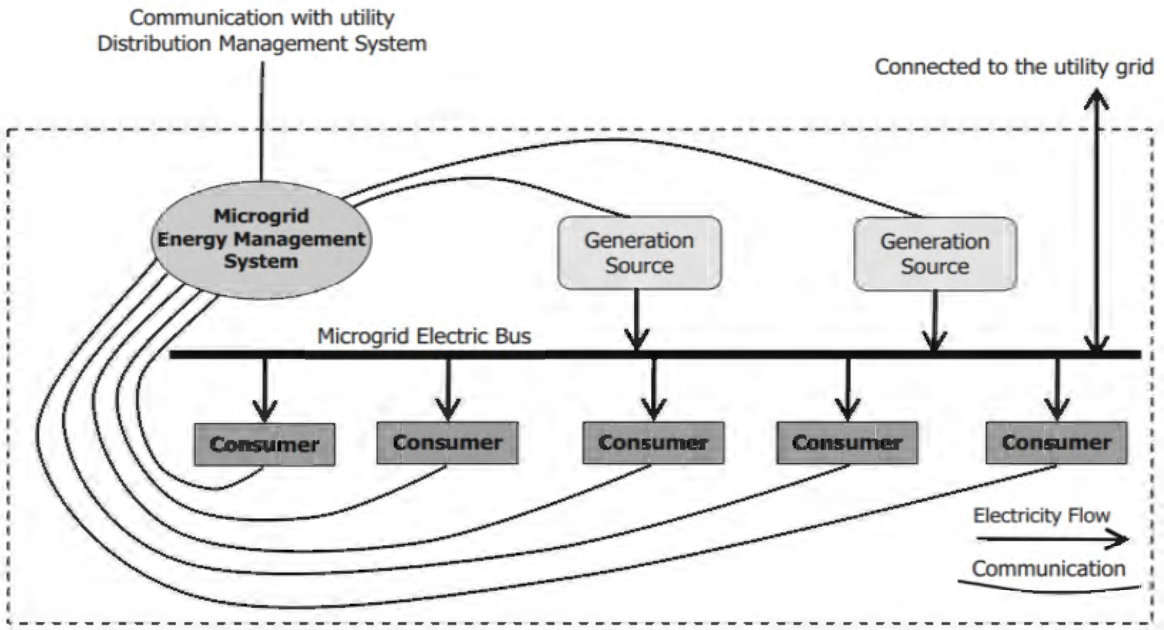


Fig. 6. Diagrams for a microgrid.

The Markets for Retail Energy

Wholesale energy markets (WEMs) are traditional energy markets that are attended by the owners of utilities and bulk energy suppliers. In the US, entities like Independent System Operators (ISOs) and Regional Transmission Operators (RTOs) represent the utility business in indirect participation. A utility does have agreements with a number of bulk energy providers. A significant portion of their demand,50% or more, is supplied by these contracts, with the remaining demand satisfied by purchasing power in the real-time spot markets [21] .

Response to Demand

It can require time and effort to meet consumer power demands utilizing the generation resources that are available since supply and demand are inconsistent. Demand response (DR) is the process of controlling rising demand by either lowering it or boosting the amount of electricity delivered to the grid.

Synchrophasors and Wide Area Situational Awareness

The electric grid has shown great promise in the majority of the developed world, and people have always prepared for invisible outages that have no discernible impact on the grid's services. Meanwhile, a number of unforeseen power blackouts and outages that could last for several hours and impact numerous vital locations have been caused by the rising demand for electricity over the years. The capacity to show and track the power system's components and their performance throughout the interconnection of utility grids is known as wide area situational awareness and control, or WASA&C. Real-time monitoring in this instance improves the precision of regulating and fixing issues as soon as they are identified.

FACTS or Flexible AC Transmission System

In this instance, FACTS refers to the potential for dynamically adjusting the reactance of the capacitor under transient situations in order to lower the magnitude of the power and voltage transients [21]. FACTS offers reactive compensatory power as well as other features required to enhance transmission system and power flow control.

DLR or Dynamic Line Rating

Transmission lines are often made to have a standard rating even under the worst circumstances. Transmission lines can transport currents higher than their rating when the weather is better than it is at its worst. A well-known technology called DLR determines the maximum current a transmission line can carry at any given moment by taking into account the line's characteristics as well as the present weather. Nearly 95% of the time, it efficiently adds 10–15% of transmission capacity, and 85% of the time, it totally adds 20–25% of additional transmission capacity [22].

2.5 Overview of the Conventional Electric Power Grid

In a typical electric power grid, electricity is transmitted from power producing facilities to end customers in a unidirectional fashion. The government deregulated this method because of certain technical, economic, and environmental problems. A more dependable, scalable, managed, secure, and economical system is desperately needed to address the long-term evolution of the industry [23] [24]. It is anticipated that the Smart Grid, which offers two-way connectivity, would transform the transmission, distribution, and generation of power[2]. The four primary areas of the electric grid are distribution, transmission, generating, and third parties are markets and system regulators.

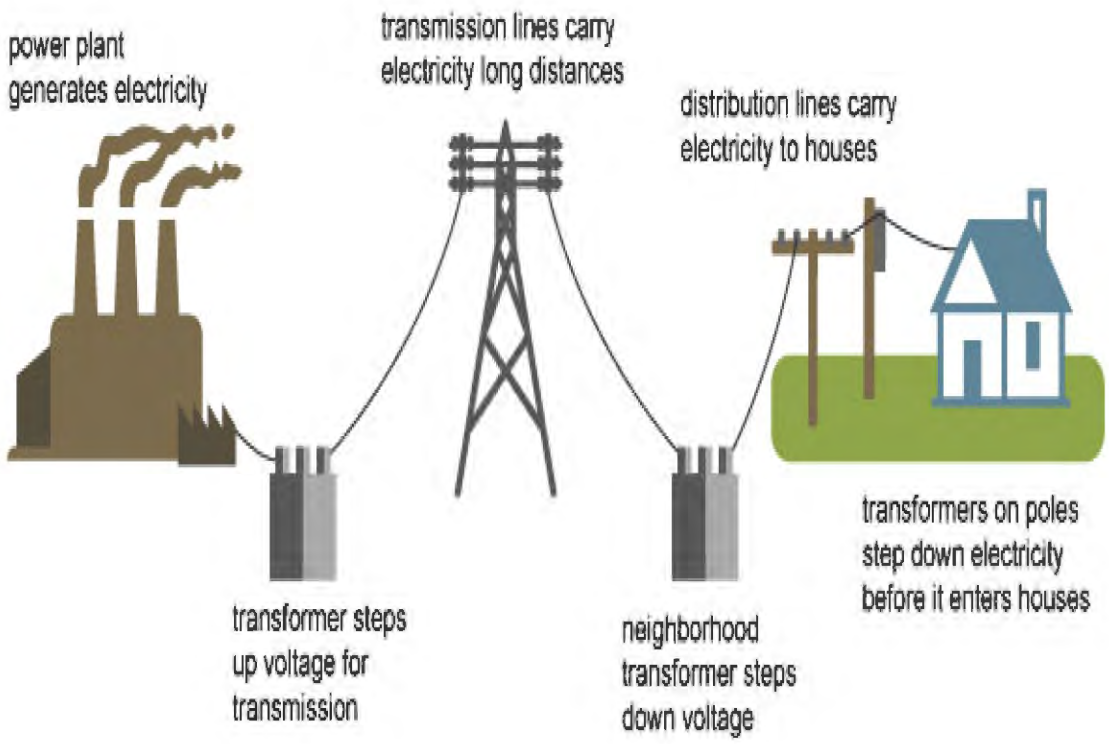


Fig. 7. The main technologies of the SG system are described.

The Electric Power Grid system's construction is depicted in Fig. 7 above. Every cyber system must meet the three essential security hygiene requirements of confidentiality, integrity, and availability [25], [26].

Generally speaking, a Smart Grid combines a conventional distribution network with a two-way communication network to sense, monitor, and distribute energy consumption data. Fig. 8 provides an illustration of a Smart Grid's communication architecture. Many power-generating and power-consuming units connected by a network make up a typical Smart Grid. The grid receives energy from the generators and uses it for their own purposes. The Smart Grid is characterized by its decentralized, dynamic, and ad hoc energy distribution [27].

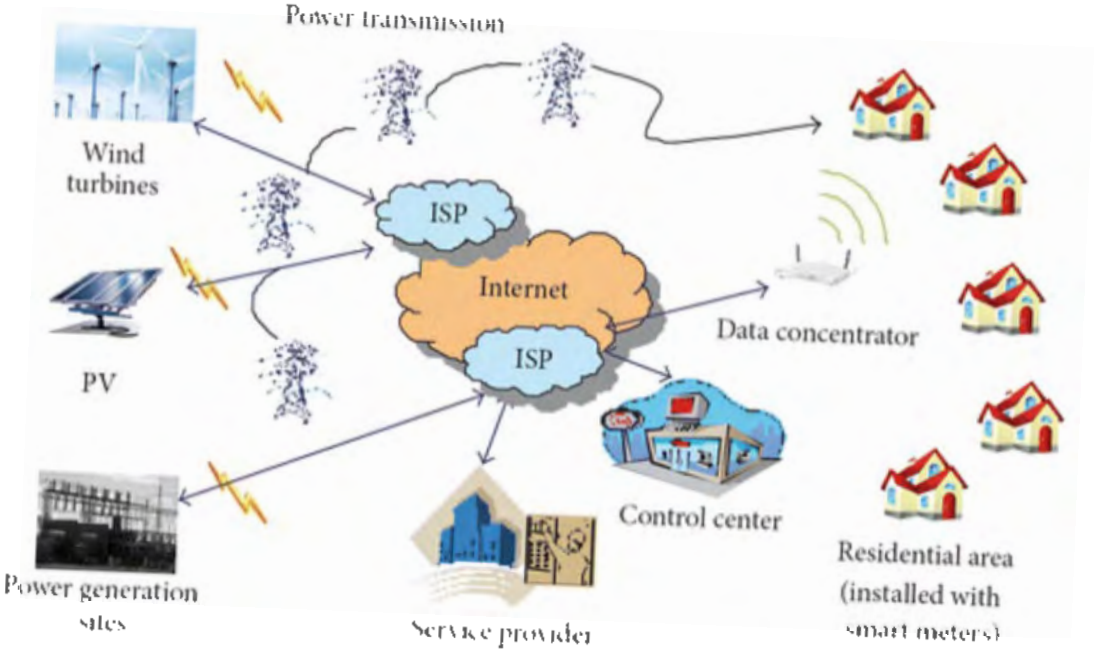


Fig. 8. Smart Grid communication architecture [27].

Generation

The creation of electricity is the major objective of the generation domain. A spinning turbine is the main source of electricity, and control algorithms are centered on controlling the generator's voltage, frequency, and power output [28], [29]. Additionally, in order to maintain proper and secure synchronization, generation must connect with authorities from outside parties. This is accomplished via the wide-area Automatic Generation Control (AGC), which modifies and tracks a generator's frequency in response to variations in loads. To avoid any physical failures, generating systems also need to employ a variety of protection mechanisms.

Transmission

Moving high-voltage power from large generators to the distribution domain is the principal responsibility of the transmission domain. Substations serve as a location for the deployment of multiple control mechanisms and primarily support the requirement to convert power between different voltages on nearby lines [28], [29]. Consistent transmission line monitoring should be required to make sure that the load on the lines stays within their physical bounds. State estimation control methods are used for this. In order to determine the flow on the transmission system, this wide-area monitoring system gathers data from power lines and sends it back to the control center. Protection measures should be in place since the lines are physically exposed and are primarily affected by faults that alter power flow. Both broad and local protection plans are put into action.

Distribution

Distribution focuses on using lower voltage lines to carry electricity from the transmission lines to the end user. Distribution systems have historically been less

automated than the transmission and generation sectors, according to observations [28] [29]. Breakers are used to trip relays on distribution feeders, and load shedding has been a key distribution control function. Protection systems are typically utilized in distribution systems to shield equipment from malfunctions, much like in the transmission and generation sectors.

Operators of Market Systems

The supervision and management of the numerous utilities is one of many additional responsibilities that are essential to the day-to-day functioning of the grid [30]. To keep the load balanced, independent system operators (ISOs) are in charge of coordinating transmission and generation across several utilities. Additionally, ISO offers marketplaces that help customers and energy providers manage the supply and demand for power.

2.6 Traditional Electric Grid vs. Smart Grid

Limited one-way or unidirectional interactivity is used by the current grid. Power moves efficiently and with little information exchange from the power plant to the end user. Data collection from a small number of sensors at the primary transmission and distribution points, as well as a small number of control signals for fault detection and transmission, are the primary functions of classic grid communication systems. Data collection is done using SCADA systems. The conventional grid required improvements to keep up with modern life, while being an engineering marvel. Similar to the Smart Grid , the traditional electric grid used electricity flowing via its lines to power our homes, but it stopped there [31], [32]. People were simply getting energy, and the utility provider was not receiving any data on whether or not people were utilizing it. It was challenging for

consumers to cut back on their energy use because they also required feedback on how they were using their electricity. Furthermore, it was hard to predict whether there would be any blackouts.

Utility providers can communicate with homes and businesses in both directions thanks to the Smart Grid. Compared to the conventional grid, it features a reassuringly greater number of actuators and sensors. To manage such massive data flows and offer secure real-time communications, the Smart Grid includes modern, dependable, and strong communication infrastructure. Wide bandwidth is provided by the Smart Grid communication infrastructure to guarantee a significant information flow throughput.

Utility companies can now receive reports from homes and businesses about problems that can be signs of upcoming power outages. Power utilities and consumers may communicate with each other in both directions thanks to the Smart Grid 's two-way communication method. Conventional and Smart Grid s are contrasted in Table 3 and Fig. 9.

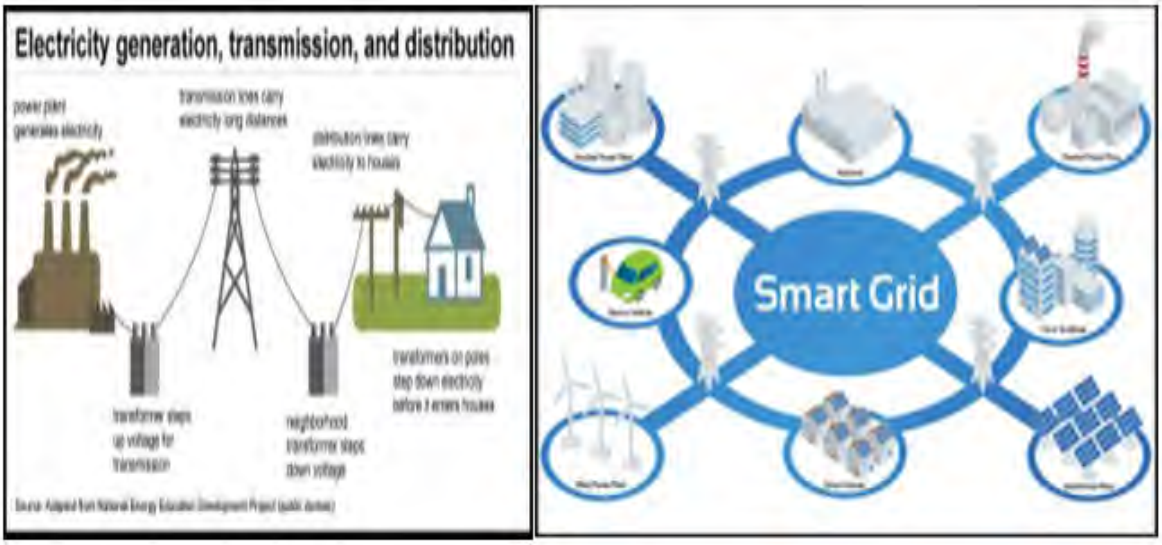


Fig. 9. The Reasons for Smart Grid [31], [32].

TABLE III
THE REASONS FOR SMART GRID [31], [32]

Conventional Grid	Smart Grid
Electromechanical	Digital
One-way communication	Two-way communication
Centralized generation	Distributed generation
Few Sensors	Sensors throughout
Manual restoration	Self-healing
Manual monitoring	Self-monitoring
Failures and blackouts	Adaptive and islanding
Limited control	Pervasive control
Few customer choices	Many customer choices
Customer calls when the power goes out	Utility knows when power is out and restores it automatically
Utility meets peak demand	Utility suppresses peak demand, thus lowering cost
Difficult to manage high wind and solar penetration	Utility can manage distributed energy resources safety
10%+ power loss in T&D	Utility reduces power loss by 2+%, and reduce emissions and electricity bills of customers

This expanding communications, automation, computer, and control networks make the grid more dependable, secure, efficient, and "greener." The Smart Grid also

makes it possible to integrate renewable technologies into the country's electrical infrastructure [32]. Local distribution repair teams can address power outages more quickly thanks to the Smart Grid 's ability to remotely predict and respond to issues.

2.7 Advantages of Smart Grid Technology

The modern, new electrical infrastructure has changed how people live. Now that utility companies can locate the cause of a power outage and fix it, people may relax. The Smart Grid alters the game in the following ways [29], [30], [31].

Enhances communication: data about electricity usage is transmitted to the utility company and returned to customers, allowing them to know how much energy they consume, thanks to the two-way connection between Smart Grid s and meters. Energy firms can more quickly address problems that lead to blackouts and power outages by using Smart Grid communication.

Minimizes power outages: utility companies may anticipate future power outages before they occur because of the Smart Grid 's two-way connectivity. In this manner, outages are promptly addressed by taking preventative action right away.

Prevents waste: the Smart Grid provides continuous input on how the electricity is used, allowing the ability to spot areas of overuse and make required reductions. Additionally, by using smart meters, utility firms may better eliminate waste, resulting in a more efficient delivery of electricity to all neighborhoods.

One type of gas and electricity metering technology that can electronically communicate real energy consumption to the utility provider is called a smart meter. This implies that households will not have to rely on anticipated energy bills or let meter readers into their houses in order to manually read the meters [31], [32].

Customers can also get data about their energy consumption in almost real-time through the smart meter, which is depicted in Fig. 10. This enables them to better understand, assess, and control their energy consumption, which lowers energy waste and, consequently, emissions from power plants.

Fig. 10. A smart meter example [32].

Additionally, utilities can gain a better understanding of residential electricity use patterns by using data from smart meters.

Removes estimated bills: in order to prevent customers from paying for more electricity than they really use, the Smart Grid measures bills in real-time and removes predicted billing.

Enables new pricing plans: Smart Grid s and meters brought with them new pricing schemes that let customers reduce their electricity use during periods of peak demand and save money or get bill credits [32].

Renewable energy adoption: the Smart Grid 's cutting-edge technology optimizes output and efficiency and works with renewable energy sources like solar and wind.

Key Takeaway: utility companies can help us interact with homes more effectively, reduce power outages, stop waste, receive accurate bill projections, get new pricing plans, and adjust to new technology by implementing advanced Smart Grid communication.

Improves Energy Conservation: the old electrical grid made it simpler to keep track of daily energy usage by facilitating communication about how customers use electricity in our homes. Since consumers did not know how much energy they were using until a large bill showed up in their mailbox, it was simple to inadvertently waste electricity. By using fossil fuels, people unintentionally emit harmful greenhouse gases into the atmosphere when all this additional energy burns away in the power plants. Communities that prioritize environmental justice were disproportionately affected by the excessive pollution and negative health effects caused by wasted energy.

Positive Environmental influence: by lowering energy consumption, the Smart Grid assists users in lessening their influence on the environment. By utilizing energy only when necessary and eliminating waste, smart meters and thermostat senable homes and buildings become more energy efficient. The smart Grid is prepared to accommodate renewable energy sources like solar and wind because of its updated technology [33].

Offers Smart Electricity Options: utility companies can create innovative pricing schemes to incentivize consumers to reduce their electricity consumption thanks to the modern Smart Grid. In addition to lowering greenhouse gas emissions and saving consumers money, this assists utilities in lowering energy demand to avoid power disruptions!

It Improves Quality of Life: by communicating energy use to consumers and utilities through contemporary technology, the Smart Grid goes beyond the conventional

electric grid [34]. Consumers can lower energy waste, power outages, and greenhouse gas emissions by managing the energy use with the help of the Smart Grid. Customers who take part in pricing initiatives that give them more control over their energy use can also save money. Simple lifestyle changes can improve the general quality of life on the planet. Because consumers were not aware of how they were using their energy, a lot of it was wasted, which resulted in pollution, extra greenhouse gas emissions, and negative health effects.

2.8 Mathematical Algorithm in Smart Grid Communication Network Attack

This approach, which is predicated on scenario prediction, describes the Cyber-Attack Scenario in the industry. People presume that coordinated attacks against industries take place in order to inflict the greatest amount of harm. The time spent looking for the emergency situation's correspondence to one of the previously simulated situations determines how long it takes to detect an attack.

The power system operating mode is linearized and represented as a collection of passive (complex resistances) and active (current sources in the nodes) elements in order to compute cyber-attack scenarios [35], [36]. The load and generation nodes are thus depicted as ideal current sources, where the respective nodes are characterized by the signs of the real and imaginary components. Concentrated complex resistances that ignore mutual induction are used to depict the windings of power transformers and power transmission lines.

An incident matrix is a mathematical representation of the electrical network, which is described as a directional graph. The voltage vectors at the nodes and currents in the

branches are then found by applying the Gauss method to solve linear equation systems using the incidence matrix of the electric network graph.

$$\vec{U} = (\mathbf{U_1}, \mathbf{U_{2,,,,,,...}}\mathbf{U_n})^T \text{----------(1)}$$

$$\vec{I} = (\mathbf{I_1}, \mathbf{I_{2,,,,,,...}}\mathbf{I_n})^T \text{----------(2)}$$

In the electric power grid model, "n" stands for the number of nodes. The node parameters of the electrical networks district model are described by expressions (1) and (2). The reference of the criterion for the existence of the mode is the voltage. The branch currents serve as the second reference value. It is assumed that the transformer ratios for the branches are accurate [37]. A column-matrix is represented by the currents in the branches.

$$\vec{J} = (\mathbf{J_1}, \mathbf{J_{2,,,,,,...}}\mathbf{J_m})^T \text{----------(3)}$$

In the electric power grid model, "m" stands for the number of branches.

From a mathematical perspective, the challenge of figuring out the state mode of the electric network model is nonlinear, its solution can be found, for instance, by iterative techniques. The steady-state mode of a particular electrical grid model is iteratively recalculated to produce cyber-attack scenarios based on the state indexes of the elements [38]. Each scenario is composed of groups that correspond to switches [39]. Scenario groups with a single shutdown are utilized for the model in question. According to the maximum allowable current loads, the state indexes are computed in order to maintain load nodes (static stability) and keep the branches operational. For the branches, state indexes are calculated by the expression:

$$\mathbf{IS_i} = \frac{\mathbf{I_{fact,\,i}}}{\mathbf{I_{max,\,i}}} \text{----------(4)}$$

Where $\mathbf{I_{fact,\,i}}$ represent the modulus of current flowing in the i-branch; $\mathbf{I_{max,\,i}}$ represent the limit value of the current for a given branch. The following provisions take into account the current limit value *I*max, *i*: - The limiting current in the windings of power transformers and autotransformers is assumed to be equal to the current by their maximum allowable load; - For power lines with any number of circuits, the limiting current is assumed to be equal to the line's valid durable current.

$$\mathbf{ISi_j} = \frac{\mathbf{K_j.S_j}}{\sqrt{3}\,\mathbf{.U_j}} \quad \text{----------(5)}$$

Where $\mathbf{S_j}$ is the rated capacity of the power transformer (autotransformer); $\mathbf{K_j}$ is the coefficient of transformer (autotransformers) overload capability; $\mathbf{U_j}$ is the rated winding voltage. The following expression is used to determine the state indexes for the nodes:

$$\mathbf{ISu_j} = \mathbf{K_{s.rel,\,j}} = \frac{\mathbf{U_{fact,j} - U_{max,j}}}{\mathbf{U_{fact,\,j}}} \quad \text{----------(6)}$$

Where $\mathbf{U_{fact,j}}$ is the actual voltage in the j-load node; *U* max, *j* is the critical voltage of the load node; $\mathbf{K_{s.rel,\,j}}$ is the steady-state stability factor of the load [38]. The critical voltage *U* max, *j* of load nodes is determined by maintaining a constant workload [38]. The motor character of the load and the prerequisites for its steady functioning in the event of a voltage shift at the node are assumed in the computations. A sizable portion of the motor load is disconnected when the actual voltage on the load drops by more than 30%. By altering the node's overall power usage by 25% from the specified figure, this scenario is created and represented. Protective relaying devices are used to disconnect the node from the power system when the voltage in the node drops by more than 40%. This results in the ultimate load drop. One requirement for leaving the interactive simulations of cyberattack scenarios is a breakdown in an electrical network. The expression determines the electricity

shortfall that consumers in the electric grid experience, which is represented by this parameter.

$$\mathbf{S_{ful}} = \sum_{m=1}^{N} n.\mathbf{S_n} + \Delta S \quad \text{----------(7)}$$

In this case, *Sful* is the total value of the load nodes' capacity of the electric network's total power; n is the number of load nodes in question; and ΔS is the amount of additional capacity reserve that the power system can introduce in the event of a cyberattack. Deactivating any schema branches is the first set of situations. The groups in the second reflect branch outages and are arranged according to the network elements' current status indexes (equation 6).

To generate random fake currents in the selected branch (I_{ph}), the nominal branch voltage and the range of currents were determined from which (I_{ph}) was then selected at randomly. The average current value in the i-element of the electrical network was created according to the expression [40].

$$I_{mid.i} = \frac{S_{mid.i}}{\sqrt{3}.U_{mid.i}} \quad \text{----------(8)}$$

The middle current value ($I_{mid.i}$) in i-branch, the middle power value ($S_{mid.i}$) in the i-element of the power system model, and the middle voltage value ($U_{mid.i}$) in the i-element of the power system model are represented in (8). Both power lines and transformers (autotransformers) had their voltage values set to nominal [41]. Only power cables were used to mimic emergency modes in some tests. It was believed that there was little chance of a cyberattack on an electrical substation's main machinery. The range of random sampling of fake fault currents was established using the following expressions:

$$I_{ph.min.i}=K_{min.i}*I_{mid.i} \quad \text{----------(9)}$$

$I_{ph.max.i}$=$K_{max.i}$*$I_{mid.i}$ ----------(10)

Where $I_{ph.min.i}$ is the minimum value of the falsified current for the i-element of the electric network; $I_{ph.max.i}$ is the maximum value of the falsified current for the i-element of the electric network; $K_{min.i}$ is the value coefficient value determining the lower bound range, $K_{max.i}$ is the coefficient value determining the upper limit range. The value of the false voltage of the i-branch was calculated by a random sample from $I_{ph.min.i}$ to $I_{ph.max.i}$ (expression 9). The maximum and minimum values of short-circuit currents on this line, as determined by the analysis of emergency situations characteristics, were determined to be 2 and 57 for the chosen branch $K_{min.i}$ and $K_{max.i}$. Ohm's law was used to determine fictitious voltages in a straightforward method. The voltages of the branch's starting node (node "F") and ending node (node "S") are known parameters in this instance.

The equation below was used to determine the voltages' realistic values at these nodes.

$U_{f.i} = rand(K_U{*}U_{mid.i}, U_{mid.i})$ ----------(11)

$U_{s.i} = U_{f.i} - I_{ph.i} * Z_i$ ----------(12)

Where $U_{f.i}$ the value of the constructed voltage of the i-branch's beginning; $rand(K_U{*}U_{mid.i}, U_{mid.i})$ · is a function of random sampling from a given range; K_U ; is the coefficient of criticality of changes in the node's voltage (selected at random from the range of 0.7 to 0.8).

A generalized control-flow chart for detecting cyberattacks is shown in Fig. 11. The technique enables efficient cyberattack detection and is based on comparing real and model

data. As an automated control subsystem of dispatch control and technical management, specialized software for cyberattack detection have to be put into place [42] [43].

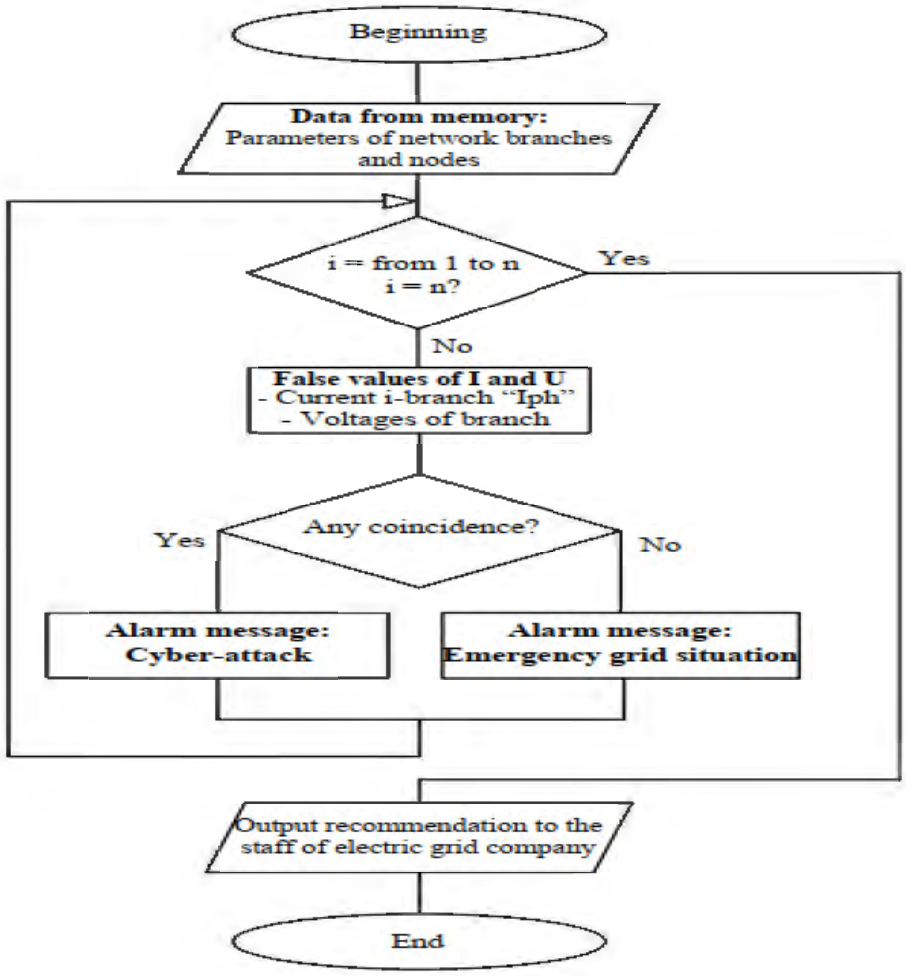


Fig. 11. Generalized block diagram of the algorithm used to identify cyberattacks.

2.9 Check for Smart Grid Detectors

Detector. to explicitly identify logical attacks, the detector looks at the AR (Attack Rate) value. It determines the total size rate (TSR) and total count rate (TCR).

$$TCR(j) = \frac{\sum_{i=1}^{n} Count(i)}{current\_count} \quad \text{----------(13)}$$

$$TSR(j) = \frac{\sum_{i=1}^{n} Size(i)}{bandwidth} \quad \text{----------(14)}$$

where n is the Heap table j's record count. The "Count" and "Size" of the i-th record are denoted by Count(i) and Size(i), respectively. The ratio of packets transmitted to destination j in this "two-second" is indicated by TCR(j). The ratio of bandwidth used by the flow transmitted to j is displayed by TSR(j). The bandwidth of various subnets may vary. A DoS or DDoS assault is likely to occur if TCR(j) or TSR(j) surpass their respective thresholds, thd1 and thd2, respectively. Our experience indicates that thd1=40% and thd2=50%. With the use of equations (12) and (13), we can detect invaders.

$$CR(i) = \frac{\text{Count(i)}}{current\_count} \quad \text{----------(15)}$$

$$SR(i) = \frac{\text{Size(i)}}{bandwidth} \quad \text{----------(16)}$$

This IP address is suspected of being a hacker if either CR(i) or SR(i) is above its threshold, Thd3 and Thd4, respectively. Our experience has shown that Thd3 = 30% and Thd4 = 40% flow levels.

3. CYBER SECURITY THREATS IN SG COMMUNICATION NETWORK

A complex system, the Smart Grid communication network system is made up of several key subsystems that can function as transmitters and receivers. These subsystems may be software-based control systems or wired or wireless communication channels. The intricacy of the Smart Grid has created a number of issues that must be resolved in order to create a solid and dependable communication system. However, the attacker must have understood how to control the system by manipulating the cyber parts for the attack to have a disruptive effect. This relationship is seen in Fig. 12.

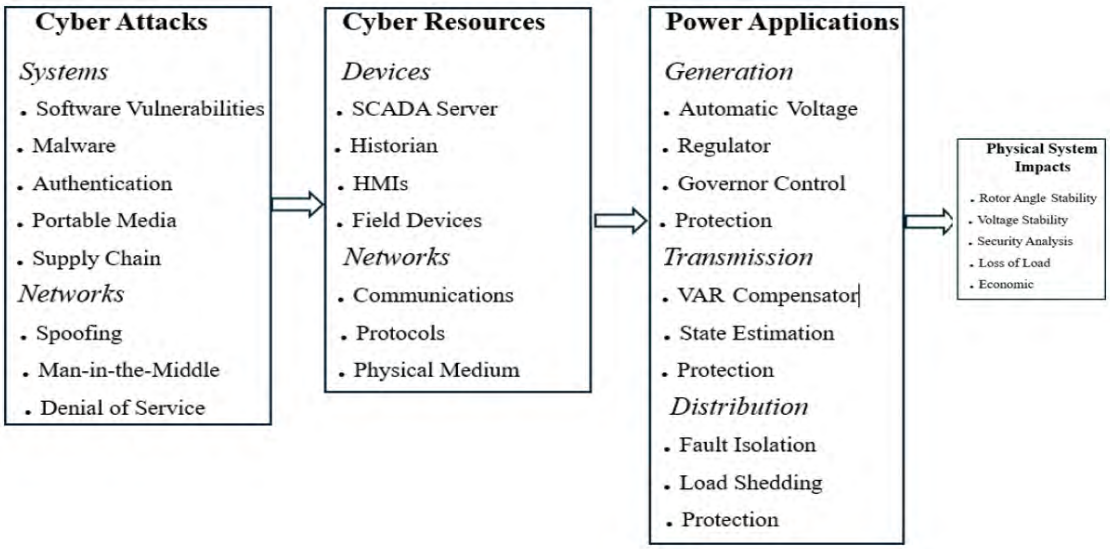


Fig. 12. How Smart Grid is being attacked [44].

An attacker could interfere with the grid's cyber resources in a number of ways. An attacker can have some degree of control over the different power applications by influencing certain cyber resources. A physical system effect could then be possible for an attacker, depending on that collection of compromised power applications. Grid instability, load loss, and price influence are examples of physical effects. The set of power applications utilized to support the different intelligent grid domains, as well as the

shortcomings in supporting cyberinfrastructure, are comprehensively examined in the study in [45].

This section will describe possible attacks that could affect the communications networks of the Smart Grid, compromise sets of devices and systems and add vulnerabilities to the intelligent grid communication system.

3.1 Lack of Consumer Awareness

A thorough and robust security architecture for the SGs, incorporating all necessary elements to assess and identify the threats, requires a great deal of research and may need to be more reasonably priced for utilities [46]. Customers must thus be sufficiently informed about the risks, expenses, and benefits of SG systems due to the need for increased utility security and support for both them and society as a whole.

3.2 New Technologies

Because their security regulations and vulnerabilities have not yet been identified, hackers and adversaries may find new technologies attractive when they are introduced to the SG. As a result, it would be easy to identify a gap to exploit the vulnerabilities.

3.3 Scalability

This is the ability of a system to adjust its size in response to an increase in the magnitude of the demand. SG technologies are thought to be viable options for managing intricate electrical power systems, which are becoming more technologically and demographically advanced. It is clear that the size and complexity of the SGs are directly impacted by the expansion of the number of data and energy flows in circulation, the SG protocols, and the scale of the network structure. If not managed and suitably accommodated in the SG, this amount of data and complexity could lead to data

accumulation and control efficiency destruction. Therefore, to avoid these issues in the system, effective data flow construction solutions are needed [47].

3.4 The Drawback of Joined Communication Technologies

The drawbacks of integrating existing ICTs into SG structures include the potential for the SG system to inherit nearly all of the vulnerabilities and unresolved issues such as Denial of Service attacks, IP spoofing, and routing issues, of these technologies.

3.5 Absence of Standards and Regulations

The capacity of different systems to collaborate, exchange tools or data, and employ the complementary components to complete a task is known as interoperability of an SG. All SG components must be included in standards and regulations in order to achieve interoperability. It is also important to note that new protocols, such Distributed Network Protocol, which are constantly being published, can occasionally result in security flaws in the SGd [47].

3.6 Lack of Network Segmentation

The attack surface is increased when vital control networks cannot be separated from public networks.

3.7 Software Flaws

An attacker may be able to get around authentication and take over the system by exploiting flaws in software, such as buffer overflows, integer overflows, and SQL injection. According to recent research, innovative grid systems are severely hampered by software vulnerabilities [48] [49]. Furthermore, the requirement for high uptime makes patching control systems challenging. Systems will probably become very susceptible to software flaws as a result of this limitation.

3.8 Authentication problems

A lot of Smart Grid devices require strong authentication techniques. Devices or systems frequently lack authentication support if they are set up with weak passwords [50]. Unauthorized users may be able to alter system settings and functions due to authentication problems.

3.9 Malware

Any harmful software that an attacker can install on a target machine in order to take control of it is known as malware. Malware that prevents a system from being controlled is detrimental to the Smart Grid, even if it is commonly employed for data exfiltration in conventional ICT contexts. Stuxnet evoked the initial real-world scenario of malware deliberately infecting and carrying out evil acts within field devices [51], notwithstanding researchers' suggestion that malware may affect SCADA systems by injecting malicious control communications [52].

3.10 Compact medial

The majority of Smart Grid gadgets do not have direct connections to the unreliable Internet. This does not offer total protection, even though it makes it much harder for an attacker to access the system. A skilled hacker might be able to use portable media of some kind to introduce malware into the system. Stuxnet showed that malware may propagate via portable press to infiltrate air-gapped control systems [52].

3.11 Supply chain

Any attack method that jeopardizes a system's integrity prior to deployment may be considered a supply chain attack. Although it takes a high level of knowledge to attack

the supply chain, new findings indicate that many foreign network devices might have back-doors that allow unauthorized users to enter the system [53]. Similar to attacks on portable media, supply chain assaults do not necessitate an attacker's physical access to the system. The requirement for reliable system upgrades and patches, which have been employed in complex cyberattacks, is another aspect of supply chain problems [54].

3.12 Spoofing

Spoofing is the process by which an attacker introduces a fake message into the network to give the impression that it comes from a reliable system. Although both wired and wireless systems can do this, the latter is still more susceptible since an attacker can more readily access the physical media. By using cryptographic authentication, which forces the attacker to encrypt or sing the fake message using a private or shared key to confirm its integrity, spoofing is typically avoided. However, because many protocols were established with inadequate authentication, new grid connections raise a number of issues [55]. Applying more secure ways is also complicated by the numerous devices and high availability requirements [56].

3.13 DOS or Denial of Service

If an attacker is able to introduce huge packets into a network, they can cause congestion to the intended functions and limit the network's availability. Both wired and wireless networks are susceptible to DoS attacks, however because attackers find it more difficult to access the physical media, wireless networks are nevertheless particularly vulnerable. DoS can also happen if a malicious packet causes the server to crash or shut down while it is being processed.

3.14 Man-in-the-Middle Attack

This kind of eavesdropping involves the suspect attempting to establish several connections with potentially dangerous communication at both endpoints and sending data in between. Furthermore, the endpoints' authorized users believe they are communicating with one another directly through their connection. Without additional cyber protections like SSL, some utilities continue to send the data measured by the Phasor Measurement Unit (PMU) via the typical User Datagram Protocol (UDP). This may make it more likely that MITM attacks will be exploited. Furthermore, a Wide Area Network (WAN) is the network that connects the substation to the control center. Corrupt data, such as measurement values, control directives, and pricing signals, are susceptible to MITM attacks [57].

3.15 Misconfigurations

Communication networks are also seriously vulnerable to network misconfigurations. Device configurations like firewalls concentrate on separating a network's trustworthy and untrusted areas. As a result, if these devices are configured incorrectly, an unauthorized person could have access to vital system components. One of the main issues with the Smart Grid has been found to be improper and inadequate network segregations [58].

3.16 False data injection attack

A skillfully constructed form of integrity attack, a false data injection attack can affect the control and operation of SGs by using state estimation to get past the poor data detection systems and tricking the impacted sensors into simulating events that never happened [59]. To alter the state variables, the attacker could insert the malicious data into

a particular meter or a randomly selected vector. Since the attacker initiates predetermined changes in the state variables and has sufficient knowledge of the network topology, the latter assault is more serious. If critical meters are compromised, it becomes more difficult to detect malicious data attacks. False data injection attacks can be mitigated by certain traditional methods that safeguard particular vital sensors in the power system. Depending on the kind of meters being targeted, these assaults can take many different forms. For example, in load relocation and alteration attacks, the number of meters is changed in order to launch a cyberattack on the SG.

3.17 Vulnerabilities in Protocol Translators and Communications over External Connections

The following list includes some relevant problems with communication over external connections:

Unsecured protocols for communication

Protocols that lack methods for authentication

Protocols that are susceptible to flooding attacks with ease

Protocols like Modbus that don't have encryption built in

A protocol translator that is not secure

It may involve third-party software, open ports, or public internet connections, much like end-point device vulnerabilities.

Individual microgrids lack intrusion detection/prevention systems and firewalls.

Unable to identify or stop harmful communications

Inadequate communication network architecture that causes excessive external connection latency

It may make it more difficult to quickly communicate important information, including protection settings.

3.18 DDOS or Distributed Denial of Service Attacks

This study concentrated on DDOS attacks in the context of Smart Grid s and how the suggested remedy, which makes use of modern technology, can successfully lessen the negative impact on the grid system. When necessary, a DoS attack renders a critical resource inaccessible to authorized users in a sufficient volume. Every communication channel in the power system needs to be as open as possible, especially when the system is about to become unstable, and a critical control action is needed. The dependability required for contemporary power grids would be jeopardized if the DoS attack thrives in such an environment [60]. One kind of attack that infected systems utilize to target a single system is the DDoS attack. The recruitment and actual attack phases of agents pose a significant cyber danger to Advanced Metering Infrastructure [61].

Agents Recruitment Phase: an attacker must first identify the weak meters deemed to be the agents to launch a DDoS assault in the AMI network. A security flaw in one meter may be present in numerous other meters due to the AMI network's vast number of homogenous devices. The attacker then connects to a large number of IP-based intelligent meters that have previously been compromised by malicious code. By taking advantage of flaws in both software and hardware, the attacker can alter the firmware or implant the malicious application during the communication connection rather than logging in with several agents. To disseminate attack malware, the administrator ought to select an appropriate propagation model. In the repository model, the attacker places the malicious program in a file source, and each agent copies the code from it. In the back-chaining

model, the attacker forces the dangerous agent to download the malware from the attacking hos; or in the autonomous model, the agents are infected and exploited without having to download the malware from a designated source. Finding the assault source among several meters becomes more difficult when IP spoofing is used to conceal the infected agents [61].

Phase of the Actual assault: a DDOS assault on AMI infrastructure can be initiated in three different methods [61].

Protocol attacks: the attacker can use the user's resources by exploiting the protocol's flaws. For instance, in an AMI environment that employs Transportation Control Protocol, a TCP SYN flooding attack can deactivate the service on the head-end or data-collecting unit.

Attacks on infrastructure: in this scenario, the attacker may interfere with the routing tables in order to disperse the AMI packet exchange infrastructure's action efficiency of packet distribution.

Attacks on bandwidth: it is possible to control systems so that they send the system user an excessive number of communication packets. The authorized user will consequently drop some of the genuine packets due to the flooded traffic and the drop ratio can be substantial.

Jamming attack: an attacker can use a jamming assault, a kind of Denial of Service (DoS) attack, to interfere with communications in real time. Due to jamming, state estimate and online checking are only able to display the system's actual working status. The associated electricity price will be calculated incorrectly [62]. The main reason for starting the attack was to manipulate the power market's prices. When jamming happens, the control center would not be able to access the pricing mechanism, which is dependent on

the sensors' state assessment. The discrete-time method, which uses time intervals, is one of the jamming assault techniques. Because an excessive jamming attack could result in a complete region power failure, which would lead to an inaccuracy in price manipulation, only a small percentage of sensors out of all wireless sensor networks (WSNs) can be attacked in SG. Additionally, a wide area jamming attack can increase the likelihood of discovery. The following is the process of a jammer attack:

- The network's channels will jam when a time interval begins, making measurements impossible and leaving the real-time prices at associated buses unknown.
- The opponent watches the electricity market over time and tampers with the dubious readings.
- The opponent can get real-time measures and predict real-time prices when the jamming is stopped.

3.19 The Microgrid Vulnerabilities

Open, unused ports. These ports allow enemies to eavesdrop and change the controller settings [16]. They also expose backup system data and configurations.

Software/firmware upgrading process: if the administrator does not safely carry out the update, malicious upgrades might be pushed via man-in-the-middle or injection attacks, giving the adversary control of the microgrid controller or access to private data.

Internet/Wi-Fi connection capabilities: attackers can easily access internet capabilities. When using third-party software, make sure it is safe and secure.

Hardware supply chain: in order to defend against attacks based on hardware, compromised hardware supply chain systems should also be taken into account. The same

cybersecurity norms and restrictions that apply to microgrids should also apply to external devices like USB drives and laptops.

Propagation of compromise: independent microgrid controllers may become compromised if a central microgrid controller is compromised. This might be accomplished by sending viruses or harmful updates/settings to the separate microgrid controllers via direct communication channels, particularly if the security measures of the linked microgrids are weak or nonexistent. Could more serious cascading failures result from the expansion of cyber compromise in various microgrids? In order to achieve resilient operation of the networked microgrids, these are important issues to address.

3.20 How Environmental Attacks Occur /The Seven Kill Chains]

A cybersecurity model called the cyber kill chain (CKC) was created to help security professionals better understand the steps an attack must take in order to thwart it at every turn [63]. The seven kill chains from reconnaissance to action on the target are briefly summarized in Fig. 13 below.

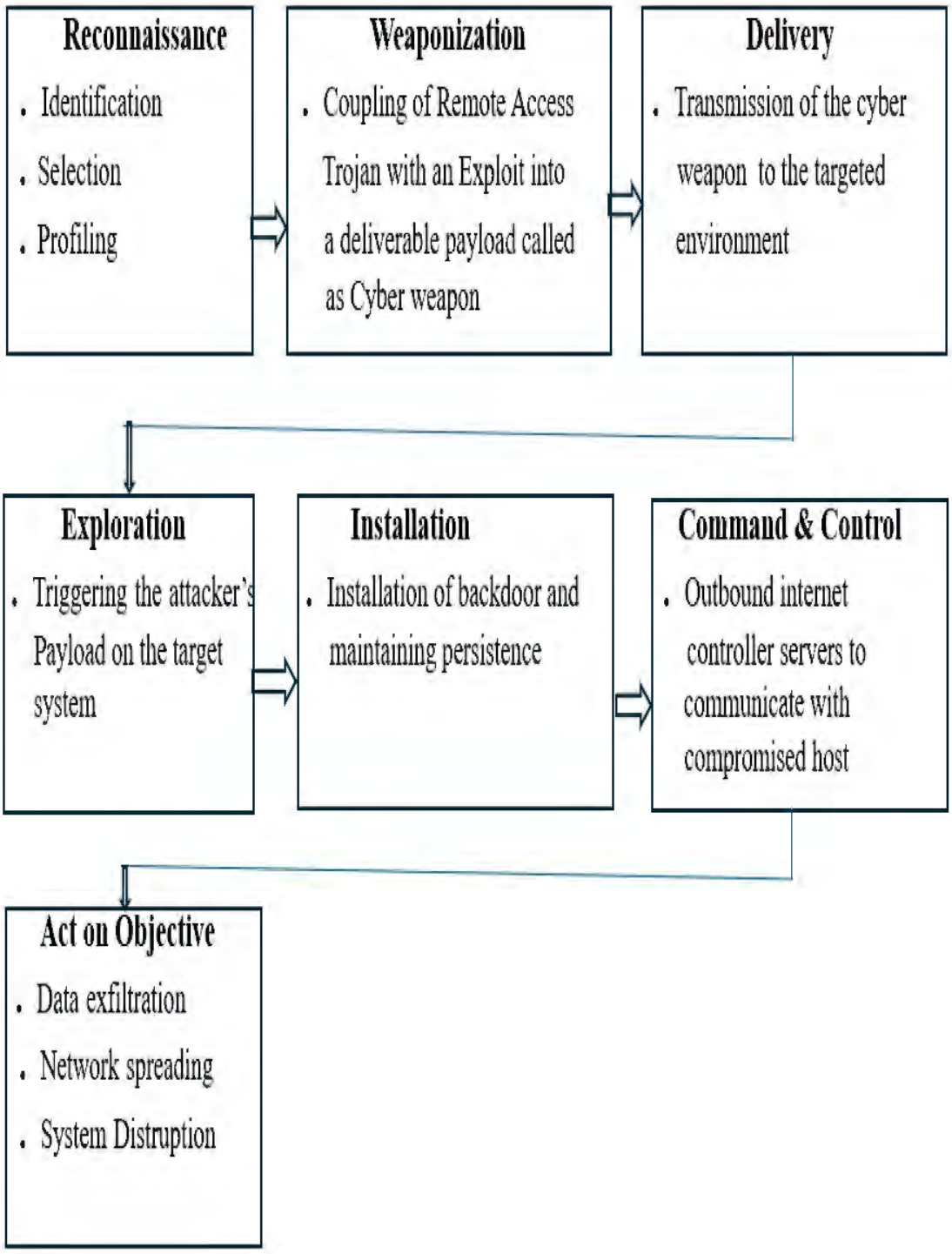


Fig. 13. Seven Kill Chains [63].

4. TECHNIQUES

In this section, the tools/devices/materials, codes, algorithms, and Lab apparatus simulation techniques used for the Detection and Mitigation of Distributed Denial of Service (DDOS) attack: Application to Smart Grid Communication Network have been discussed in detail

4.1 Materials, Devices and Tools

Building the Flow Collector, Flow Sensor, and Secure Network Analytics management console virtual machines (VMs) was the first step in this dissertation's SNA deployment strategy. IP addresses were then assigned in accordance with the simulated Smart Grid Communication Network designed model, as illustrated in Fig. 20. One of the prerequisites for implementing the Secure Network Analytics tool is the Flow Rate Licenses. In accordance with the simulated communication network, source and target virtual machines (VMs) were constructed and given IP addresses. Both are capable of sending and receiving ICMP and ping packets without any problems. During regular or baseline operation, the SNA management console also recorded the communication between the attacker's system and the target server. Traffic from the attacker's system to the target server could be recorded on the SNA control interface and thin client without any problems, according to the model configuration. In order for the model SNA tools to capture, detect, and mitigate the DDOS assault without affecting the target system, we later installed or swallowed malicious input or DDOS payloads on the attacker's computer to perform DDOS operations on the target server or workstation. As illustrated in Fig. 43d, the simulation will notify the administrator when the flow level on the target system

surpasses the baseline that our coding/algorithm has established to take appropriate action before influencing the target server.

4.2 Flow Collector VM for Secure Network Analytics [FC]

Telemetry and application data gathered from exporters like routers, switches, firewalls, endpoints, and other network infrastructure devices were aggregated, normalized, and analyzed by a flow collector, which can be a physical or virtual appliance. It had a NetFlow/SFlow/IPFIX Collector with great performance and can support up to 25 units per deployment. The FC back view of connectivity is displayed in Fig. 14 below. Up to 4096 exporters, up to 65535 interfaces, and up to 250,000–500,000 fps was supported by this 1U physical appliance.

1. SFP (eth0 (optional) FC Management for Data Store deployment only and Primary Collection) (10 Gbps SFP+ copper twinax cable)
1a. SFP Reserved
2. Serial Console (115200 8-N-1)
3. (default) FC Management and Primary Collection (eth0) (100Mbps/1Gbps/10Gbps)
4. Additional Collection (eth1) (100Mbps/1Gbps/10Gbps)
5. CIMC Management (100Mbps/1Gbps)

Fig. 14. Flow Collector view [64].

4.3 Flow Sensor VM or Secure Network Analytics [FS]

Another part that offered telemetry for parts of the switching and routing architecture that were unable to produce NetFlow natively was the Flow Sensor. In order to improve security analytics, it also makes it possible to see the application layer data and other security context. By collecting application data and producing contextually

intelligent warnings, the 1U physical Flow Sensor 4210 offered true layer 7 application visibility. Fig. 15 below shows the connectivity back view of FS.

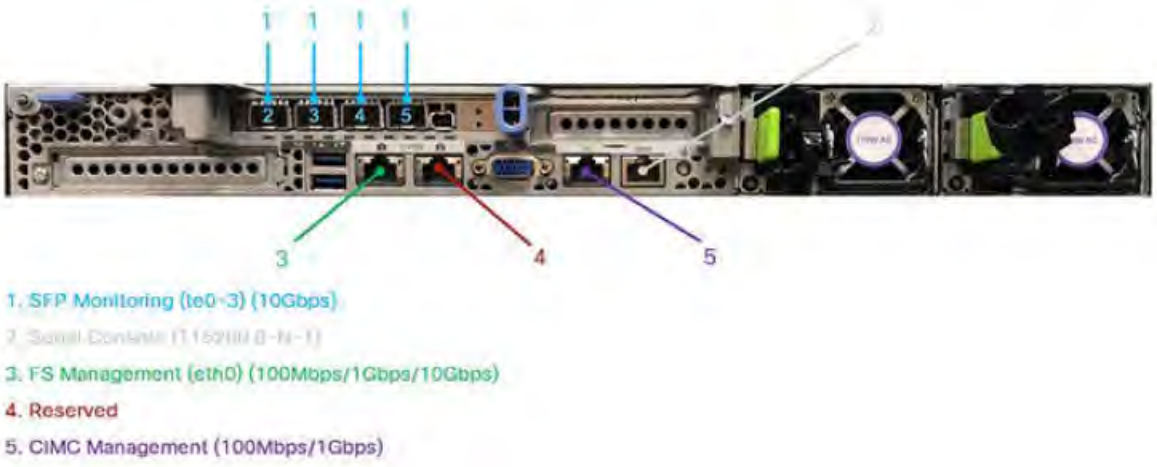


Fig. 15. Flow Sensor view [64].

4.4 Management Console VM for Secure Network Analytics [SMC]

A physical or virtual device called SNA Security Manager collects, arranges, and displays data from up to 25 flow collectors and other sources. With a maximum of two devices per deployment, it serves as the central management for all Secure Network Analytics devices via a Secure Network Analytics user interface. Fig. 16 shows the connectivity back view of SMC

Fig. 16. SMC view [64].

4.5 Flow Rate License for Secure Network Analytics

Telemetry was gathered, managed, and examined by Secure Network Analytics. Using the network FPS Estimation Tool, the number and kind of switches, routers, firewalls, and probes determined the flow rate license. It was necessary for the manager to collect, monitor, and analyze flow telemetry and aggregate flows. Fig. 17 below shows the illustration of a Flow License.

Fig. 17 . SNA Flow Rate License [64].

The amount of flows that can be collected is known as the Flow Rate License, and it is precisely based on flows per second (fps). The components of Secure SNA Analytics employed in this study to identify and counteract DDOS assaults in a Smart Grid system are depicted in Fig. 18.

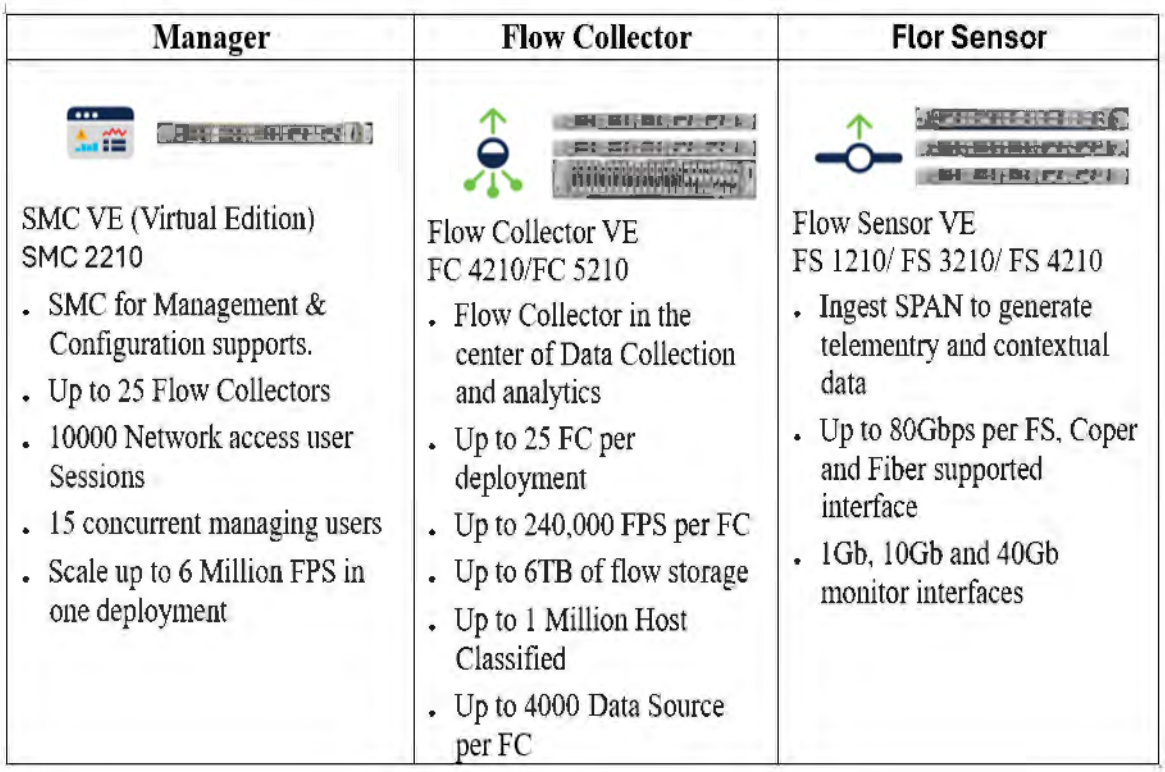


Fig. 18. Components of a Secure Network Analytics Tool [64].

4.6 Algorithm/Flow for Secure Network Analytics TLS Encryption

By employing new kinds of data pieces or telemetry that were independent of protocol specifics, SNA's encryption capabilities through Encrypted Traffic Analytics (ETA) technologies assisted with uncovering hidden corners in encrypted traffic without the need for decryption. This improved encrypted traffic telemetry was produced by the Secure Network Analytics Flow Sensor. To safeguard the integrity, confidentiality, and authentication of data while in transit, SNA employed the TLS encryption method for both symmetric and asymmetric encryption. As the name suggests, symmetric encryption is used to exchange data within a secure session, while asymmetric encryption is used to create a secure session between a client and a server. Fig. 19 displays the technology and functions of the TLS algorithm.

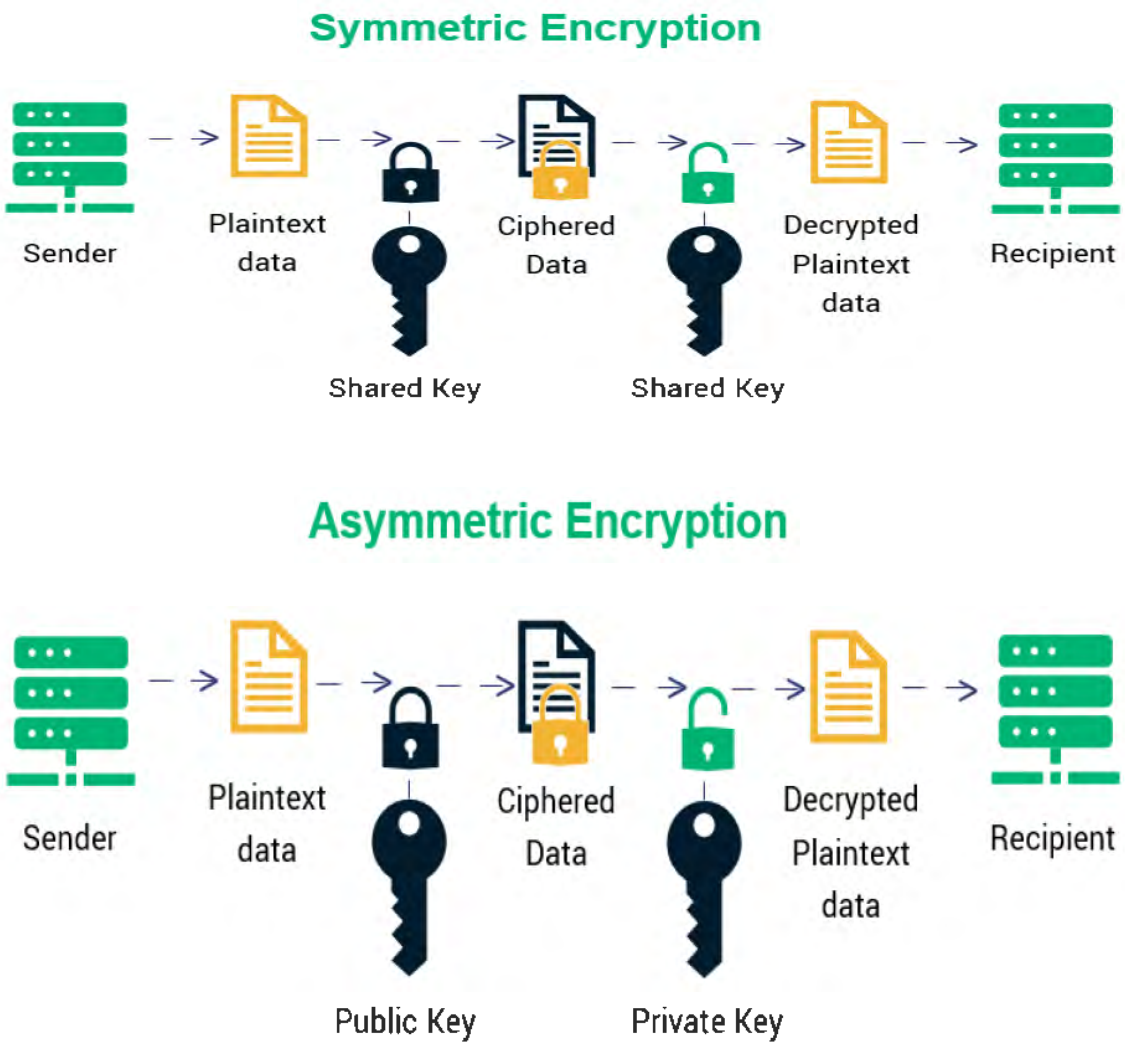


Fig. 19. The algorithm/flow for SNA TLS encryption [65].

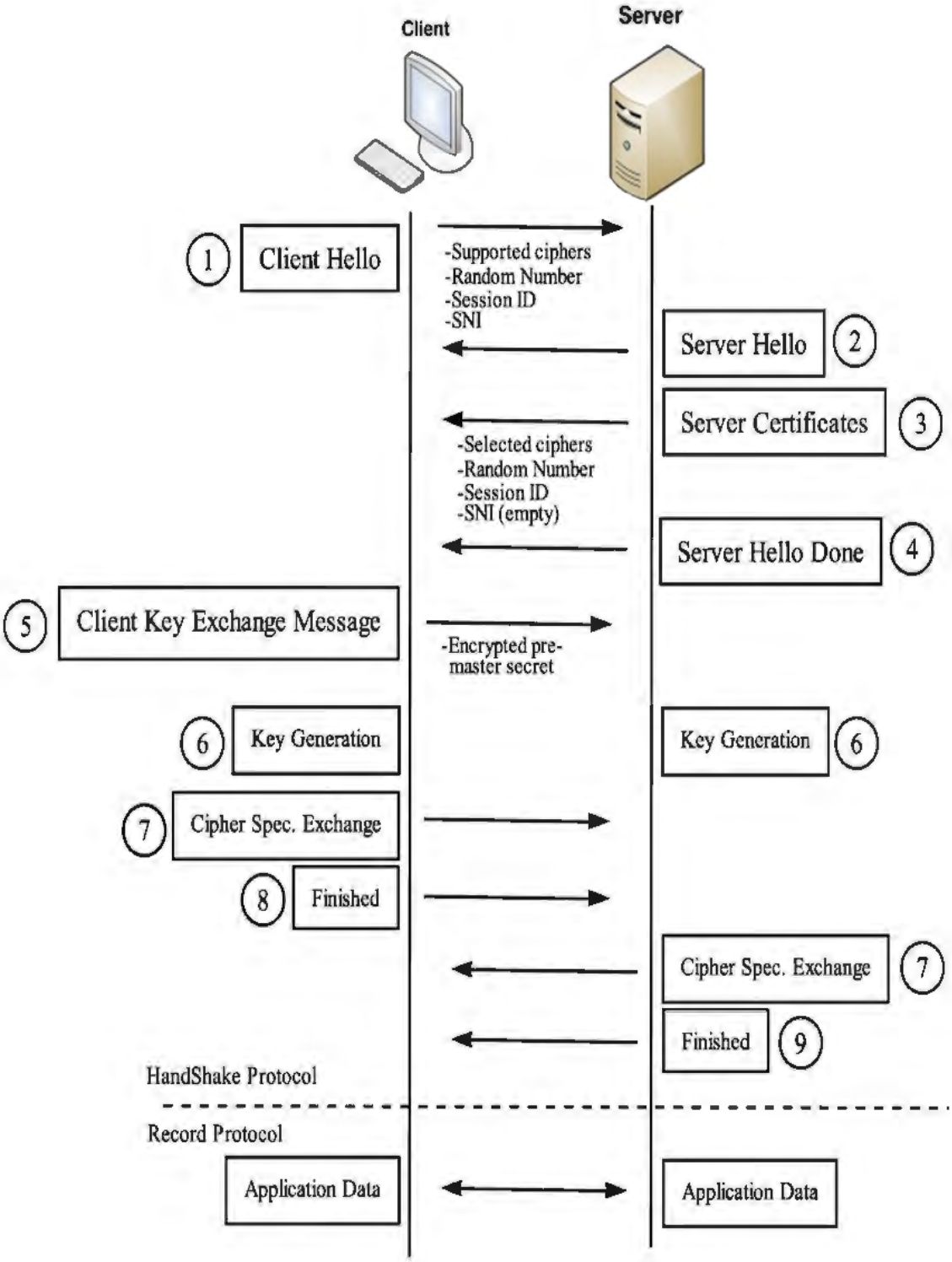
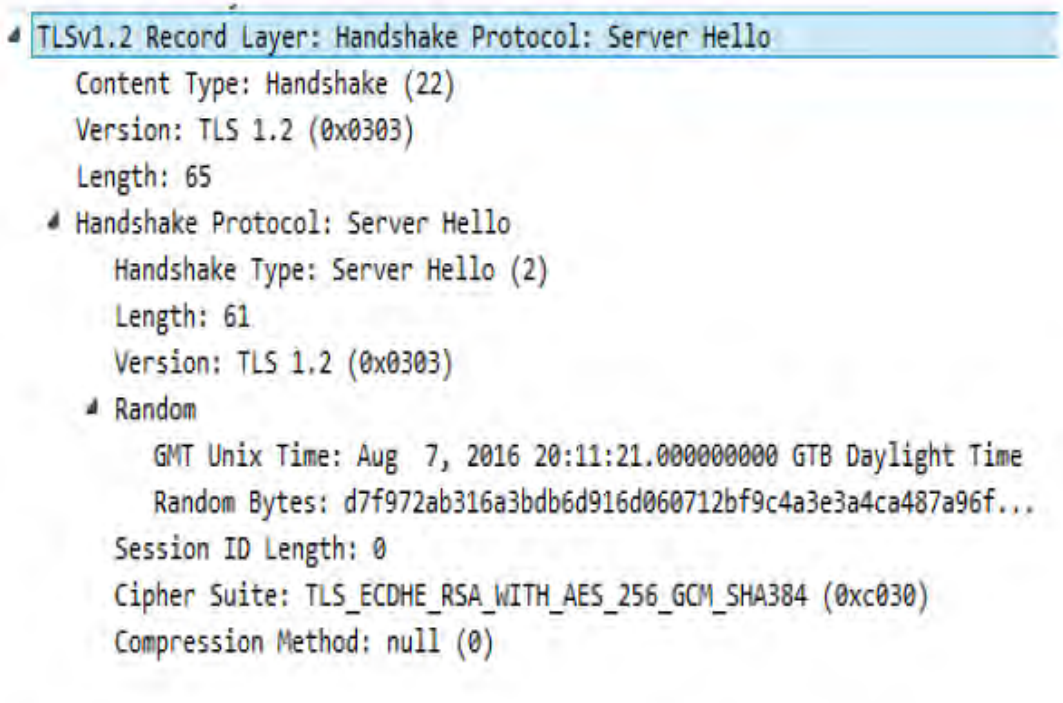


Fig. 20. The algorithm/flow for SNA TLS encryption [65].



Description	Value
TLS_AES_128_GCM_SHA256	{0x13,0x01}
TLS_AES_256_GCM_SHA384	{0x13,0x02}
TLS_CHACHA20_POLY1305_SHA256	{0x13,0x03}
TLS_AES_128_CCM_SHA256	{0x13,0x04}
TLS_AES_128_CCM_8_SHA256	{0x13,0x05}

Fig. 21. The algorithm/flow for SNA TLS encryption [65].

4.7 Smart Grid Secure Network Analytics Tool Alarm Types

Fig. 22. displays the Smart Grid SNA dashboard along with the several types of alarms.

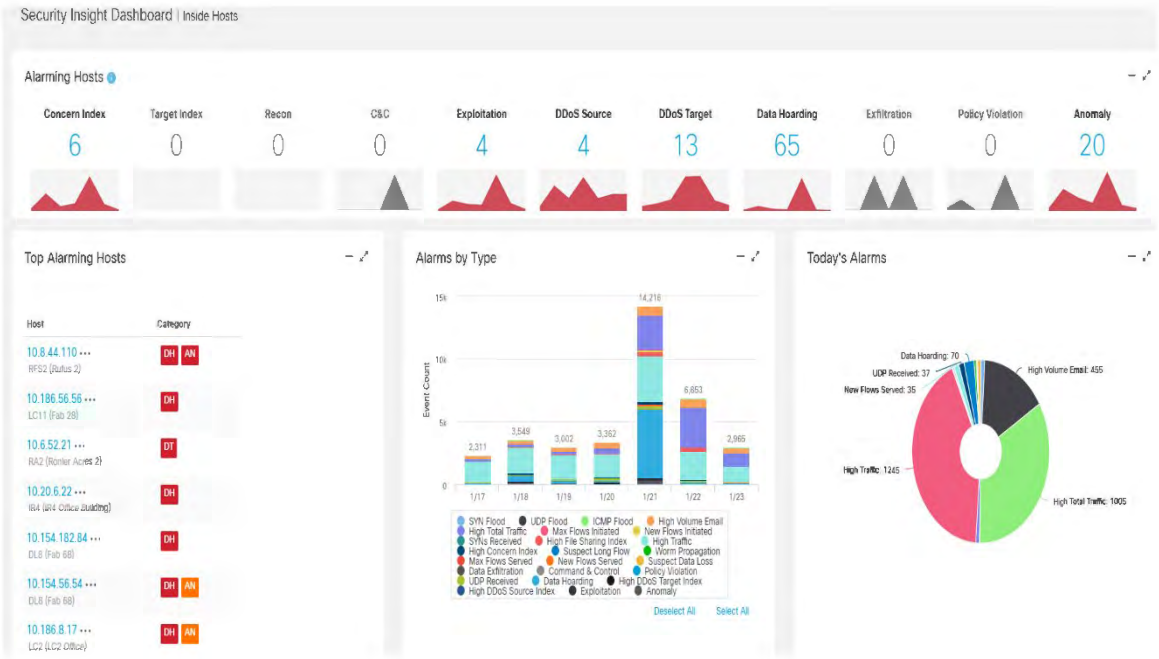


Fig. 22. Categories of Smart Grid SNA Dashboard Alarms.

4.8 Categories of Alarm

An observed behavior event that satisfies a small number of criteria is represented by the alarm category. An alert is triggered when network activity satisfies or surpasses a specific set of criteria designated for this alarm type. Every alarm category contains a list of security events that can trigger alarms and contribute index points. Depending on the settings used in policies, a security event is an algorithm that searches for particular activity on the network and can provide the user notification. It accomplishes this by either assigning index points to alarm categories, which may then cause a host alarm, or by directly creating a host alarm if configured to do so. A security incident that sets off an alarm is known as a host alarm.

Target Index and the Concern Index

Target Index monitors hosts whose worry index has significantly climbed or surpassed the worry Index (CI) threshold. The same security events are used by the Concern Index and Target Index categories. A Concern Index alarm is generated if an event is triggered by a source host. A Target Index alarm is generated if a target host initiates an event.

Recon

The existence of unapproved and perhaps harmful TCP or UDP scans against the hosts of a company is known as recon. Reconnaissance scans, which can originate from both inside and outside the company, are a precursor to network attacks.

Control and Command

Control and command show that there are hosts or servers on the network that are trying to get in touch with a C&C server but are actually bot infected.

Exploitation

In this instance, exploitation monitors hosts' direct attempts to attack one another, including worm propagation and brute-force password cracking.

Source of DDoS

When a host is marked as the origin of a DDoS attack, it is said to be the DDoS Source.

Target for DDoS

A host has been recognized as the target of a DDoS attack when it is marked as DDoS Target.

Hoarding Data

Hoarding Data shows that an abnormal volume of data has been downloaded from one or more hosts by a source or target host within a network

Exfiltration

Exfiltration monitors both external and internal sites to which an unusual volume of data has been sent. An alarm for data exfiltration will sound if a host initiates enough of these activities to surpass a predetermined threshold.

Violation of policy

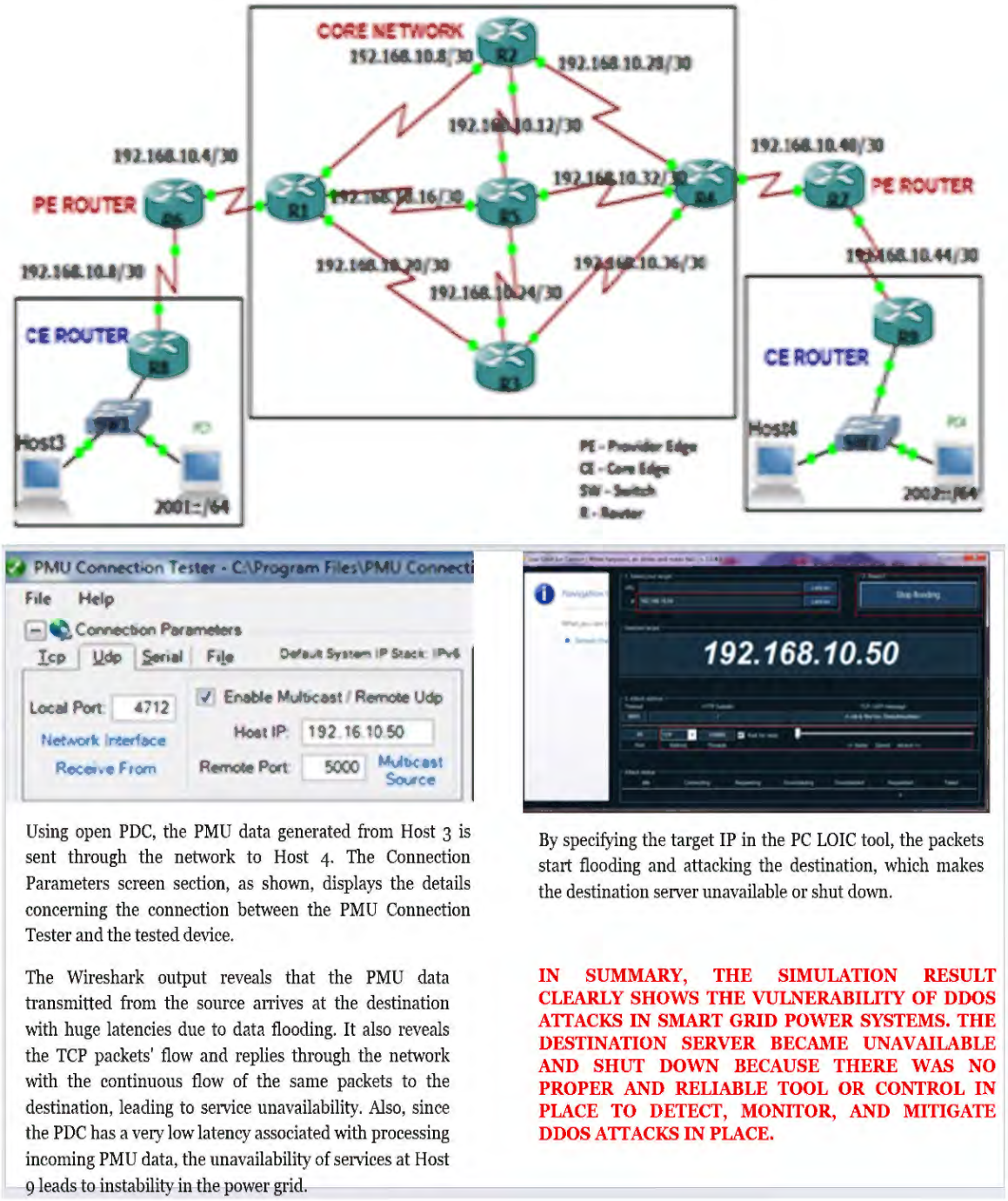
Violation of policy means the subject is acting in a way that is against standard network guidelines.

An irregularity

These events show hosts acting strangely or producing odd traffic but not fitting into another activity category are tracked by anomaly.

4.9 Current and Proposed Design Using GNS3 and SNA Tools

The present Smart Grid Communication Network design utilizing GNS3 is depicted in Figs. 23. However, it is limited in that the simulation result made it evident that a Smart Grid power system was susceptible to DDOS attacks. Because there was no appropriate and trustworthy technology or control in place to identify, monitor, and mitigate DDOS attacks, the destination server went down and became unavailable.



Using open PDC, the PMU data generated from Host 3 is sent through the network to Host 4. The Connection Parameters screen section, as shown, displays the details concerning the connection between the PMU Connection Tester and the tested device.

The Wireshark output reveals that the PMU data transmitted from the source arrives at the destination with huge latencies due to data flooding. It also reveals the TCP packets' flow and replies through the network with the continuous flow of the same packets to the destination, leading to service unavailability. Also, since the PDC has a very low latency associated with processing incoming PMU data, the unavailability of services at Host 9 leads to instability in the power grid.

By specifying the target IP in the PC LOIC tool, the packets start flooding and attacking the destination, which makes the destination server unavailable or shut down.

IN SUMMARY, THE SIMULATION RESULT CLEARLY SHOWS THE VULNERABILITY OF DDOS ATTACKS IN SMART GRID POWER SYSTEMS. THE DESTINATION SERVER BECAME UNAVAILABLE AND SHUT DOWN BECAUSE THERE WAS NO PROPER AND RELIABLE TOOL OR CONTROL IN PLACE TO DETECT, MONITOR, AND MITIGATE DDOS ATTACKS IN PLACE.

Fig. 23. Grid Communication Network Simulations using GNNS3 Cont [66].

Scenario Formation

Fig. 24. uses the SNA tool to illustrate the proposed networked Smart Grid and its communication computer network design, which was taken into consideration in this study. Host 1 (192.168.232.209) was the source in this network, and Host 2 (192.168.233.214) was the destination, both of which were connected to Routers R3 and R9. The Customer Edge networks included the routers R1 and R9.

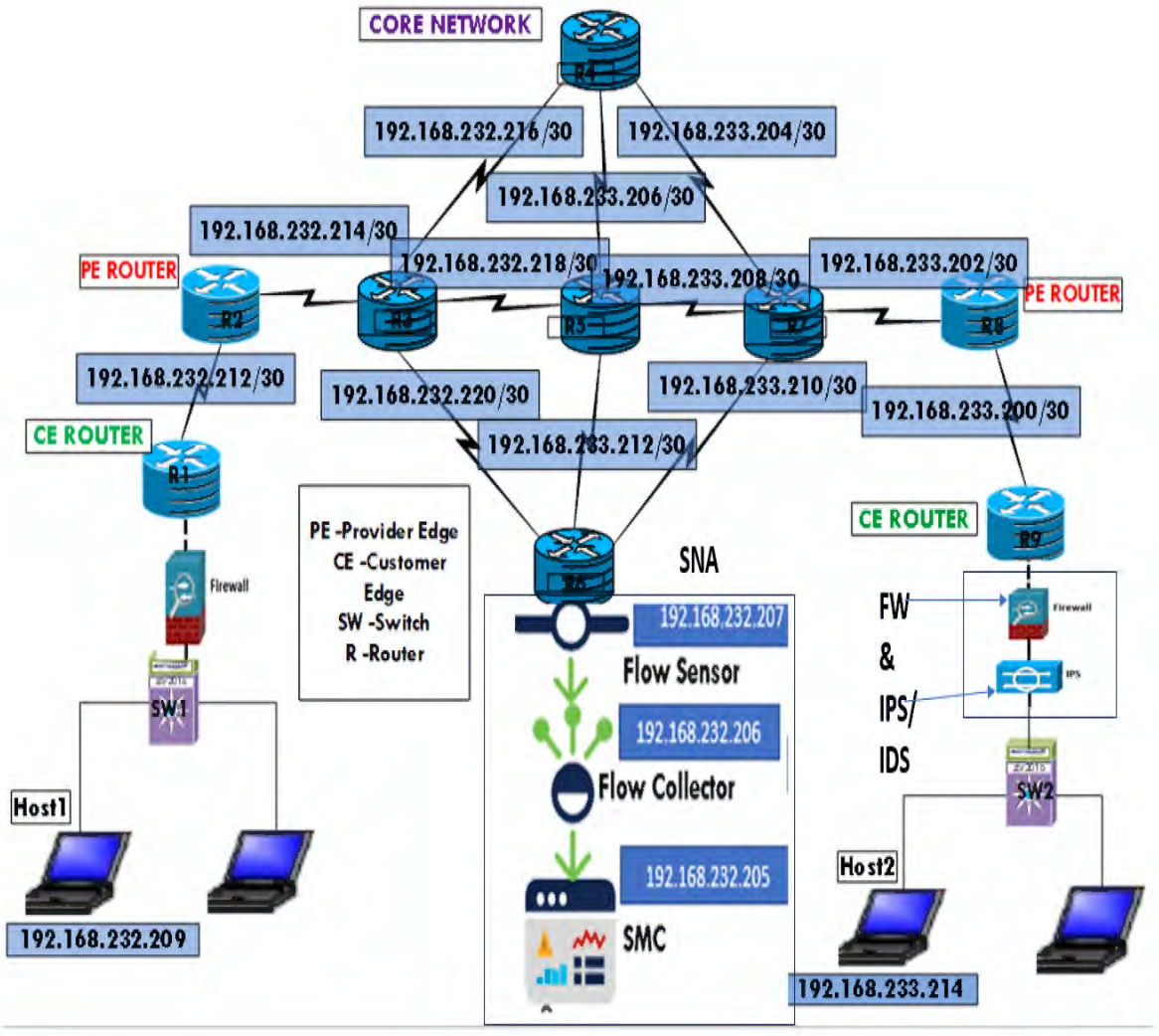


Fig. 24. SNA Tool-Based Smart Grid Communication Network Proposals.

In this case, Host 1 and Host 2 were both linked to a virtual computer that was built using VMware. An ISP router included all other routers. As seen in the accompanying Fig., addresses were assigned after the network was created. In this case, we went with IP addressing, a logical addressing method. This research primarily used the IPv4 addressing scheme, which was subnetted using VLSM to minimize IP waste. Every network in the suggested architecture was IPv4-enabled and successfully linked to the network. The detailed instructions for building each of the virtual machines utilized in this study are provided below.

4.10 Build a Flow Collector

The procedures or actions taken to build the Flow Collector utilized in this study are listed below.

After the VM's assignment.

Step 1: Navigate to the Network option and enter the configuration mode.

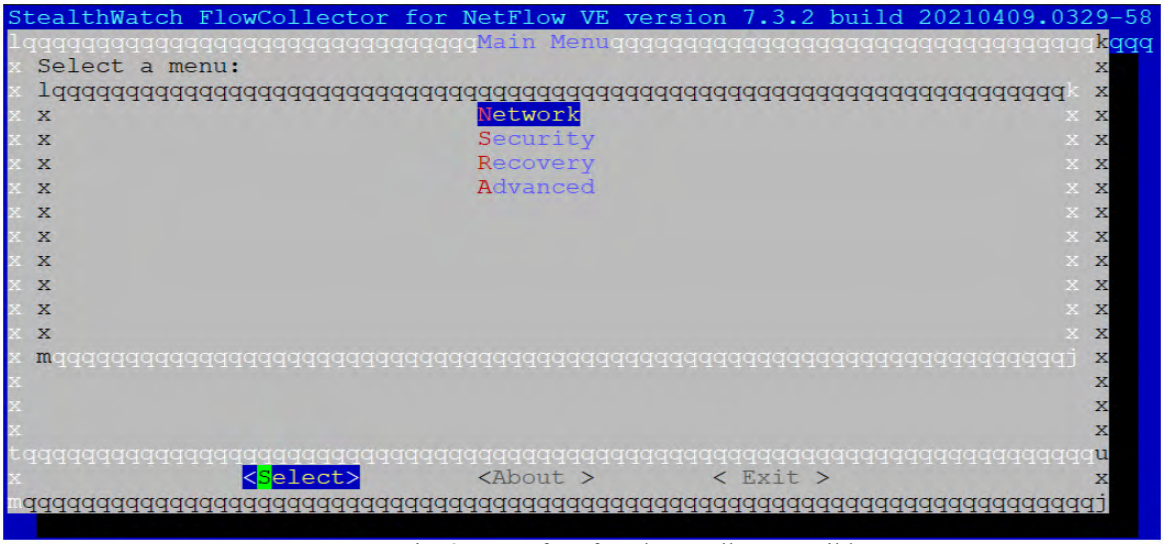


Fig. 25. Interface for Flow Collector Build.

Step 2: Set up FC's hostname and IP address information as indicated below:

The FC IP address is 192.168.232.206

The Subnet Mask IP address is 255.255.255.255.192/26

The Gateway address is 192.168.232.193

The Broadcast IP address is 192.168.232.255

The Hostname is fm2lab-sw-fc01

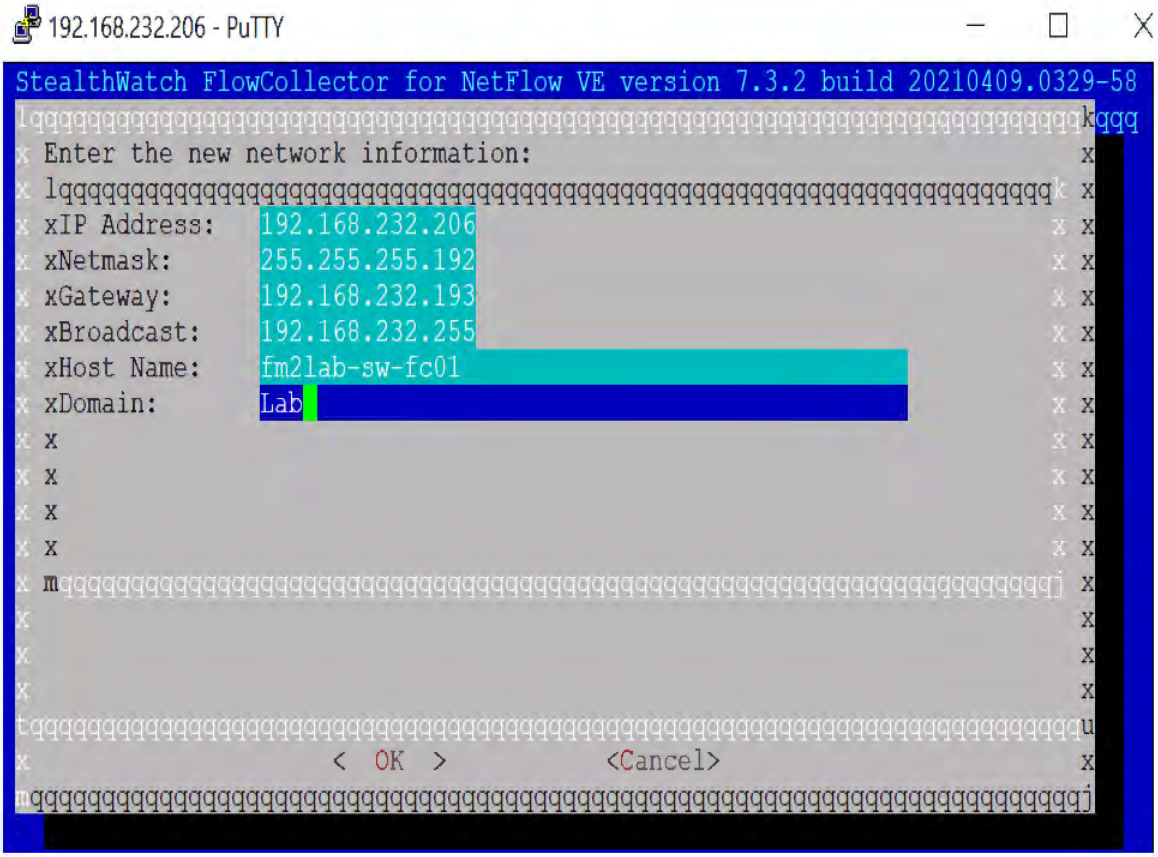


Fig. 26. Configuring Network Interface for the Flow Collector.

Step 2: Verify access to the FC VM console using the CLI as indicated below:

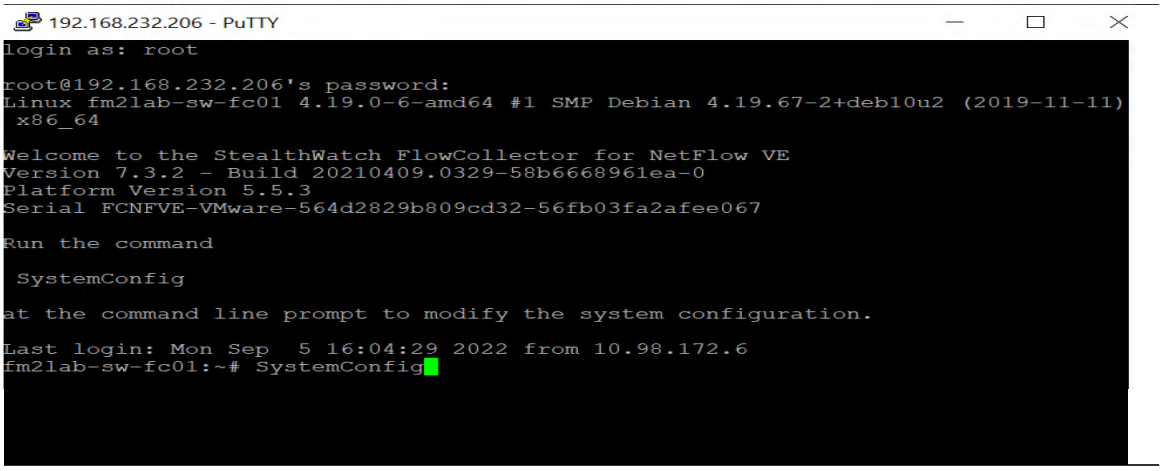


Fig. 27. Interface for Flow Collector SSH/CLI.

4.11 Build a Flow Sensor

The procedures or actions taken to construct the Flow Sensor utilized in this study are listed below.

Following the VM's assignment,

Step 1: Navigate to the Network option and enter the configuration mode.

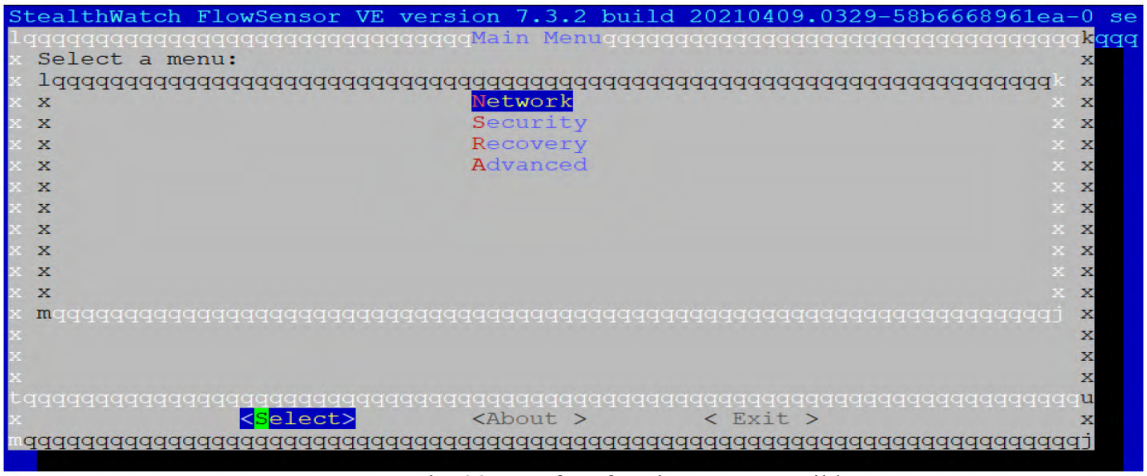


Fig. 28. Interface for Flow Sensor Build.

Step 2: Set up FS's hostname and IP address information as indicated below:

The FS IP address is 192.168.232.207

The Subnet Mask IP address is 255.255.255.255.192/26

The Gateway address is 192.168.232.193

The Broadcast IP address is 192.168.232.255

The Hostname is fm2lab-sw-fs01

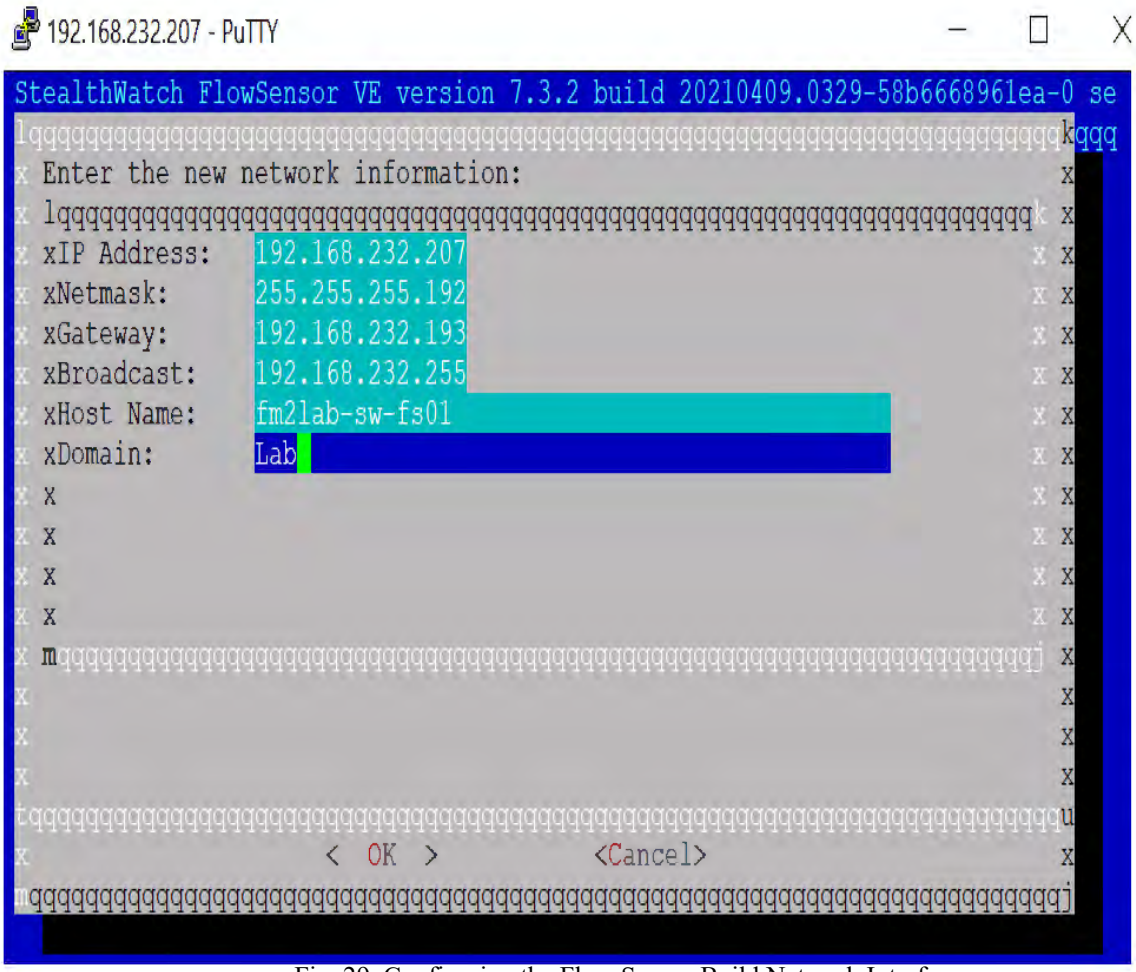


Fig. 29. Configuring the Flow Sensor Build Network Interface.

Step 2: Verify access to the FS VM console using the CLI as indicated below:

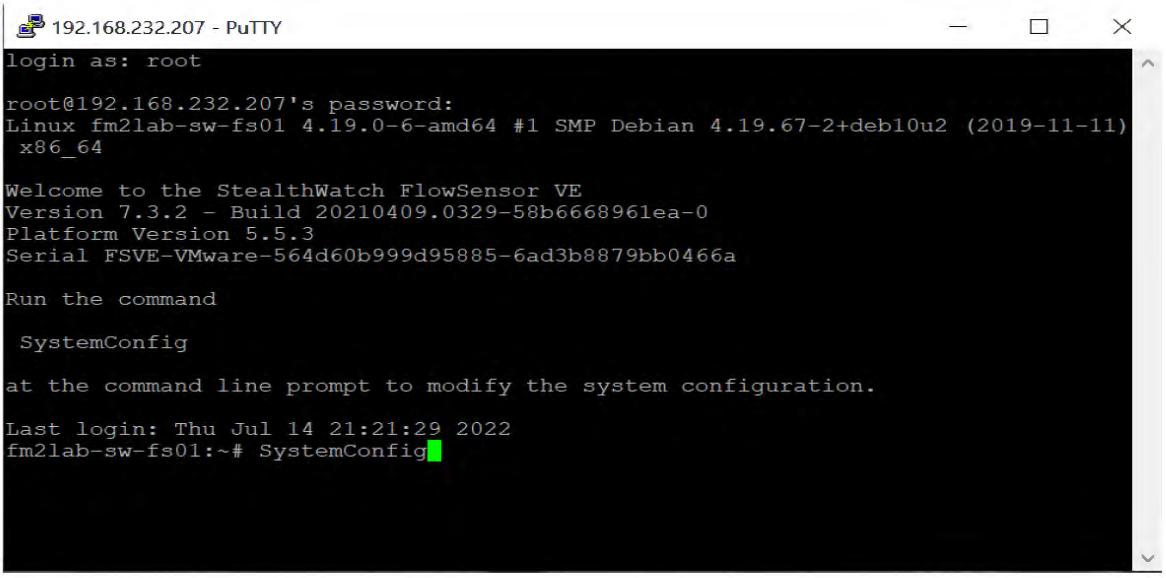


Fig. 30. Interface for Flow Sensor SSH/CLI.

4.12 Build *a* Secure Network Analytics Management Console

The procedures or actions taken to construct the SNA Management Console utilized in this study are listed below.

Following the VM's assignment,

Step 1: Navigate to the Network option and enter the configuration mode.

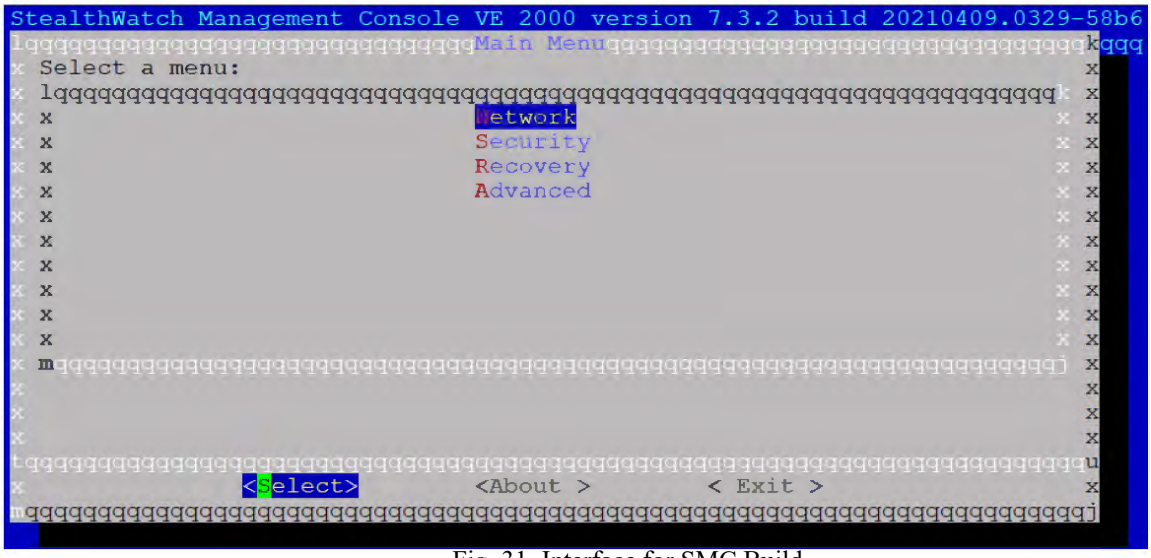


Fig. 31. Interface for SMC Build.

Step 2: Set up SMC's hostname and IP address information as indicated below:

The SMC IP address is 192.168.232.205

The Subnet Mask IP address is 255.255.255.255.192/26

The Gateway address is 192.168.232.193

The Broadcast IP address is 192.168.232.255

The Hostname is fm2lab-sw-smc01

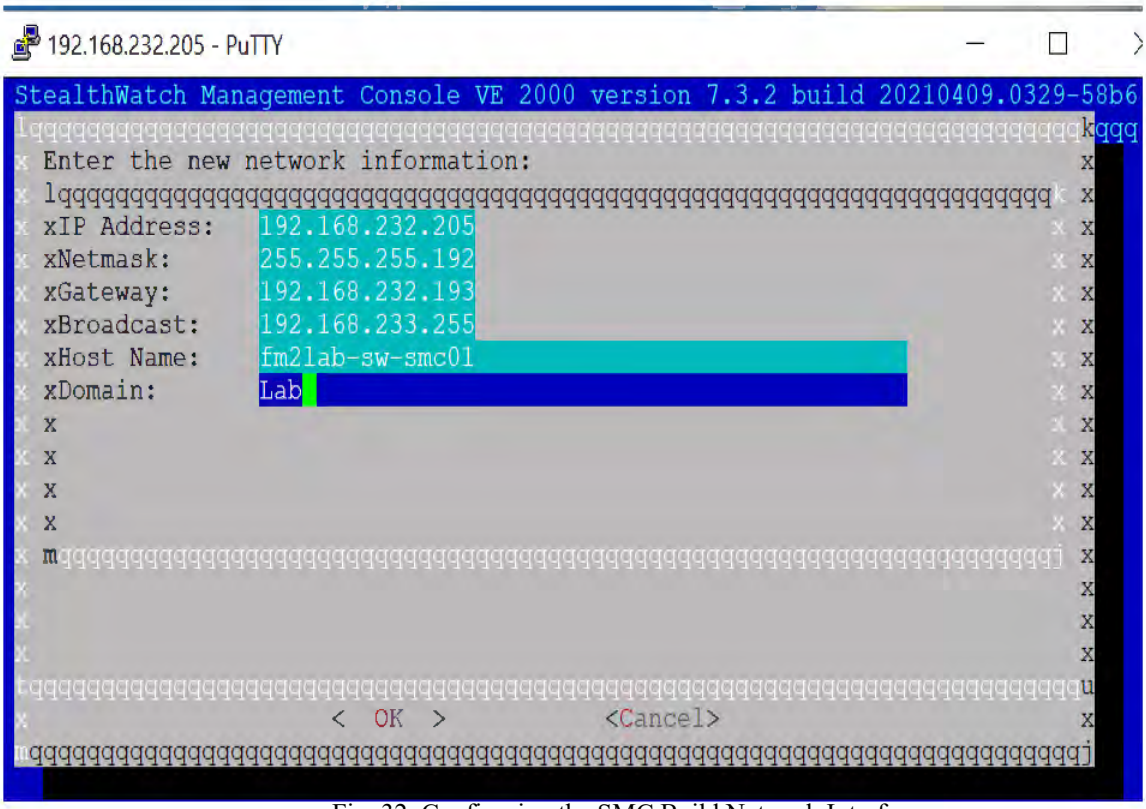


Fig. 32. Configuring the SMC Build Network Interface.

Step 2: Verify access to the SMC VM console using the CLI as indicated below:

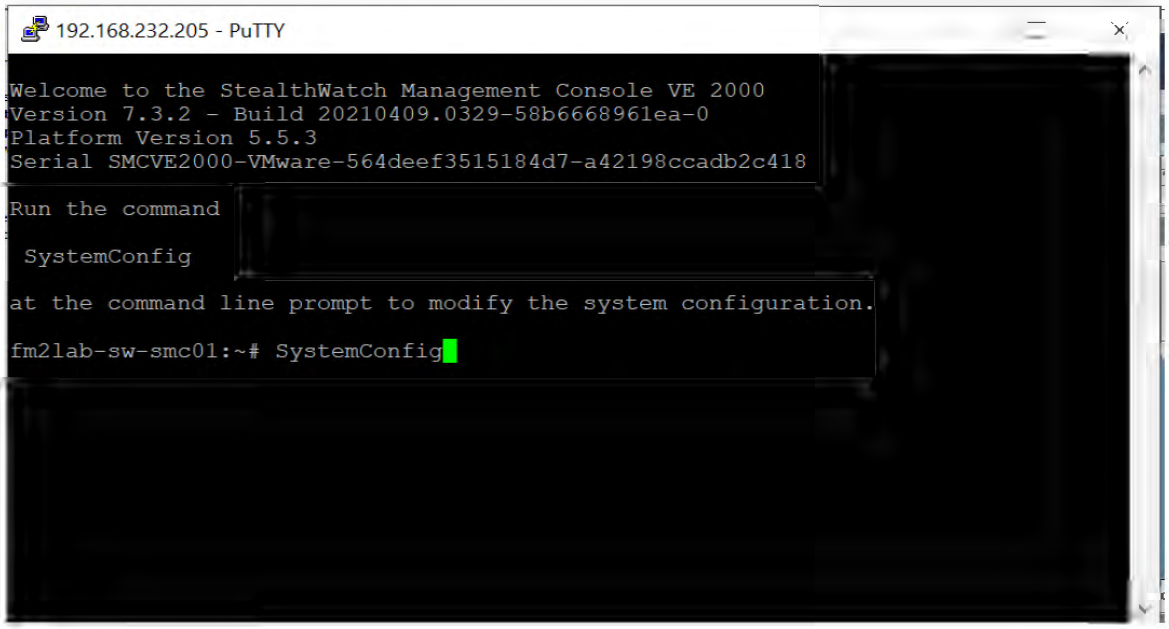


Fig. 33. Interface for SMC SSH/CLI.

4.13 System Build for Attacker-Source Host1

The setup build for the attacker's/Host1 virtual machine utilized in this study is shown below:

Following the VM's assignment,

Step1: Configuring the IP address

The Attacker's IP address is 192.168.232.209

The Gateway address is 192.168.232.193

The Subnet Mask IP address is 255.255.255.255.192/26

The Broadcast IP address is 192.168.232.255

The Hostname is fm2lab-nsm

Step2: Build the System

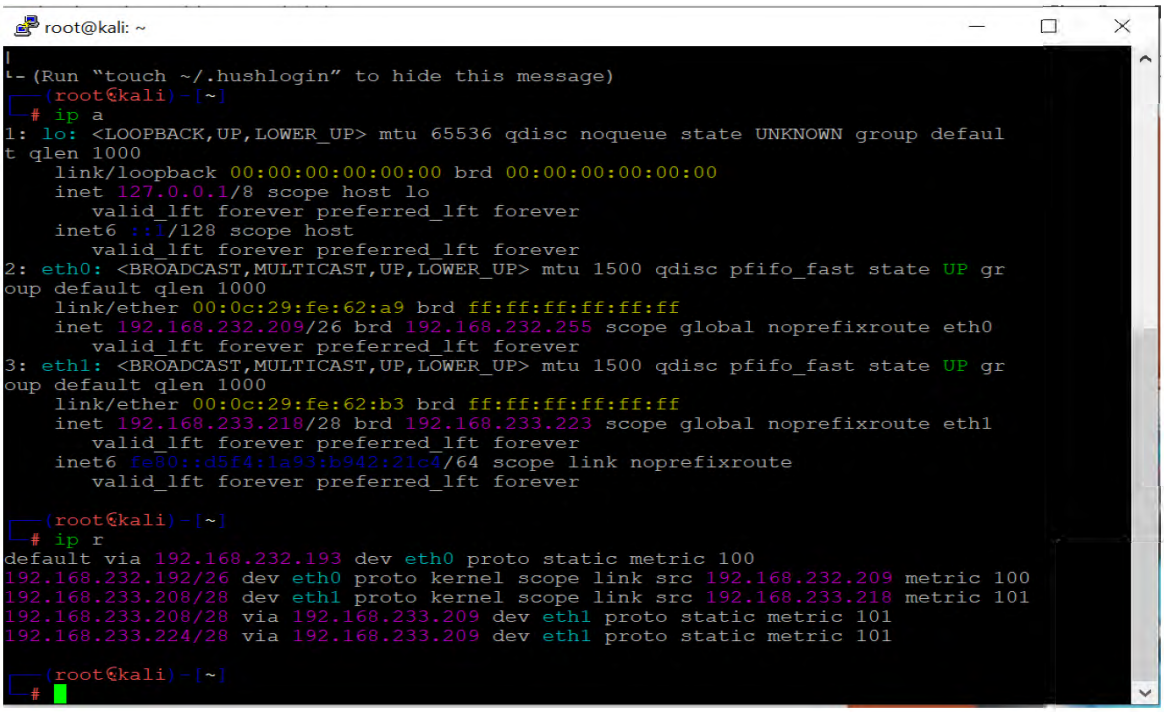


Fig. 34. VM Build for Attacker [Host1].

4.14 System Build for Target-Destination Host

The setup build for the Target's/Host2 virtual machine utilized in this study is shown below:

Following the VM's assignment,

Step1: Configuring the IP address

The Attacker's IP address is 192.168.233.214

The Gateway address is 192.168.233.209

The Subnet Mask IP address is 255.255.255.255.240/28

The Broadcast IP address is 192.168.233.223

The Hostname is ubuntu214

Step2: Build the System

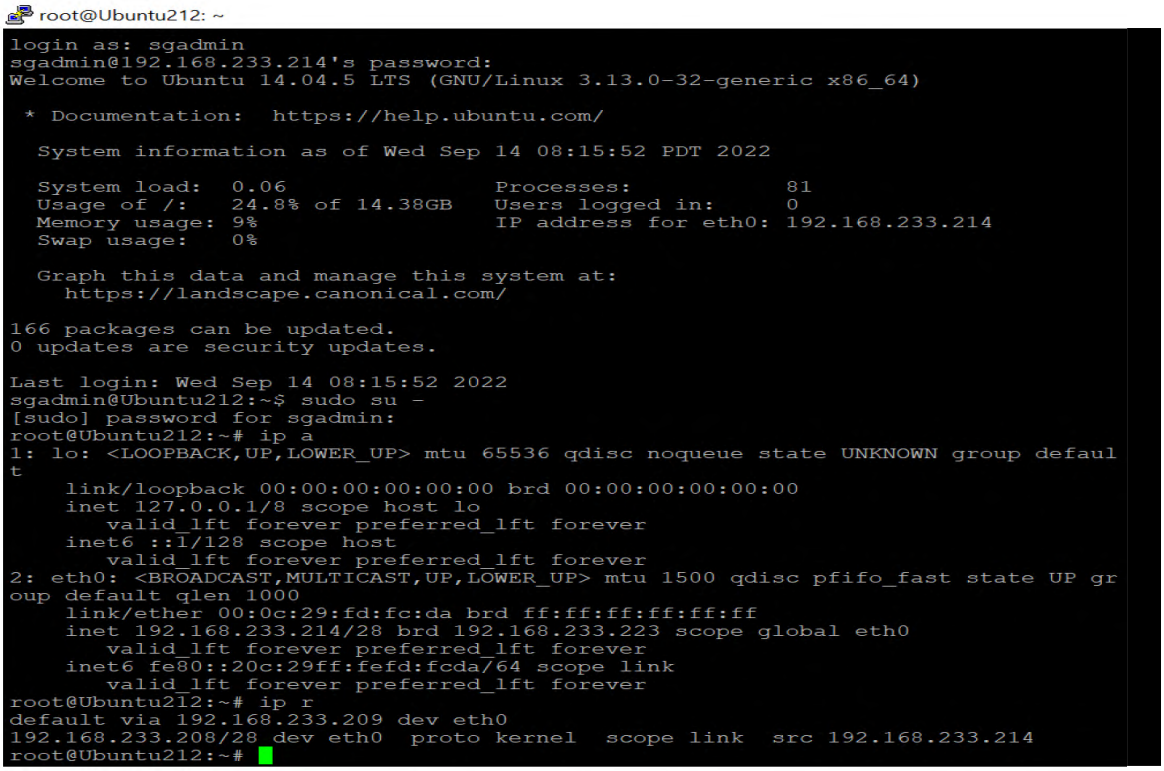


Fig. 35. VM Build for the Target Server [Host2].

Fig. 35 illustrates the connection between the source node [attackers VM] and the destination node [target within host] via the designed/proposed SNA network after all of the virtual machines (VMs) have been constructed and assigned IP addresses. In this study, we utilized the ping command, which was based on the ICMP protocol, to verify that the requested nodes were communicating with one another. The echo request and echo reply between the source and destination allow us to determine the current state of communication. Furthermore, Fig. 35. shows the ping status throughput using our SNA tool to verify that the two virtual machines were successfully communicating. The ability of the SNA to see the traffic going via the grid system was further confirmed by Fig. 37.

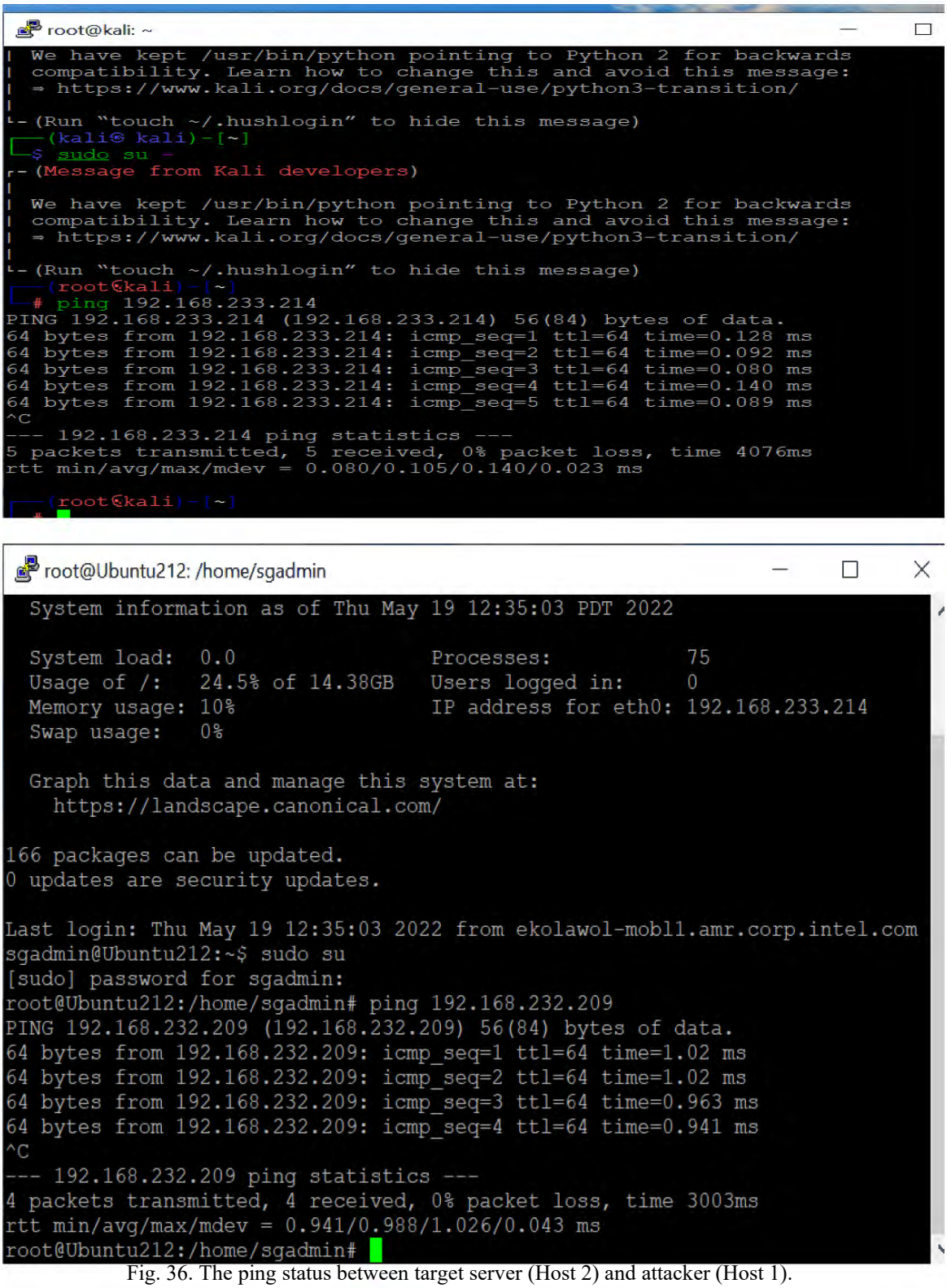


Fig. 36. The ping status between target server (Host 2) and attacker (Host 1).

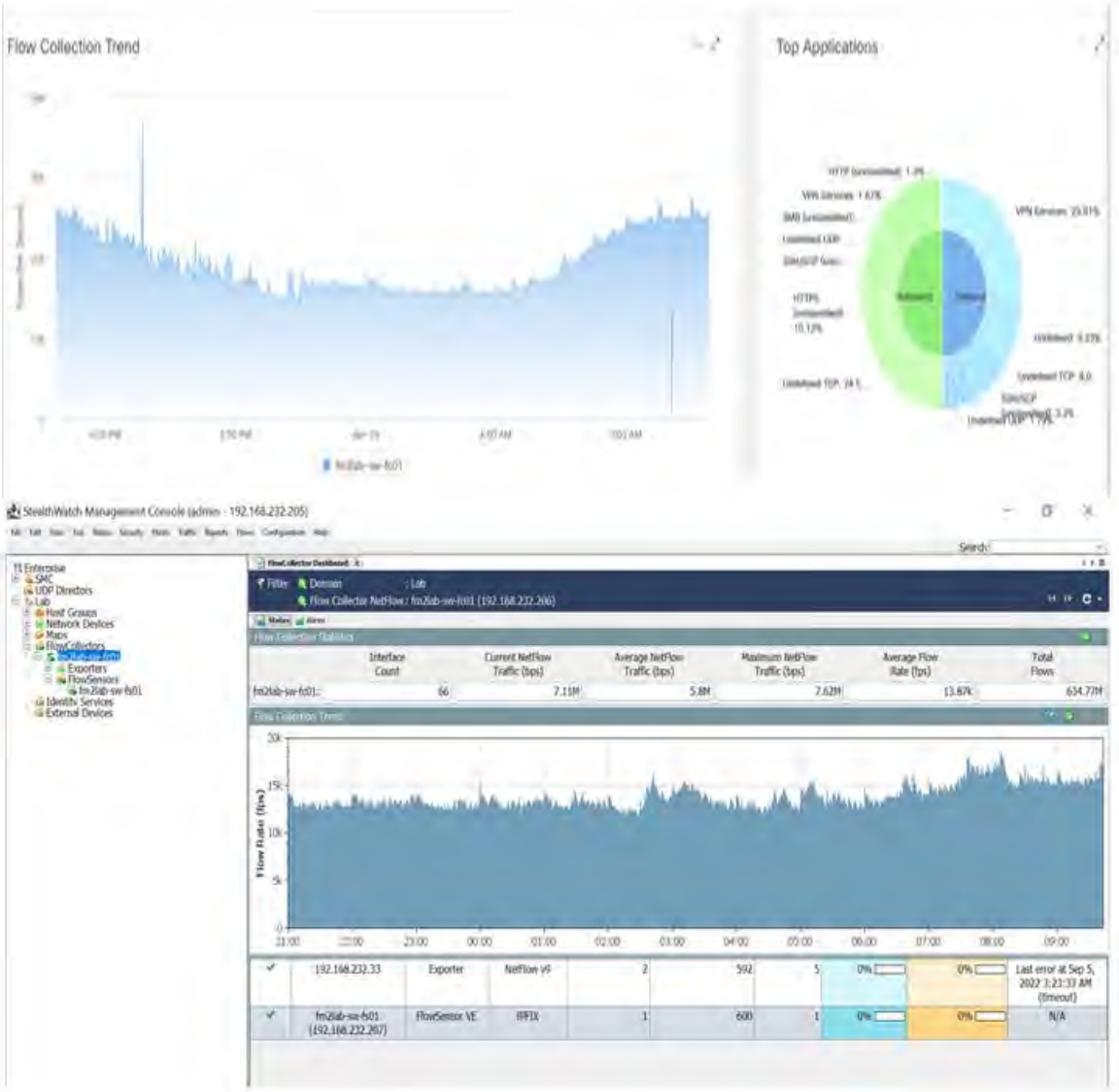


Fig. 37. Flow level between the target server (Host 2) and the attacker (Host 1).

4.15 Flow Data Algorithm with Smart Grid Coding

When the SNA tool was deployed, the default codes in Figs. 38 and 39 were utilized to define parameters depending on baseline per traffic volume. The optimized/modified SNA codes shown in Figs. 40, 41, and 42 were employed in this study to actually identify and mitigate DDOS attacks in the Smart Grid. An important aspect of the research was identifying any anomalies in the Smart Grid system so that they could be quickly identified and fixed before they had an impact on the Grid System. The codes, which displayed the

baseline for the tool used in this study, were written in a language called phyton/scala type. It confirmed the device's typical operating model and traffic volume and alerted management to any deviations from the baseline, which were detected by elevated traffic volume and signified unusual behavior in the surroundings.

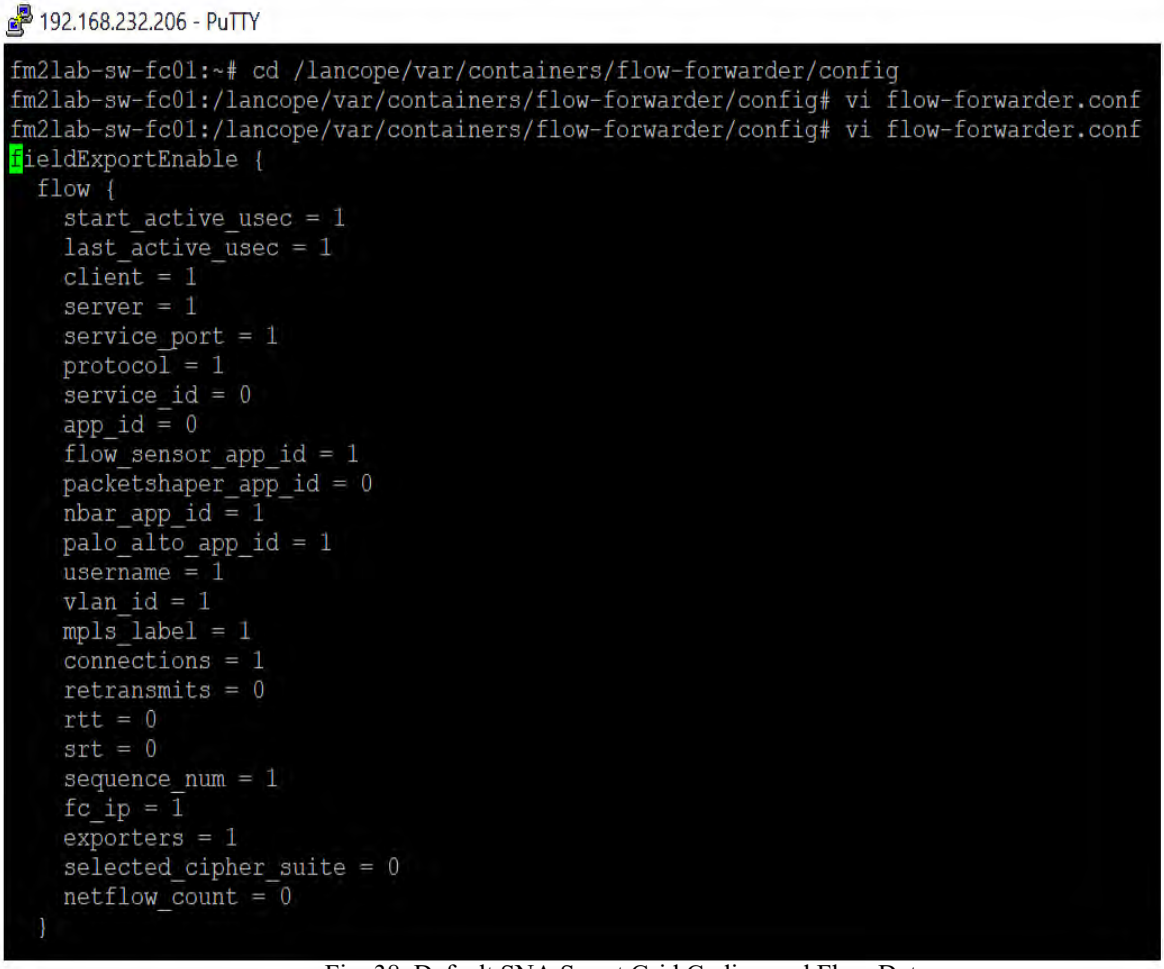


Fig. 38. Default SNA Smart Grid Coding and Flow Data.

```
  host {
    ip = 1
    port = 1
    port_max = 0
    xlate_ip = 1
    xlate_port = 1
    mac = 1
    asn = 1
    payload = 0
    payload_ex = 1
    group_list = 1
    num_bytes = 1
    num_packets = 1
    syn_packets = 0
    syn_ack_packets = 0
    rst_packets = 0
    fin_packets = 0
    sgt_id = 0
    sgt_name = 0
    total_bytes = 1
    total_packets = 1
    process_name = 0
    process_hash = 0
    process_username = 0
    parent_process_name = 0
    parent_process_hash = 0
    parent_process_username = 0
    idp = 1
    byte_distribution = 1
    tls_version = 1
    tls_session_id = 1
    payload_binary = 1
    payload_ex_binary = 1
    sequence_packet_lengths_times = 1
  }
}
```

Fig. 39. Default SNA Smart Grid Coding and Flow Data-cont.

The implementation's optimized/modified codes are listed below. It demonstrates that, in the absence of a DDOS assault, the flow rate's baseline volume was set at 15,000.

The parts that are highlighted in green are the altered codes that were added to the standard Scada-type code to fit the research.

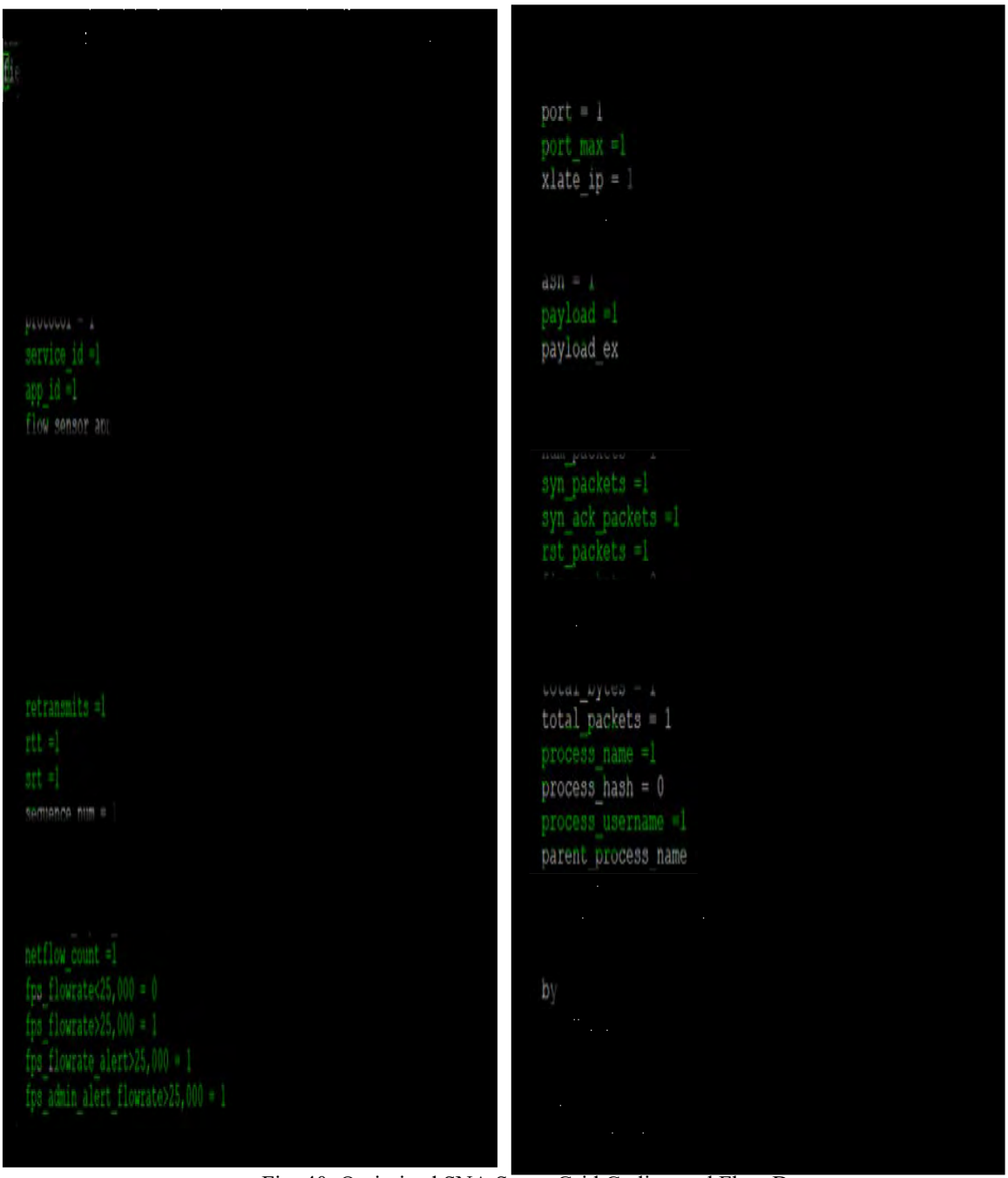


Fig. 40. Optimized SNA Smart Grid Coding and Flow Data.

```
host {
  ip = 1
  port = 1
  port_max =1
  xlate_ip = 1
  xlate_port = 1
  mac = 1
  asn = 1
  payload =1
  payload_ex = 1
  group_list = 1
  num_bytes = 1
  num_packets = 1
  syn_packets =1
  syn_ack_packets =1
  rst_packets =1
  fin_packets = 0
  sgt_id = 0
  sgt_name = 0
  total_bytes = 1
  total_packets = 1
  process_name =1
  process_hash = 0
  process_username =1
  parent_process_name = 0
  parent_process_hash = 0
  parent_process_username = 0
  idp = 1
  byte_distribution = 1
  tls_version = 1
  tls_session_id = 1
  payload_binary = 1
  payload_ex_binary = 1
  sequence_packet_lengths_times   1
 }
}
```

Fig. 41. Optimized SNA Smart Grid Coding and Flow Data—cont.

Fig. 42. Optimized SNA Smart Grid Coding and Flow Data—cont.

4.16 Flowchart, Security Event, and Secure Network Analytics Smart Grid Firewall-IPS Rules

In the course of this study, the firewall rule used with Forcepoint's next-generation firewall is shown in Fig. 43 below. The access permitted between the attack system or source client and the target server or destination server is shown by the firewall rule. At the bottom of the firewall rule, the default denial rule was configured for the best practice.

ID	Source	Destination	Service	Action	Logging	Rule Name	Comment
Secure Network Analytics-Smart-Grid-LAB-Rules							
2179	h_192.168.232.209	host_192.168.23	ANY	Allow	Stored Connection Closing: No Log	@2227354.7	Secure Network Analytics-Smart-Grid-Rules
2180	host_192.168.233.214	h_192.168.232.2	ANY	Allow	Stored Connection Closing: No Log	@2227355.7	Secure Network Analytics-Smart-Grid-Rules
2181	FM_LAB_192.168.232.0_24	FM_LAB_192.16	ANY	Allow	Stored Connection Closing: No Log	@2227352.7	Secure Network Analytics-Smart-Grid-Rules
2182	FM_LAB_192.168.233.0_24	FM_LAB_192.16	ANY	Allow	Stored Connection Closing: No Log	@2228379.4	Secure Network Analytics-Smart-Grid-Rules
2183	ANY	FM_LAB_192.16 FM_LAB_192.16	ANY	Discard	Stored Connection Closing: No Log	@2228378.5	Secure Network Analytics-Smart-Grid-Rules

Fig. 43. SNA Smart Grid Firewall Rules Proposed.

The intrusion Detection/Prevention System (IDS/IPS) rules that were put into place throughout this study to safeguard and secure the complete Smart Grid system use case are shown in Fig. 44.

Fig. 44. SNA Smart Grid IDS/IPS Rules Proposed.

Furthermore, the SNA's security events settings, which are displayed in Fig. 45, notified the administrator of any abnormality or departure from the security baseline so

that prompt action or mitigation could be taken. This aided in identifying any irregularities in the grid before an attacker shut it down.

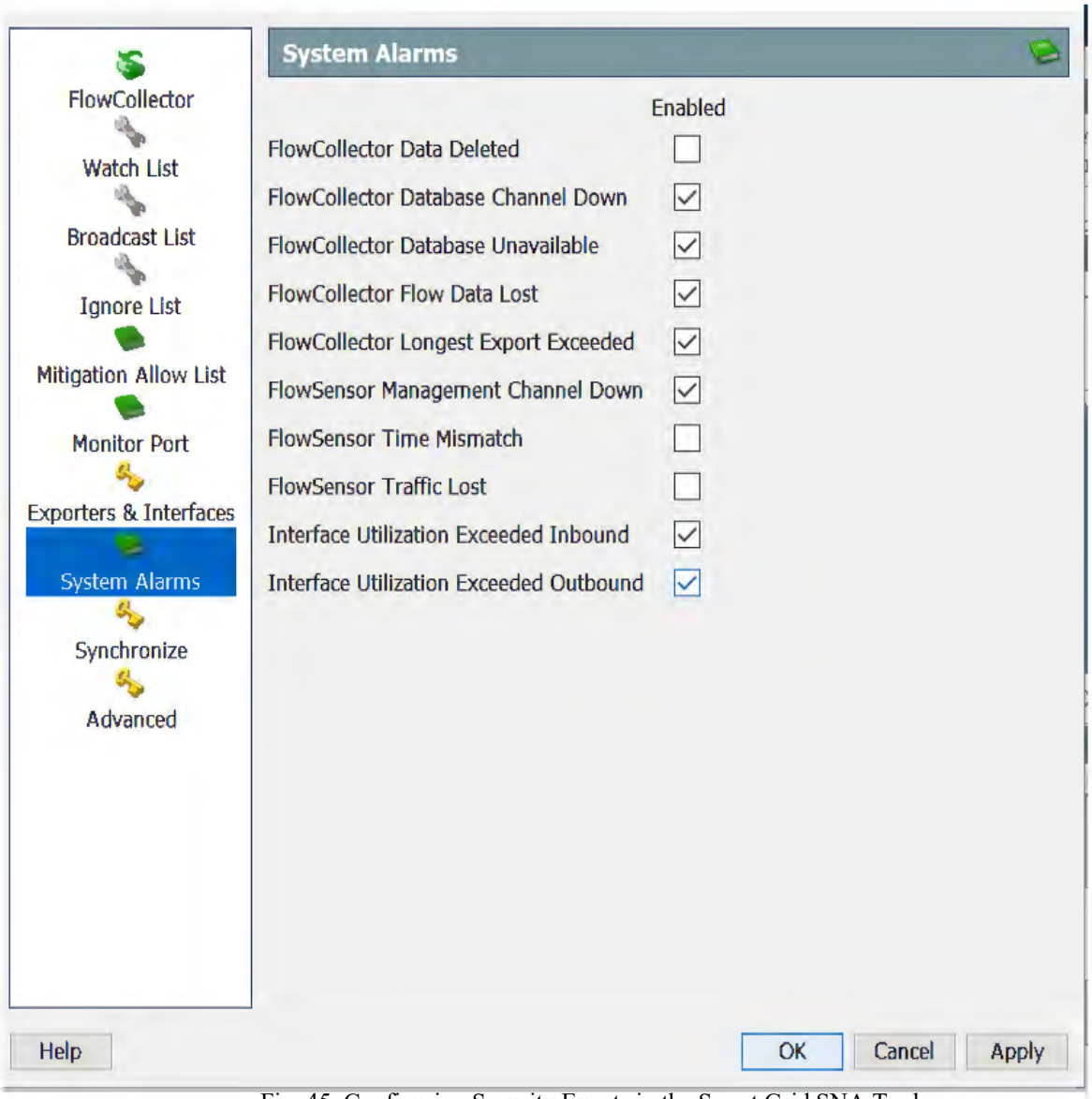


Fig. 45. Configuring Security Events in the Smart Grid SNA Tool

The SNA appliance manager dashboard, displayed in Fig. 46, displays the operational and upstate conditions of the tools following their construction and mapping.

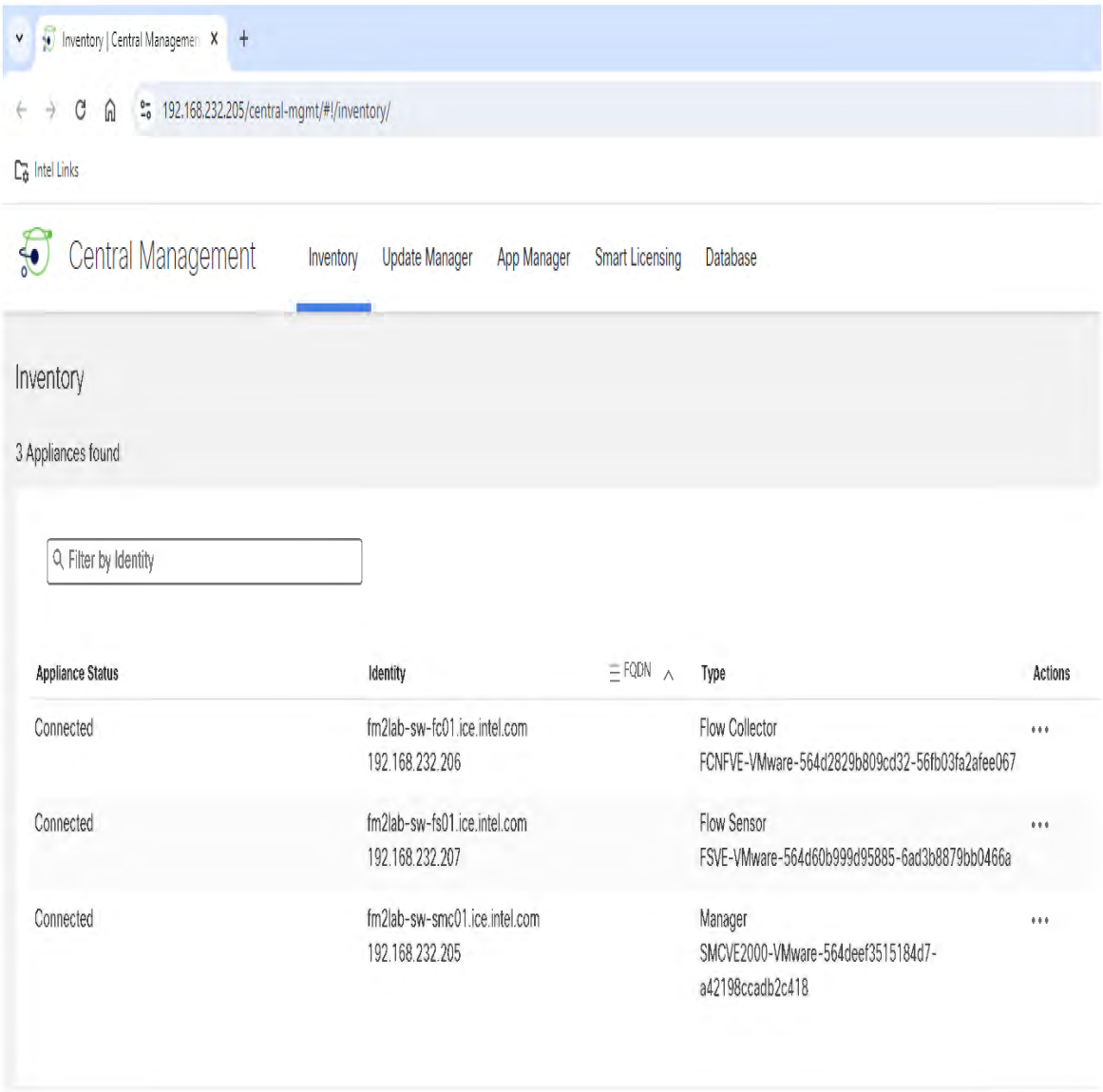


Fig. 46. Dashboard for the Smart Grid SNA appliance management.

Fig. 47 displays the updated flowchart of the SNA-based cyberattack algorithm. It describes how SNA uses the threshold volume level to identify network problems and produce alerts.

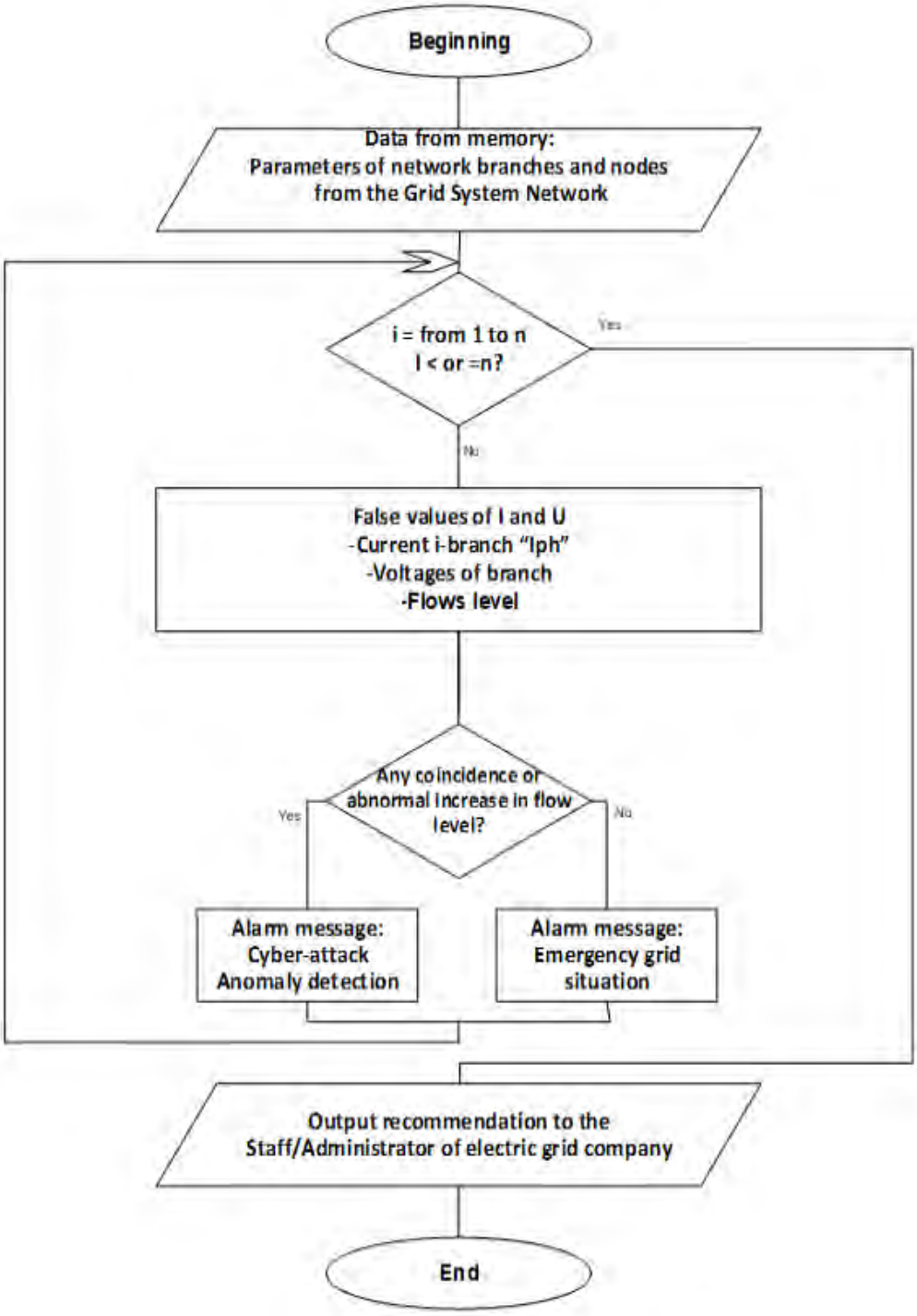


Fig. 47. Proposed block diagram for the SNA-based SG cyberattack methodology.

5. RESULTS

This section's primary goal is to demonstrate the effects of a DDoS attack on the suggested Smart Grid distribution network and how the Secure Network Analytics (SNA) tools and device can identify, capture, and mitigate the attack before it totally shuts down the grid. The SNA central management console was used to record the data packets that were transferred from Host1 to Host2. Fig. 50 demonstrates how the Smart Grid SNA computer network facilitated communication between source node-host 1 (Attacker) and destination node-host 2 (Target Server). The picture also demonstrates how the ICMP/ping protocol allowed the attacker server (host 1), which had IP address 192.168.232.209, to contact host 2, which had IP address 192.168.232.214, and vice versa.

5.1 Simulations Prior to the Attack

The ping status between the attacker and target systems during the simulation phases is displayed in Fig. 48 and 49.

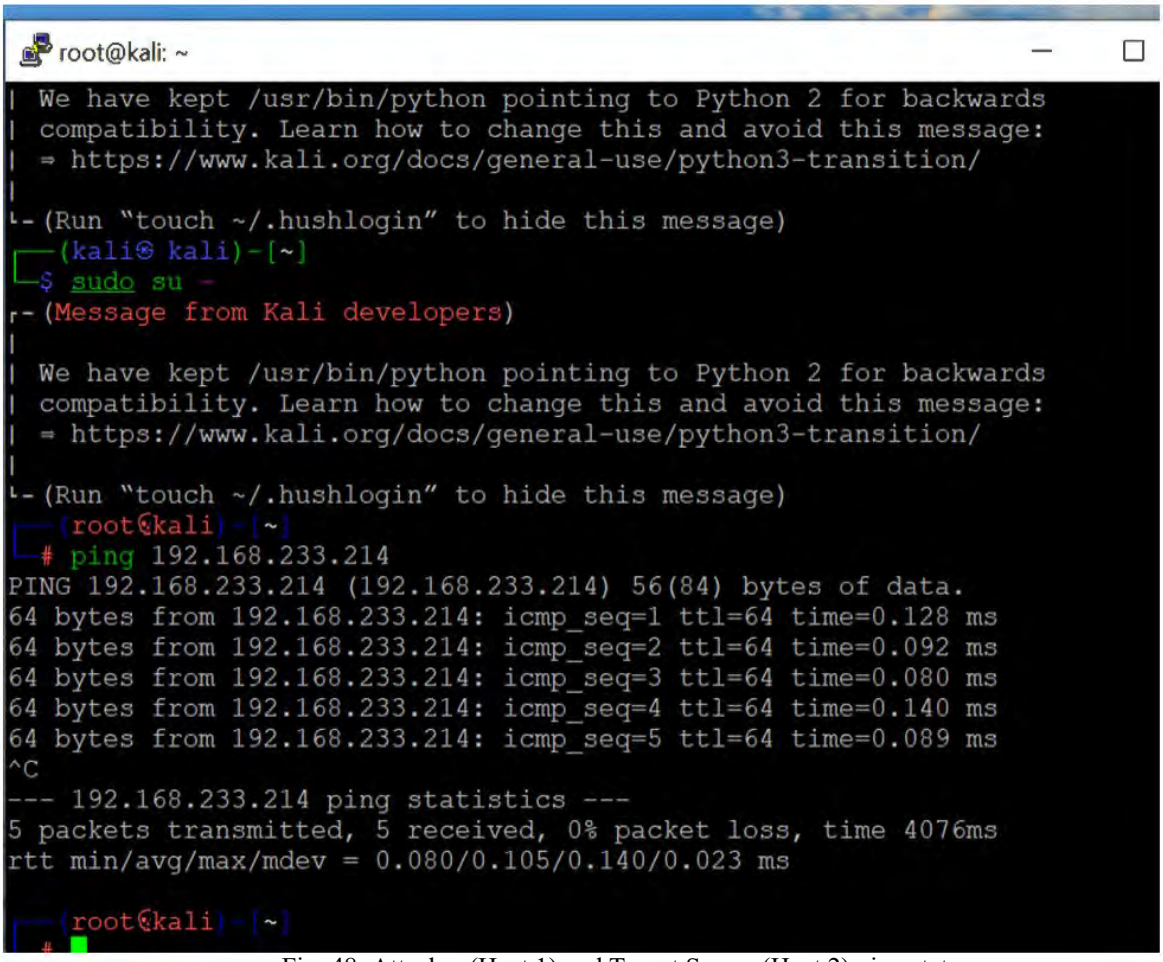


Fig. 48. Attacker (Host 1) and Target Server (Host 2) ping status.

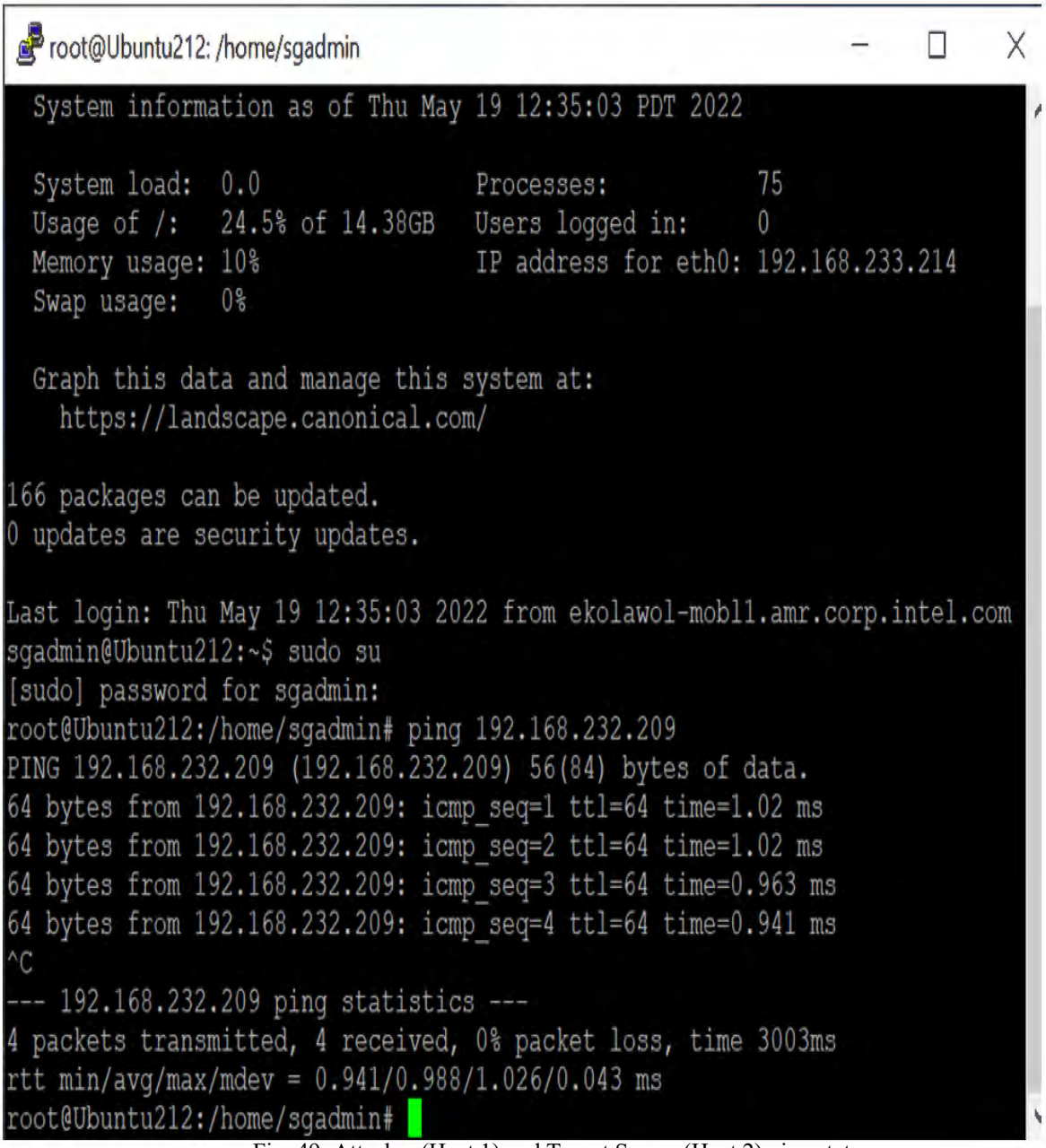


Fig. 49. Attacker (Host 1) and Target Server (Host 2) ping status.

The SNA Analytic tool may successfully record the communication between the attacker and the target devices, as demonstrated in Fig. 50 below. We determined the communication state based on the source and destination's echo requests and replies.

Fig. 50. Ping status btw Attacker (Host 1) and Target Server (Host 2) using SNA.

Fig. 51. displays Host 2's flow operations in normal circumstances, free from anomalous threats or DDoS attacks. At an average flow rate (fps), we could observed that the SNA tool recorded the traffic moving through the grid-modeled system every baseline at about 13.87k. This was the flow rate on Host 2 during regular operations, when there was not a DDOS attack of any kind. The flow rate should rise above the baseline established by the code and algorithms once Host 1 and the attack system DDOS Host 2 completed the attack phase of this study. Then, before the target server, which in the Grid system modeling represented a host, shuts down or becomes infected, SNA should be able to produce an alarm and turn off the grid. The ability of the Smart Grid SNA device or tool to efficiently identify and counteract DDoS attacks in Smart Grid systems was confirmed.

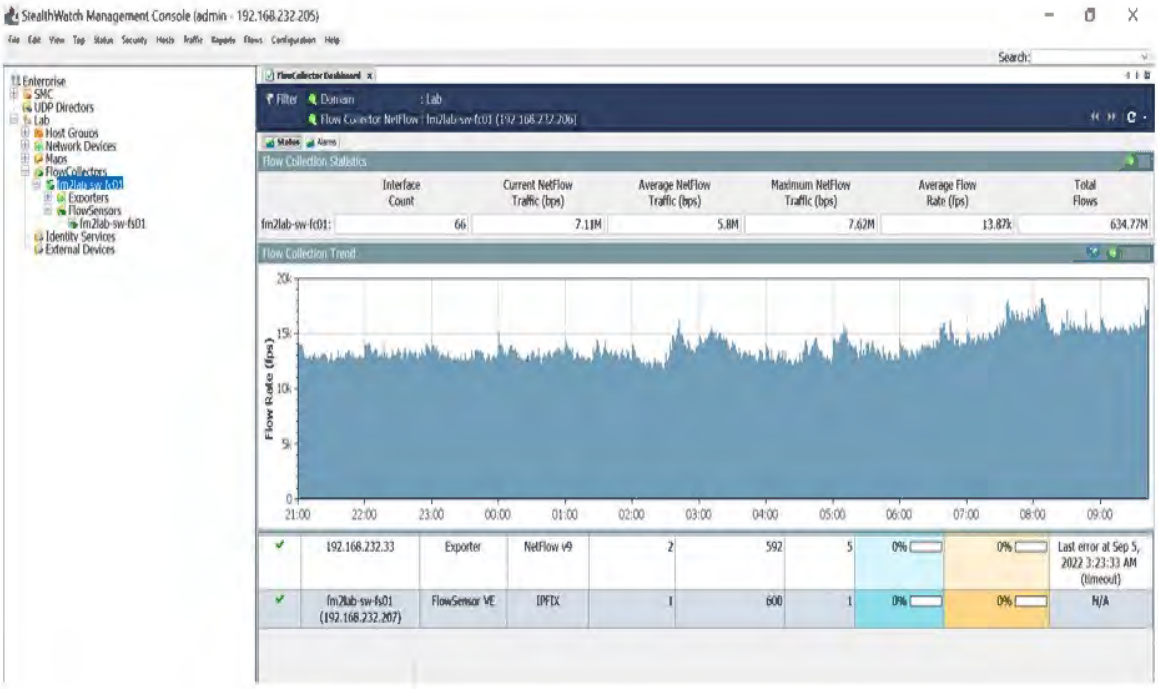


Fig. 51. Prior to the DDoS attack, Host 1 provided the recorded PMU data.

5.2 During the Attack, Simulations

Fig. 52, 53 and 54 shows the simulation results during the attack are described here. As demonstrated, it showed the ingestion of malicious software for DDOS assaults in the source client or attack system as excessive port scans of more than 600 sockets and pings. This will overload the target or destination server and cause it to shut down. The Tcpdump simulation results, which illustrated how the traffic was reaching the destination server for each payload transmitted from the attack system, are also shown in the Fig. According to TCPdump, the Attacker [Source Server-192.168.232.209] is continuously bombarding the Target [Destination Server-192.168.233.214] with ping/port scans in an attempt to overwhelm and take it down. DDoS attacks were also handled by the hping3 program, and the longer the attack lasted, the longer the target device's ping response time increased. As seen in Fig. 53, the ping response time was 2881 ms after the DDoS attack ended. However, because of the mitigation technologies in place, the Target server was not

taken down. The Tcpdump simulation results, which show how the traffic was reaching its destination per payload transmitted from the attack system, are also shown in the Fig.

Fig. 52. Simulations of SNA during the attack.

Run a tcpdump on the Target Server [destination] to see the flows

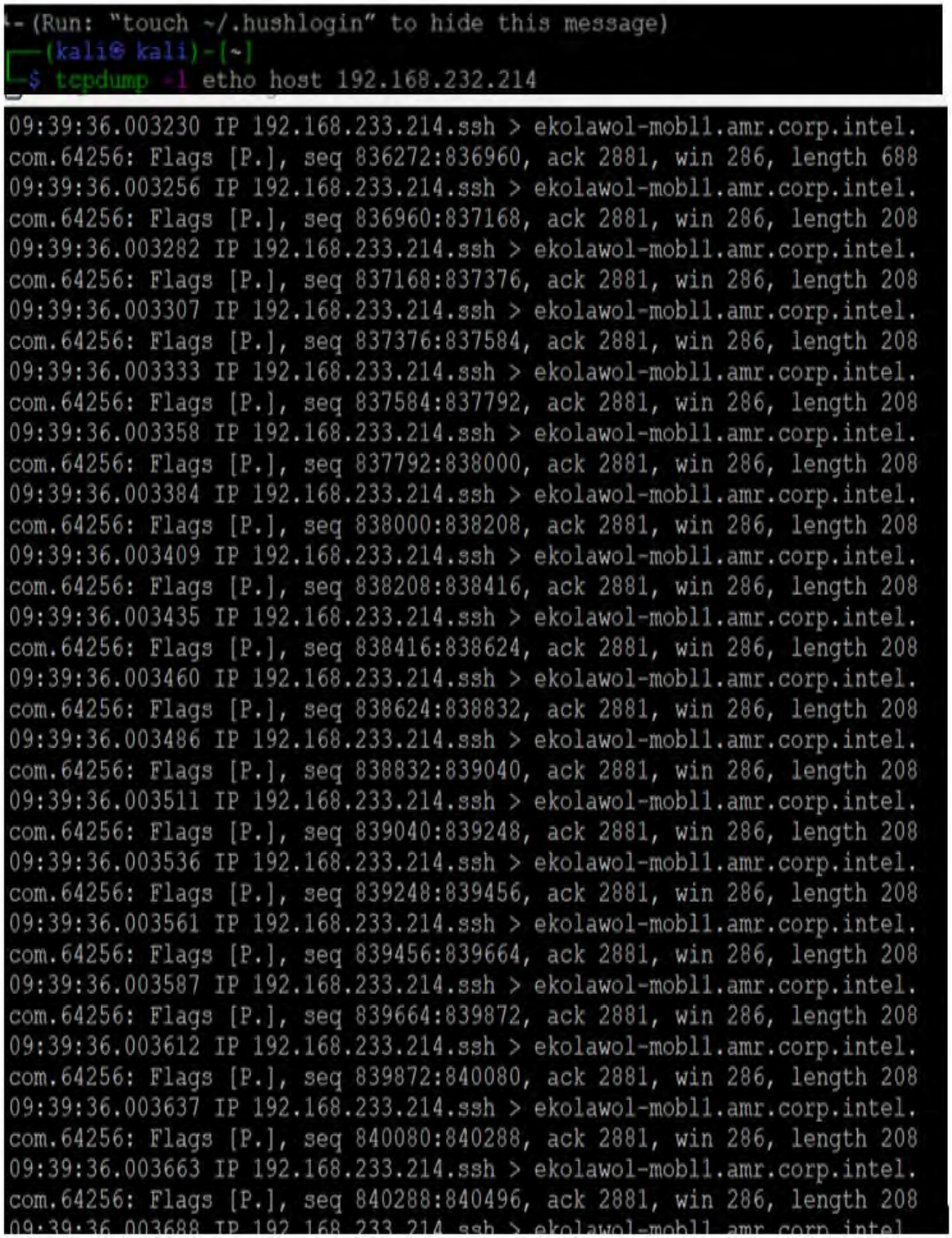


Fig. 53. Simulations of SNA during the attack.

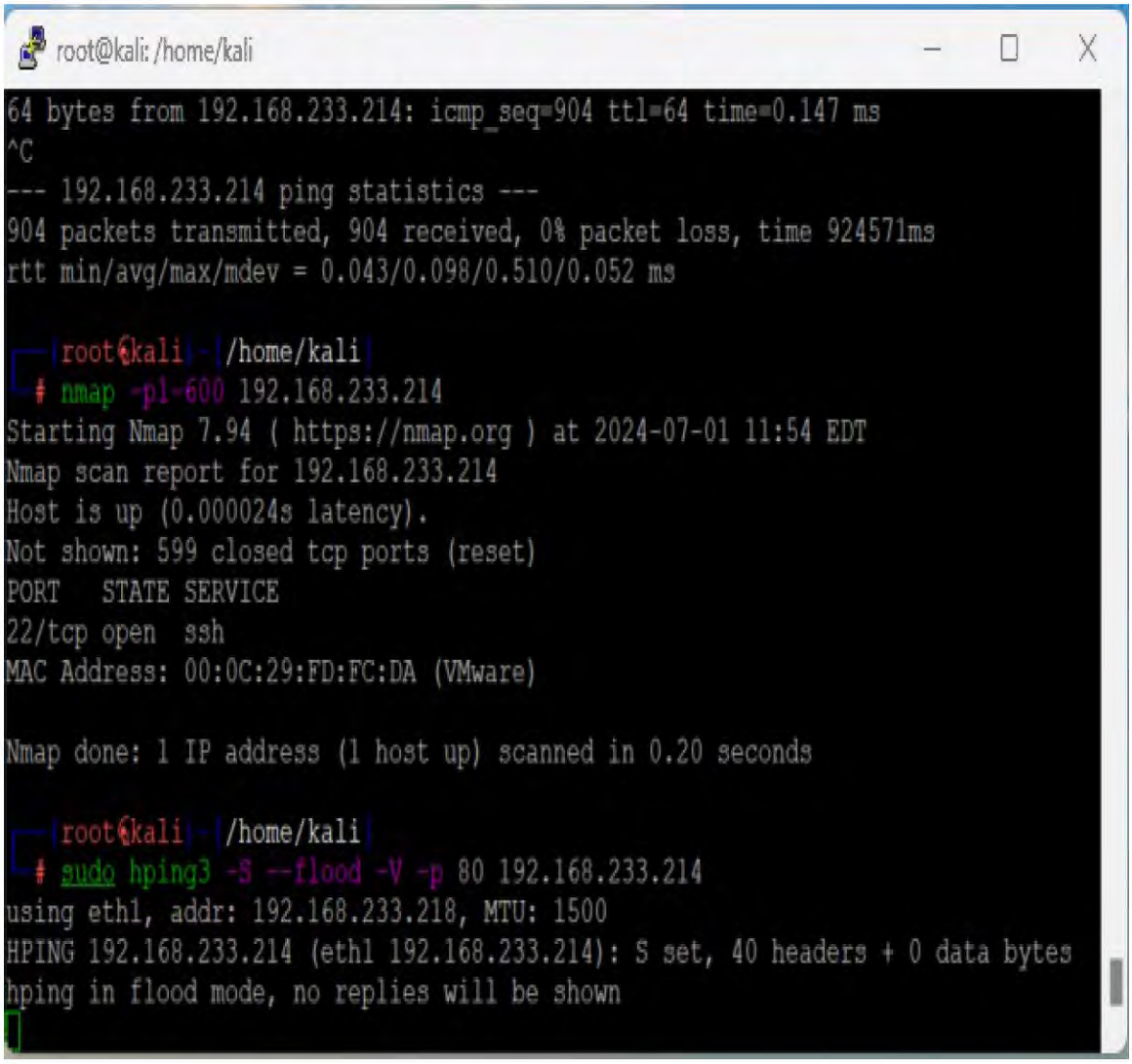


Fig. 54. Simulations of SNA during the attack.

5.3 Simulations Following the Attack

The effects and results of the attack that were initiated by the attack client or source system on the attack system or destination server are displayed in Figs. 55 to 66 below. Based on the amount of traffic, the ports used, and the frequency with which the attacker attempted to compromise the target or destination server, the SNA tool was able to identify and detect the attack.

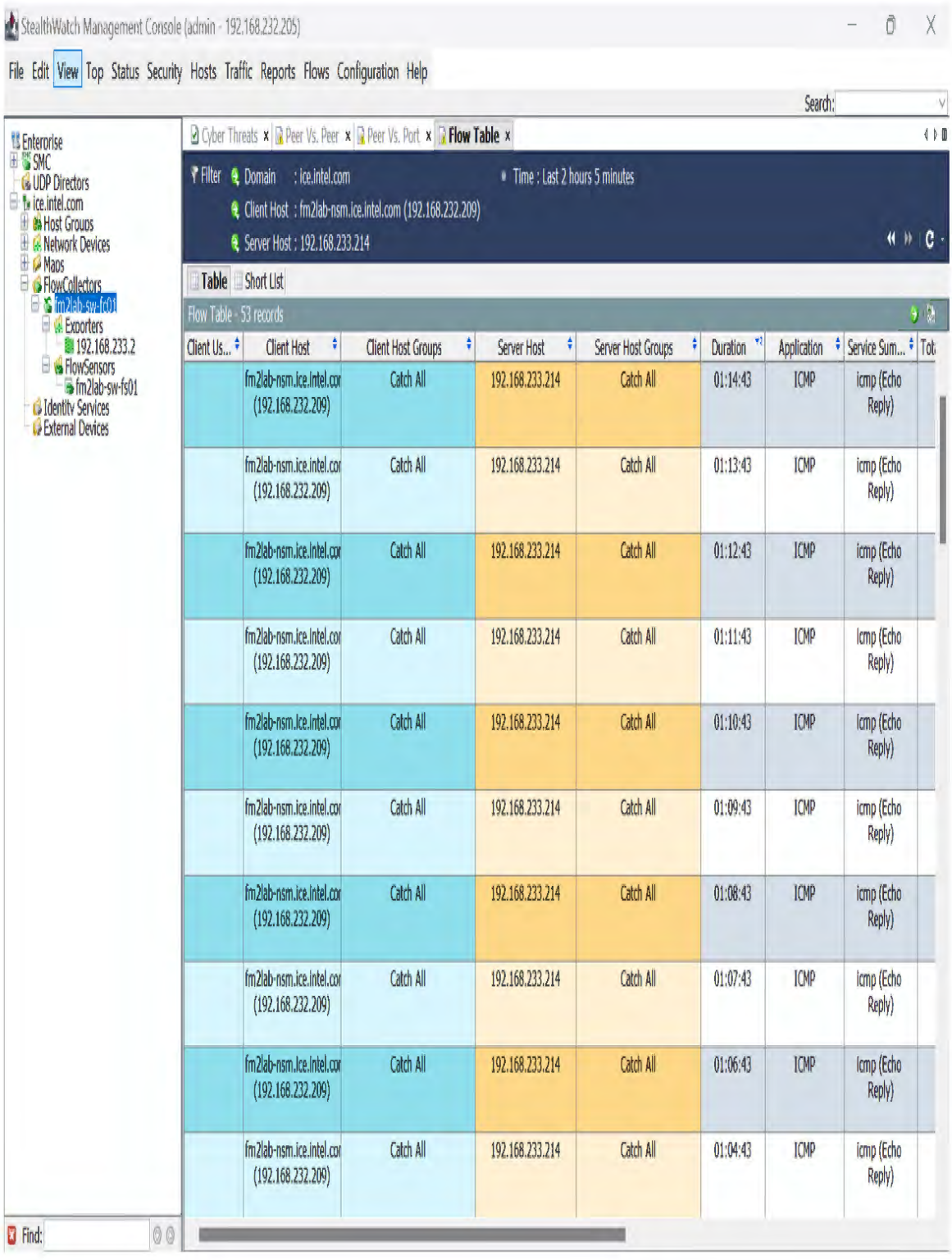


Fig. 55. SNA Simulations Following the Attack.

Fig. 56. SNA Simulations Following the Attack.

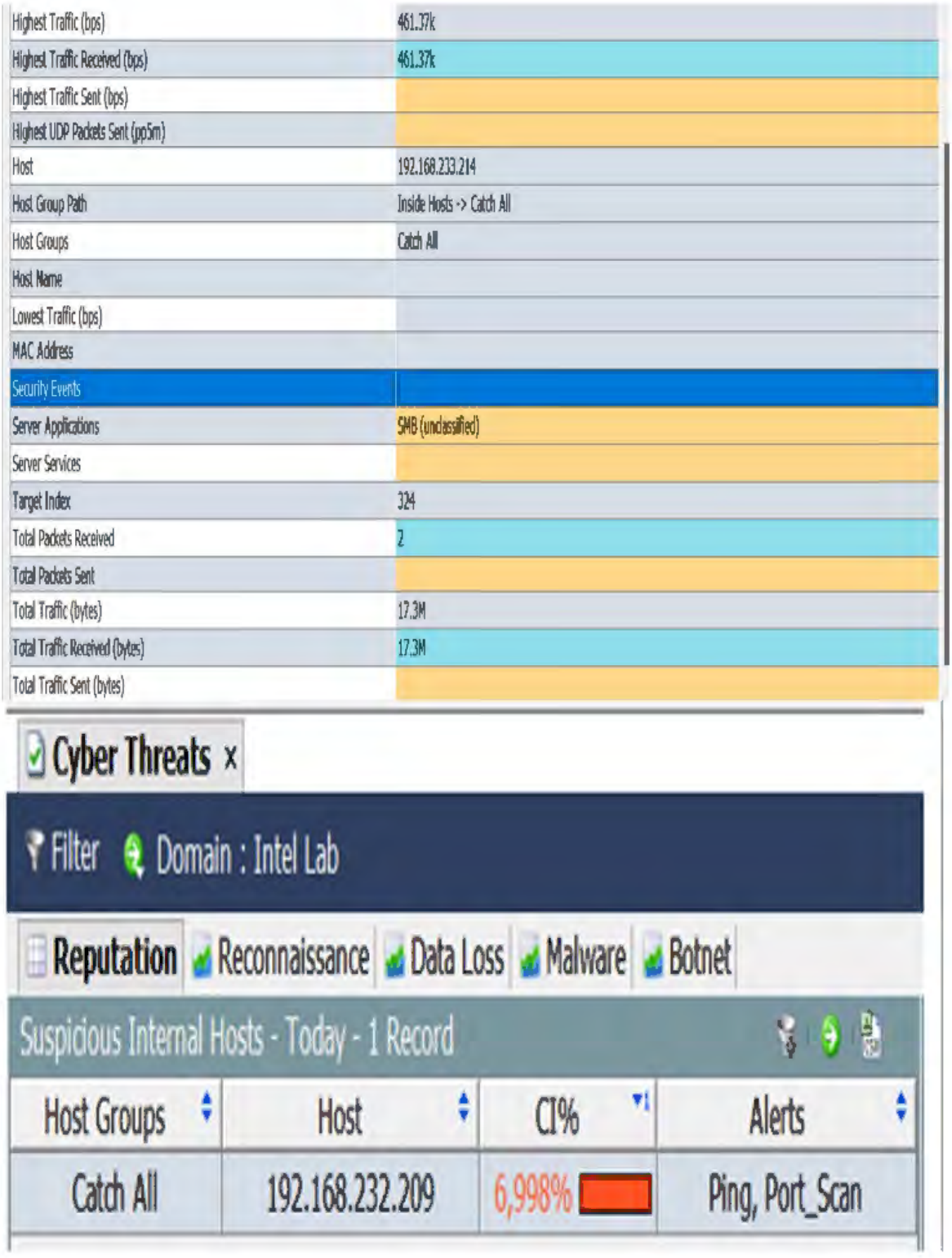


Fig. 57. SNA Simulations Following the Attack.

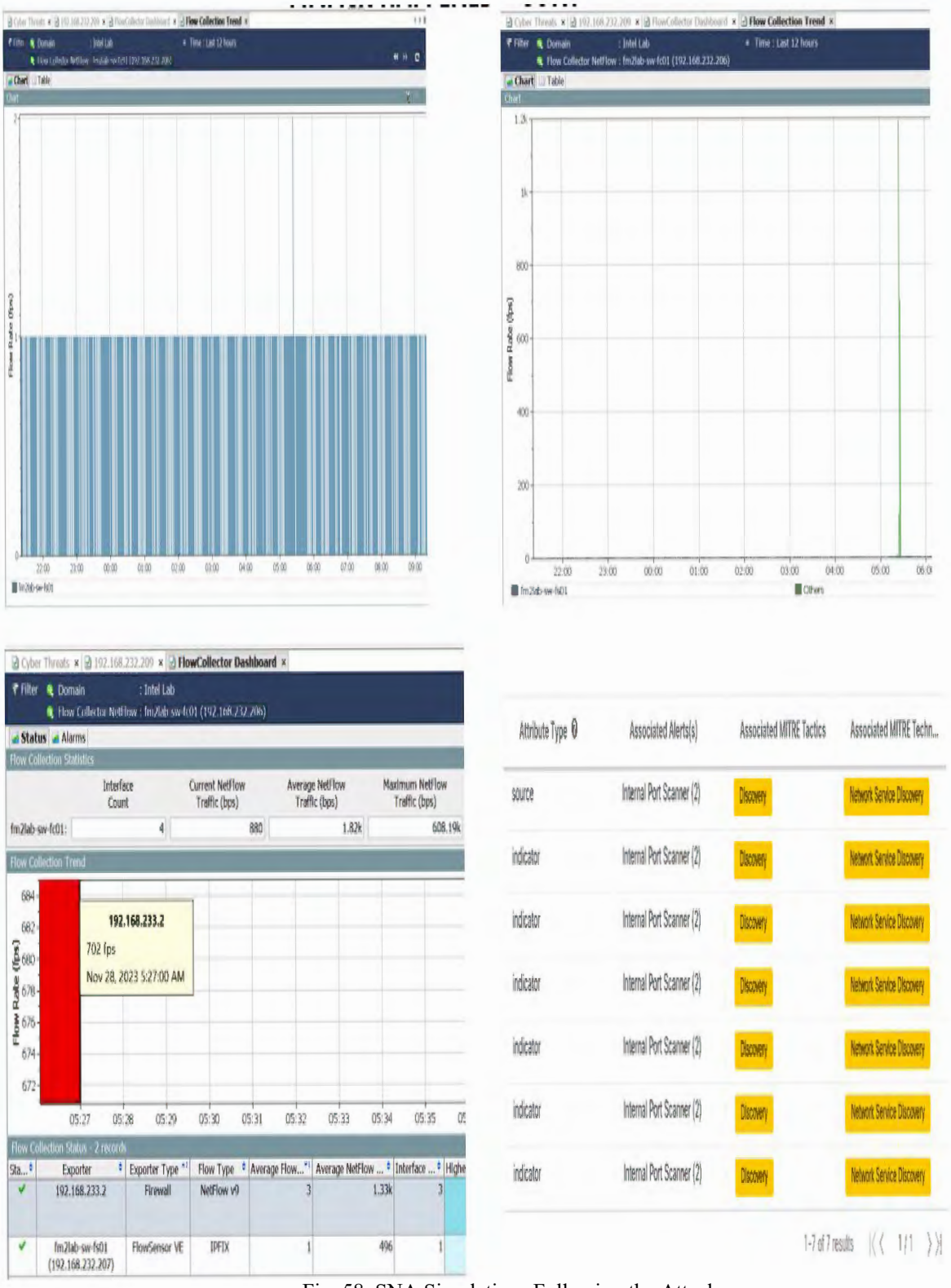


Fig. 58. SNA Simulations Following the Attack.

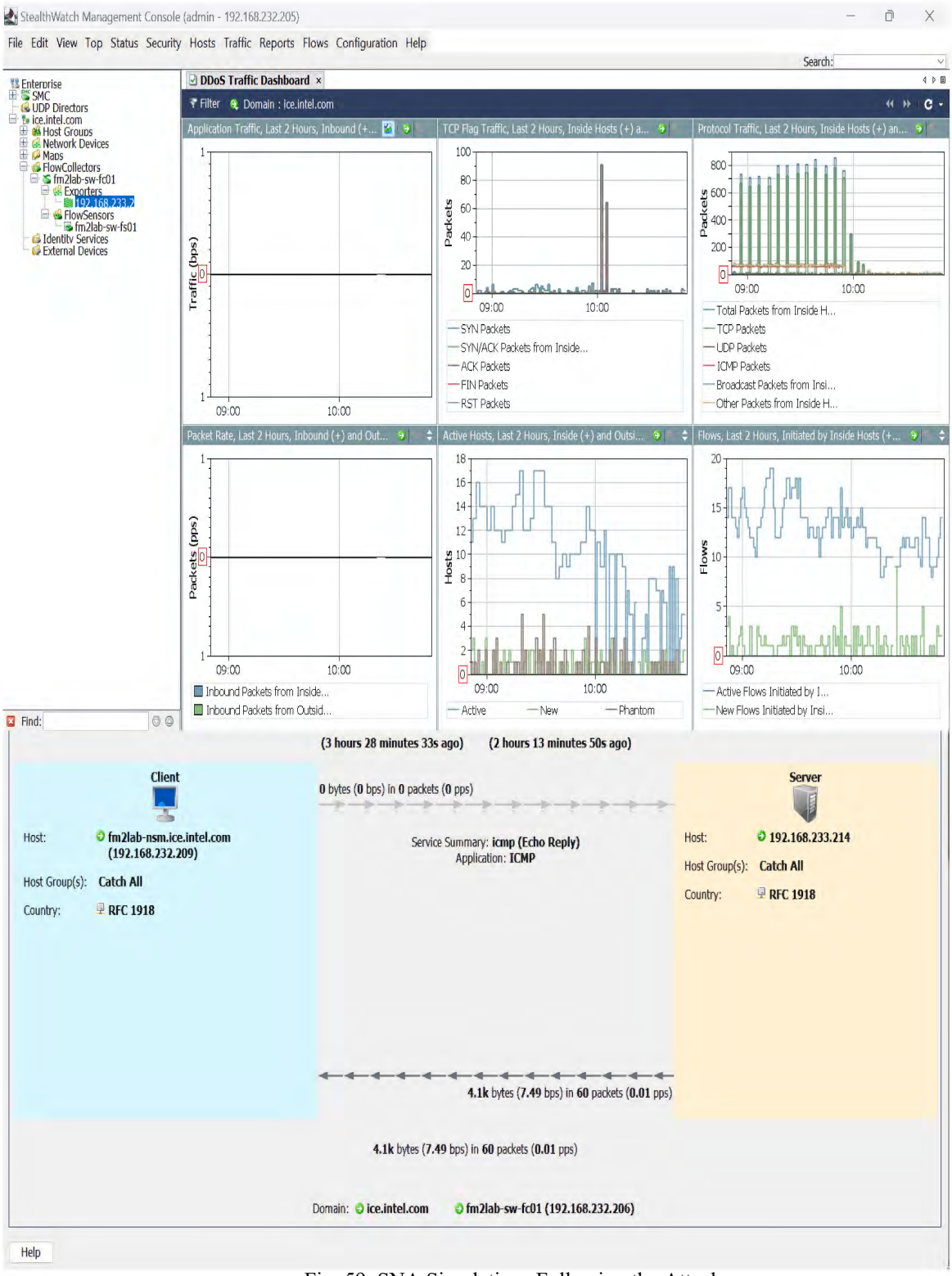


Fig. 59. SNA Simulations Following the Attack.

From: stealthwatch_alert@intel.com <stealthwatch_alert@intel.com>
Sent: Tuesday, November 28, 2023, 11:53 PM
To: Kolawole, Emmanuel <emmanuel.kolawole@intel.com>;
Subject: StealthWatch system alarms

SMC healthcheck system alarms
Status: ACTIVE
Time: 2023-11-29T07:53:14 (UTC)
ID: 6R-LMKA-9SKM

Condition:
Type: Flow Collector Management Channel Degraded
Severity: Major
Description:
Details: Unable to connect. Timeout waiting for connection. (Connect to 192.168.233.214 timed out)

Managed Device:
Name: h_192.168.233.214
IP Address: 192.168.233.214
Type: Linux Server

Fig. 60. SNA Simulations Following the Attack.

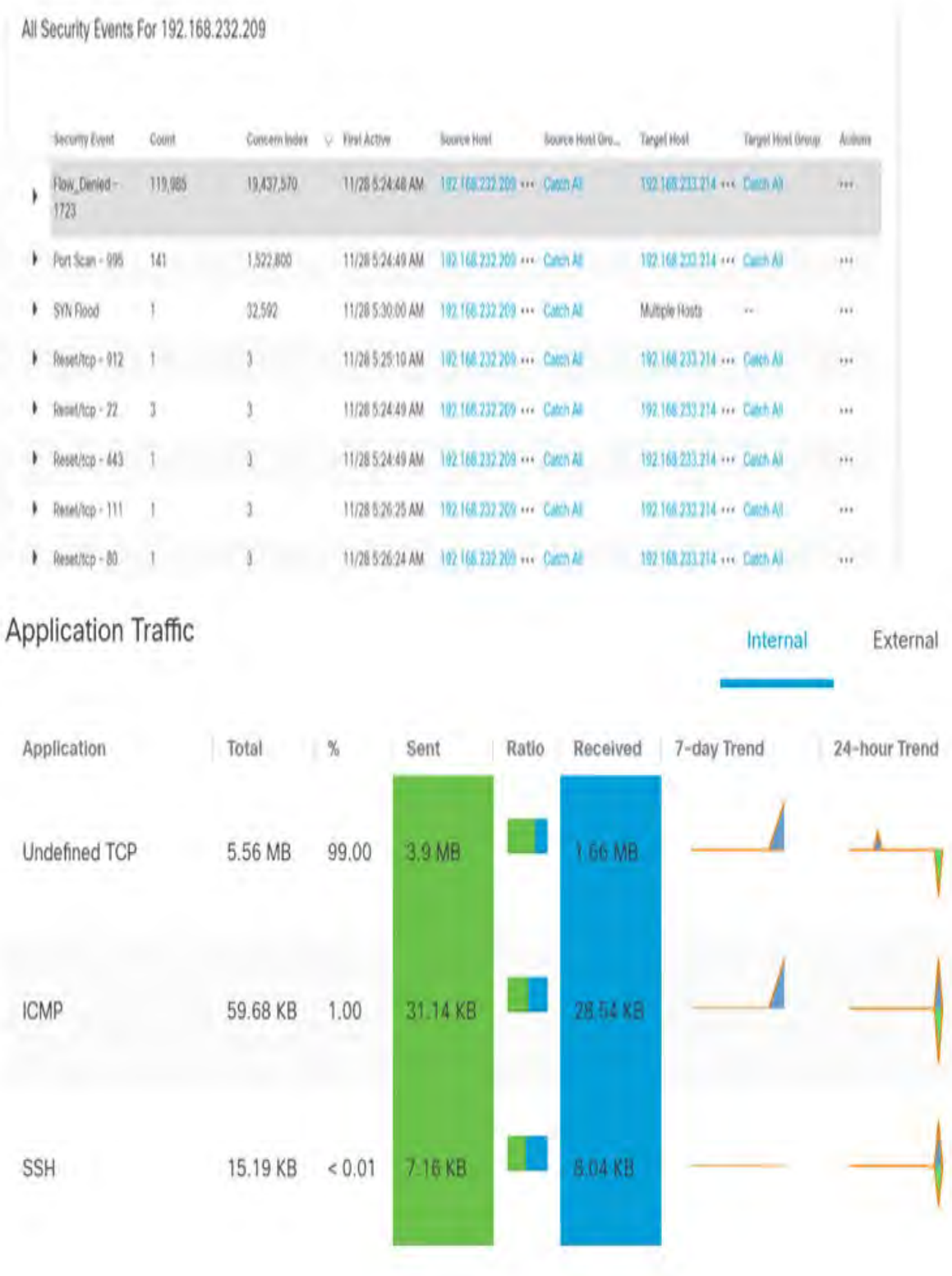


Fig. 61. SNA Simulations Following the Attack.

Fig. 62. SNA Simulations Following the Attack.

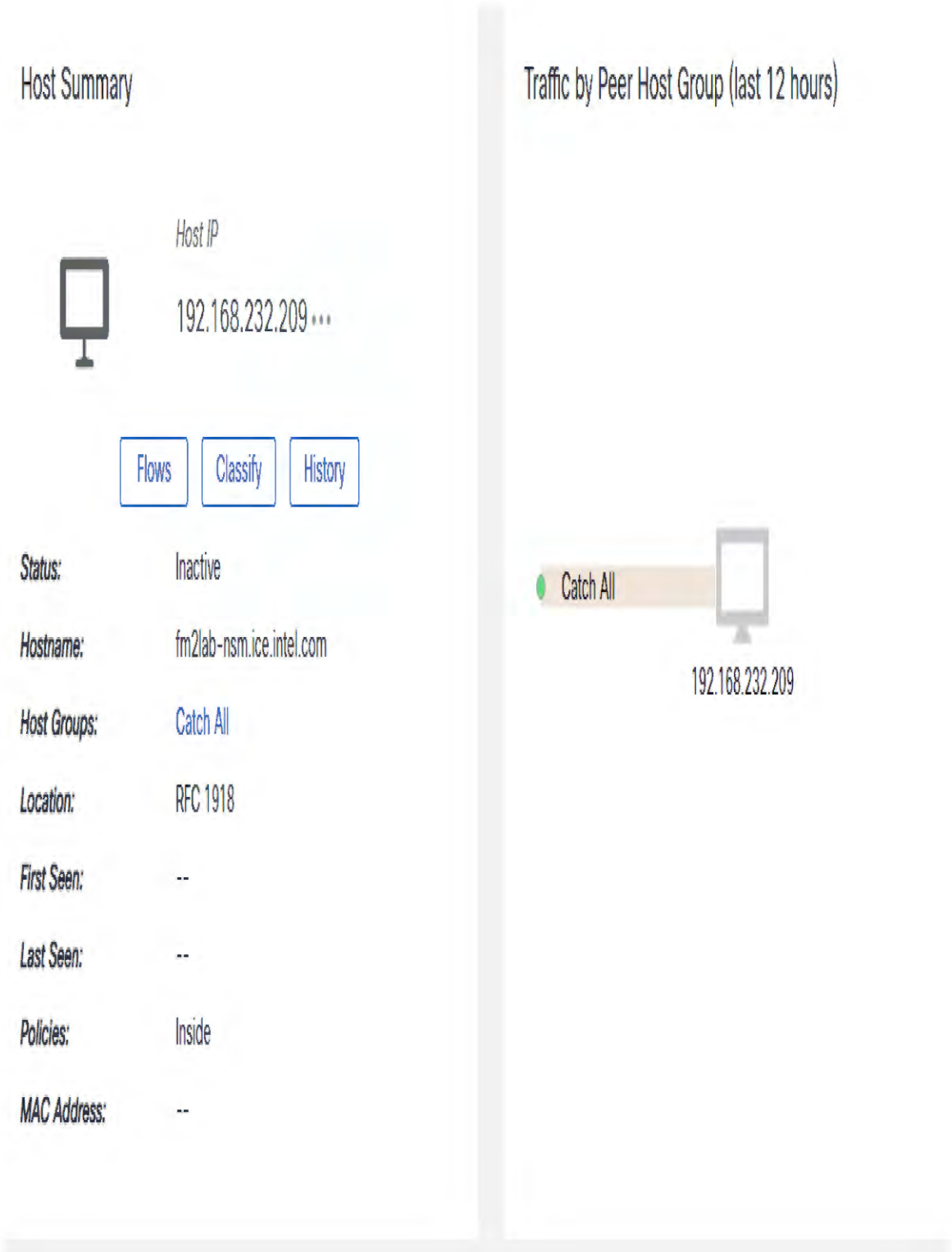


Fig. 63. SNA Simulations Following the Attack.

Duration	Subject IP Address	Subject Port/Pr...	Subject Host G...	Subject Bytes	Application	Total Bytes	Peer IP Address	Peer Port/Prot...	Peer Host Grou...	Peer Bytes	A
Ex. <=50min4	Ex. 10.10.10.10	Ex. 57100/UD	Ex. "catch All"	Ex. <=50M	Ex. "Corporat	Ex. <=50M	Ex. 10.255.255.2	Ex. 2055/UDF	Ex. "Catch All	Ex. <=50M	
1hr 9min 43s	192.168.232.209 •••	ICMP	Catch All	--	ICMP	4.1 K	192.168.233.214 •••	ICMP	Catch All	4.1 K	••
1hr 10min 43s	192.168.232.209 •••	ICMP	Catch All	--	ICMP	4.1 K	192.168.233.214 •••	ICMP	Catch All	4.1 K	••
1hr 11min 43s	192.168.232.209 •••	ICMP	Catch All	--	ICMP	4.1 K	192.168.233.214 •••	ICMP	Catch All	4.1 K	••
1hr 12min 43s	192.168.232.209 •••	ICMP	Catch All	--	ICMP	4.1 K	192.168.233.214 •••	ICMP	Catch All	4.1 K	••
1hr 13min 43s	192.168.232.209 •••	ICMP	Catch All	--	ICMP	4.1 K	192.168.233.214 •••	ICMP	Catch All	4.1 K	••
1hr 14min 43s	192.168.232.209 •••	ICMP	Catch All	--	ICMP	4.1 K	192.168.233.214 •••	ICMP	Catch All	4.1 K	••
1hr 15min 43s	192.168.232.209 •••	ICMP	Catch All	--	ICMP	2.71 K	192.168.233.214 •••	ICMP	Catch All	2.71 K	••

Fig. 64. SNA Simulations Following the Attack.

Fig. 65. SNA Simulations Following the Attack.

Fig. 66. SNA Simulations Following the Attack.

The input and output flow logs are compared in Fig. 67 to demonstrate the DDOS effect and how the tool was able to mitigate the attack before it shut down the destination server. As soon as the flowrate ratio exceeded 15 fps that had been designed per baseline defined, the system generated alerts to notify the administrator as a sign of a suspected attack. However, it had already mitigated the flow increase based on the baseline setup, Firewall rules, and the IPS policy setup.

```
fm2lab-sw-fc01:~# grep "S-per-t" /lancope/var/sw/28/logs/sw.log | grep "output flow stats"
05:20:00 S-per-t:      Input flows 1979 fps, output flow stats 134 fps, flow ratio 14.67 this period
05:25:00 S-per-t:      Input flows 2159 fps, output flow stats 131 fps, flow ratio 16.41 this period
05:30:00 S-per-t:      Input flows 2089 fps, output flow stats 130 fps, flow ratio 15.98 this period
05:35:00 S-per-t:      Input flows 1968 fps, output flow stats 132 fps, flow ratio 14.84 this period
05:40:00 S-per-t:      Input flows 1887 fps, output flow stats 132 fps, flow ratio 14.30 this period
05:45:00 S-per-t:      Input flows 2145 fps, output flow stats 134 fps, flow ratio 15.99 this period
05:50:00 S-per-t:      Input flows 2155 fps, output flow stats 136 fps, flow ratio 15.79 this period
05:55:00 S-per-t:      Input flows 2090 fps, output flow stats 129 fps, flow ratio 16.13 this period
06:00:00 S-per-t:      Input flows 1897 fps, output flow stats 132 fps, flow ratio 14.29 this period
06:05:00 S-per-t:      Input flows 1987 fps, output flow stats 131 fps, flow ratio 15.12 this period
06:10:00 S-per-t:      Input flows 2097 fps, output flow stats 131 fps, flow ratio 15.98 this period
06:15:00 S-per-t:      Input flows 2300 fps, output flow stats 135 fps, flow ratio 16.94 this period
06:20:00 S-per-t:      Input flows 2053 fps, output flow stats 134 fps, flow ratio 15.23 this period
06:25:00 S-per-t:      Input flows 1955 fps, output flow stats 128 fps, flow ratio 15.24 this period
06:30:00 S-per-t:      Input flows 1837 fps, output flow stats 132 fps, flow ratio 13.83 this period
06:35:00 S-per-t:      Input flows 2041 fps, output flow stats 133 fps, flow ratio 15.30 this period
06:40:00 S-per-t:      Input flows 2009 fps, output flow stats 132 fps, flow ratio 15.12 this period
06:45:00 S-per-t:      Input flows 2060 fps, output flow stats 134 fps, flow ratio 15.28 this period
06:50:00 S-per-t:      Input flows 1938 fps, output flow stats 135 fps, flow ratio 14.31 this period
06:55:00 S-per-t:      Input flows 1951 fps, output flow stats 130 fps, flow ratio 14.90 this period
07:00:00 S-per-t:      Input flows 2093 fps, output flow stats 131 fps, flow ratio 15.88 this period
07:05:00 S-per-t:      Input flows 2116 fps, output flow stats 134 fps, flow ratio 15.70 this period
07:10:00 S-per-t:      Input flows 2003 fps, output flow stats 132 fps, flow ratio 15.10 this period
07:15:00 S-per-t:      Input flows 2166 fps, output flow stats 134 fps, flow ratio 16.07 this period
07:20:00 S-per-t:      Input flows 1965 fps, output flow stats 135 fps, flow ratio 14.54 this period
07:25:00 S-per-t:      Input flows 2149 fps, output flow stats 131 fps, flow ratio 16.37 this period
07:30:00 S-per-t:      Input flows 2139 fps, output flow stats 131 fps, flow ratio 16.23 this period
07:35:00 S-per-t:      Input flows 1940 fps, output flow stats 129 fps, flow ratio 14.93 this period
07:40:00 S-per-t:      Input flows 1937 fps, output flow stats 131 fps, flow ratio 14.71 this period
07:45:00 S-per-t:      Input flows 2230 fps, output flow stats 135 fps, flow ratio 16.41 this period
07:50:00 S-per-t:      Input flows 2131 fps, output flow stats 134 fps, flow ratio 15.83 this period
```

Fig. 67. Comparison of Flow Collector Input and Output Flow.

The simulation flow output on the SNA tool following the attack is displayed in Fig. 68. The traffic level somewhat rose but did not cause the destination server to shut down based on the baseline.

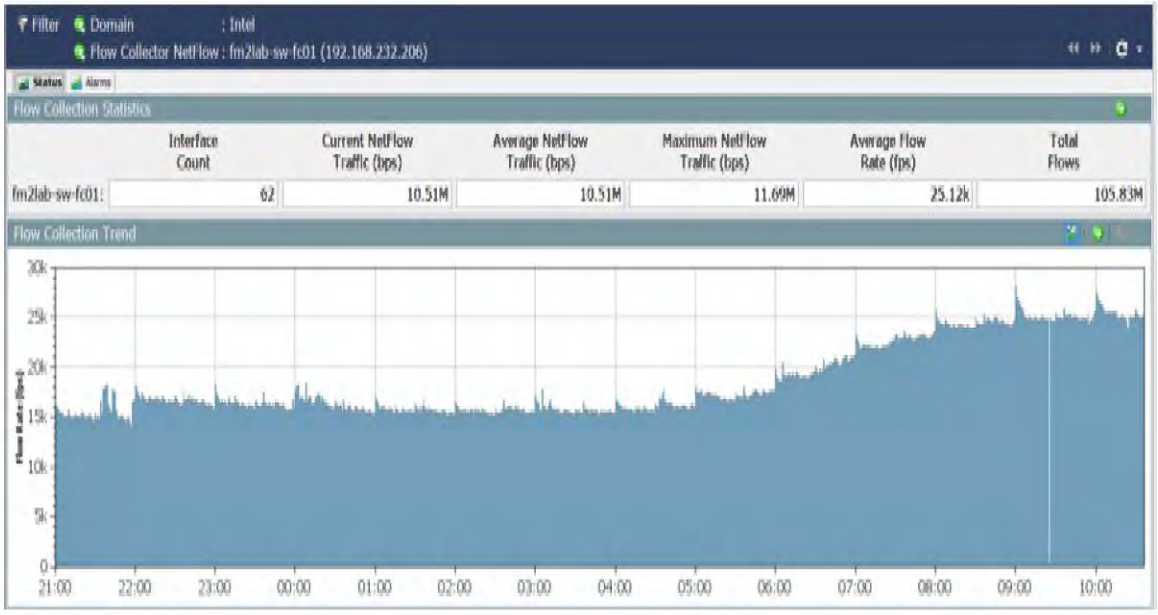


Fig. 68. SNA Simulations Following the Attack—cont.

5.4 Comparison of Output Results of DD0S Effect on Smart Grid Communication Networks using GNS3 and SNA Tools

In Fig. 23, using the GNS3 tool, we observed that the continuous flow of identical packets from the source client to the destination server resulted in the unavailability of services and the destination server's total shutdown in relation to the DDOS attack. In the meanwhile, in Fig. 68., we observed that even after the slight surge, as soon as the flowrate ratio appeared to be over 15 bytes, there were still traffic flows without any disruption or destination server shutdown, as illustrated in Fig. 68. This was established using the SNA tool as the baseline. As seen in Fig. 60, the spike caused the system to produce warnings

informing the administrator of any suspected intrusion or attack so that appropriate action can be taken. To prevent a false positive scenario, which could cause the Smart Grid to malfunction by obstructing real traffic or flows, the SNA will not totally shut down the purported IP address or hostname. However, as illustrated in Fig. 68, it has already reduced the flow growth based on the baseline configuration, Firewall rules, and the IPS signatures policy specified in Figs. 43 and 44., in addition to the notification that the administrator received regarding the increase in traffic or flow level. In order to prevent congestion that can result in a blackout, the destination or target server will then cease receiving flows from the suspected IP address or hostname. Following receipt of the alert, the administrator will conduct a comprehensive investigation to determine whether to fully block the suspicious network traffic.

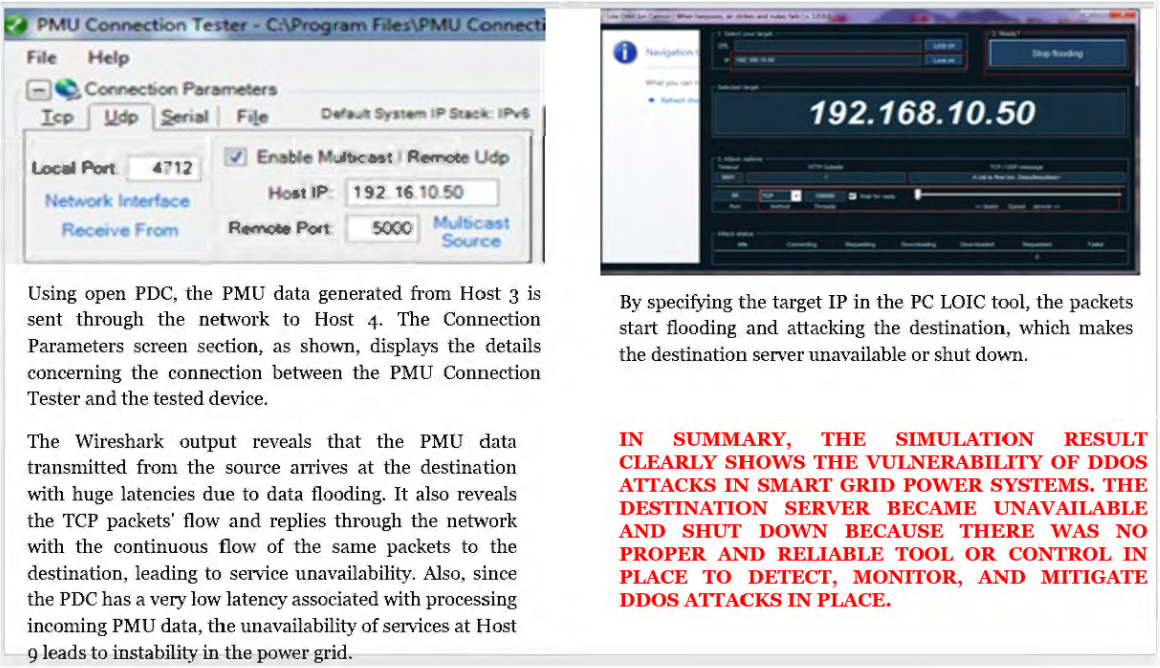


Fig. 23. Smart Grid Communication Network Simulations with GNS3 [66].

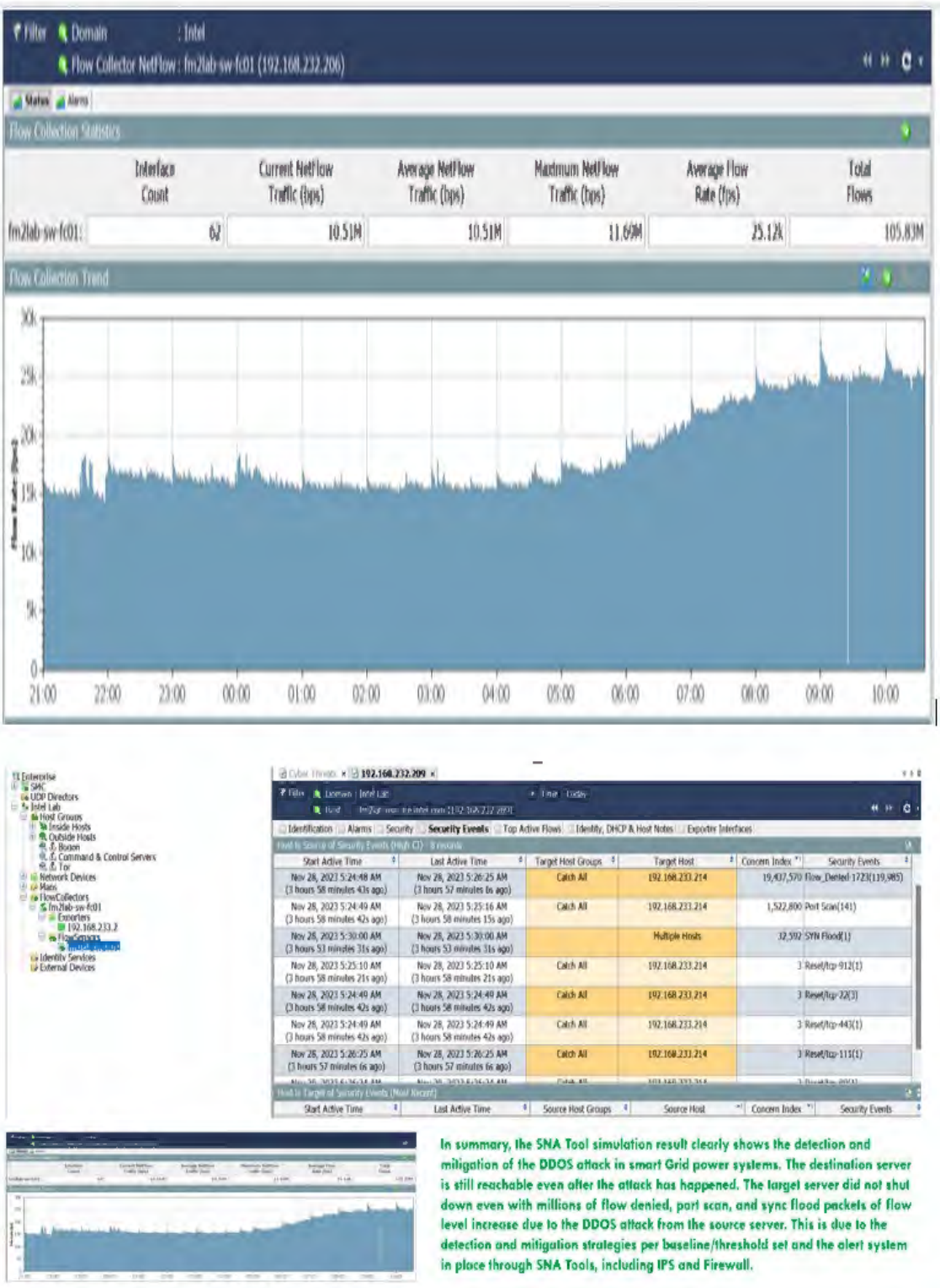


Fig. 68. Smart Grid Communication Network Simulations using SNA.

6. CONCLUSIONS

Recent security breaches and emerging cyberthreats have introduced new cybersecurity challenges for the Smart Grid communication networks, particularly with the integration of renewable energy sources. This is a highly concerning matter.

This study employed the co-simulation of GNS3 and a PMU connection tester to examine the impact of DDOS attacks on a Smart Grid WAMS communication network. The GNS tool simulation revealed the grid's system's vulnerability to a DDOS attack, resulting in its deactivation or shutdown. Subsequently, we proposed the deployment of firewalls intrusion detection and prevention systems to simulate with the SNA Tool for the identification, detection, and mitigation of DDOS attacks. The outcomes of this study demonstrated higher advancement and greater progress than those of previous researchers in combating and mitigating DDOS attacks in Smart Grid communication networks.

6.1 Contributions

This study proposed the SNA system design for Smart Grid communication networks. By refining and modifying the algorithms and codes of the SNA simulation tool, effective tactics for monitoring, detecting and mitigating the impacts of a DDOS attack on a WAMS Smart Grid communication network were developed. To enhance the detection and mitigation capabilities of the Smart Grid Communication Networks, firewall and intrusion prevention/detection systems were built. The simulation findings indicated that the mitigation methods and alarm system employed by the SNA system Tools, IPS, and Firewall successfully prevented the target system from shutting down or deteriorating due to the source attack. Below is a summary of the contribution to the research field:

(1) The ability to modify the SNA source code to effectively detect and mitigate the DDOS assault without disrupting or shutting down the targeted server or designated destination constitutes a primary contribution to this research effort. The attacker was unable to shut down the targeted server, which should have resulted in a complete shutdown or blackout of the destination or targeted server, in contrast to previous studies conducted using the GNS3 tool. The output from the GNS3 tool, which caused the targeted server to shut down as a result of the attack, and output from the SNA tool, which was able to identify and neutralize the attack without causing any downtime, are shown in Figs. 23 and 68. Additionally, listed below are the SNA-modified source codes used in this study.

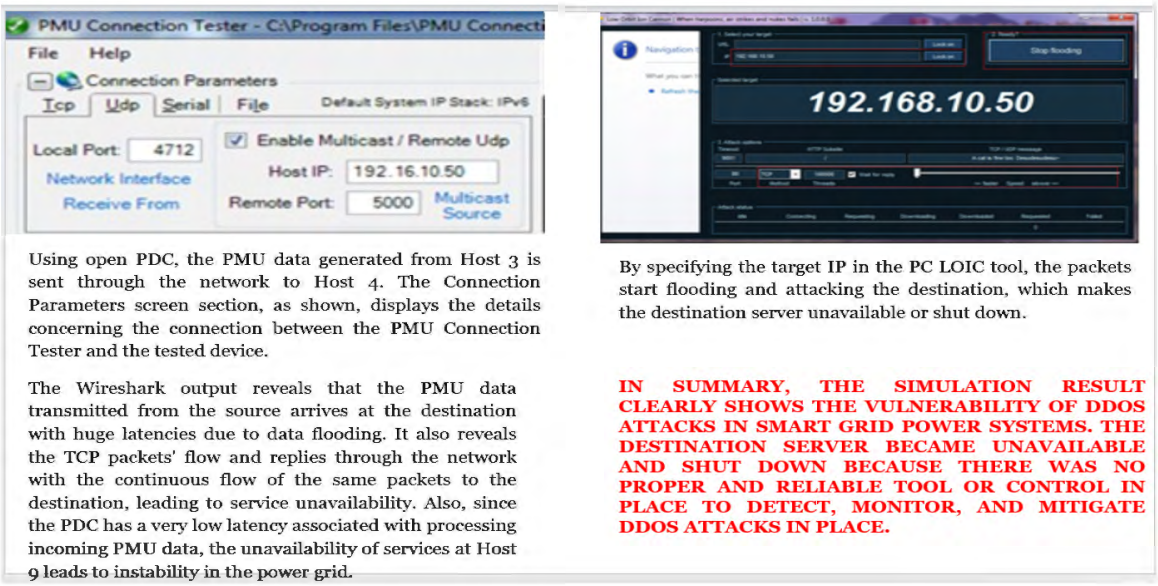


Fig. 23. Smart Grid Communication Network Simulations with GNS3 [66].

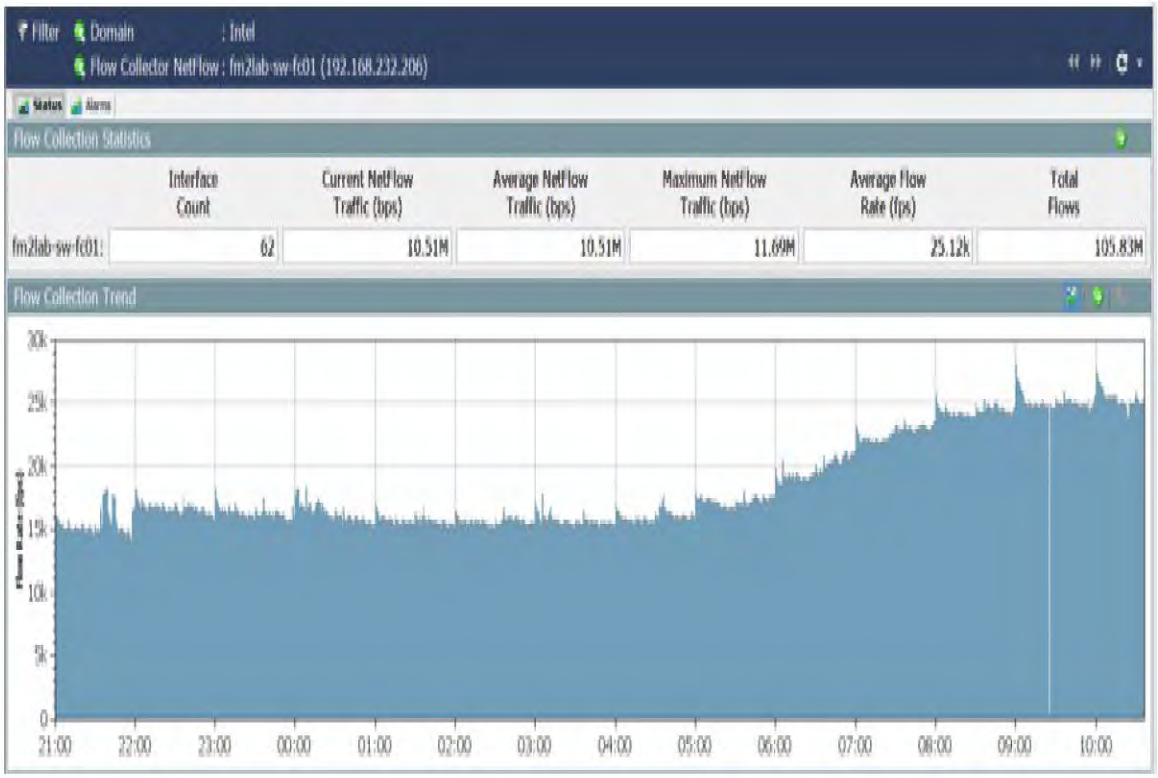


Fig. 68. SNA Simulations of Smart Grid Communication Networks.

The original Flow Collector Scala Type code configuration is shown below:

fm11d-sw-fc02:/lancope/var/containers/flow-forwarder/config# cat flow-forwarder.conf

fieldExportEnable {

flow {

start_active_usec = 1

last_active_usec = 1

client = 1

server = 1

service_port = 1

protocol = 1

service_id = 0

app_id = 0

flow_sensor_app_id = 1

packetshaper_app_id = 0

nbar_app_id = 1

palo_alto_app_id = 1

username = 1

vlan_id = 1

mpls_label = 1

connections = 1

retransmits = 0

rtt = 0

srt = 0

sequence_num = 1

fc_ip = 1

exporters = 1

selected_cipher_suite = 0

netflow_count = 0

}

host {

ip = 1

port = 1

port_max = 0

xlate_ip = 1

xlate_port = 1

mac = 1

asn = 1

payload = 0

payload_ex = 1

group_list = 1

num_bytes = 1

num_packets = 1

syn_packets = 0

syn_ack_packets = 0

rst_packets = 0

fin_packets = 0

sgt_id = 0

sgt_name = 0

total_bytes =1

total_packets =1

process_name = 0

process_hash = 0

process_username = 0

parent_process_name = 0

parent_process_hash = 0

parent_process_username = 0

idp = 1

byte_distribution = 1

tls_version = 1

tls_session_id = 1

payload_binary = 1

payload_ex_binary = 1

sequence_packet_lengths_times = 1

}

}

Below codes were added to the Flow Collector source code in this research work
fieldExportEnable {

flow

{

}

}

Service_id = 1

app_id = 1

retransmits = 1

rtt = 1

srt = 1

netflow_count = 1

fps_flowrate_ratio<15 =0

fps_flowrate_ratio>15 =1

fps_flowrate_alerts>15 =1

fps_admin_alert_flowrate_ratio>15 =1

{

}

}

port_max = 1

payload = 1

syn_packets = 1

syn_ack_packets = 1

rst_packets = 1

process_name = 1

process_username = 1

Configurations for Switch SPAN Feeds:

fm2lab-ex670A.3 # show mirror all

test_vm (Enabled)

Description: Mirror VM Traffic to FS

Mirror to port: 43

Source filter instances used: 1

Port 17, all vlans, ingress and egress

fm2lab-ex670A.4 # show port 17

(2) Modification occurred to the existing algorithm and was added codes to implement the modifications, establishing a traffic flow threshold/baseline and detecting exceeding the threshold/ baseline flow level, which indicates a potential DDOS attack.

(3) The flow chat was developed to show how a suspected attack is detected for quick action by the administrator.

(4) Ability to model the Smart Grid communication networks by designing and building various virtual machines (VMs) for the SNA tool, using VMs to incorporate the IDS/IPS & Firewall by assigning them IP addresses, and configuring SPAN feeds to fit the research work in application to Smart Grid communication networks.

(5) The IDS can be used to create a signature when an attack is detected, which can be incorporated into the design as another layer of security.

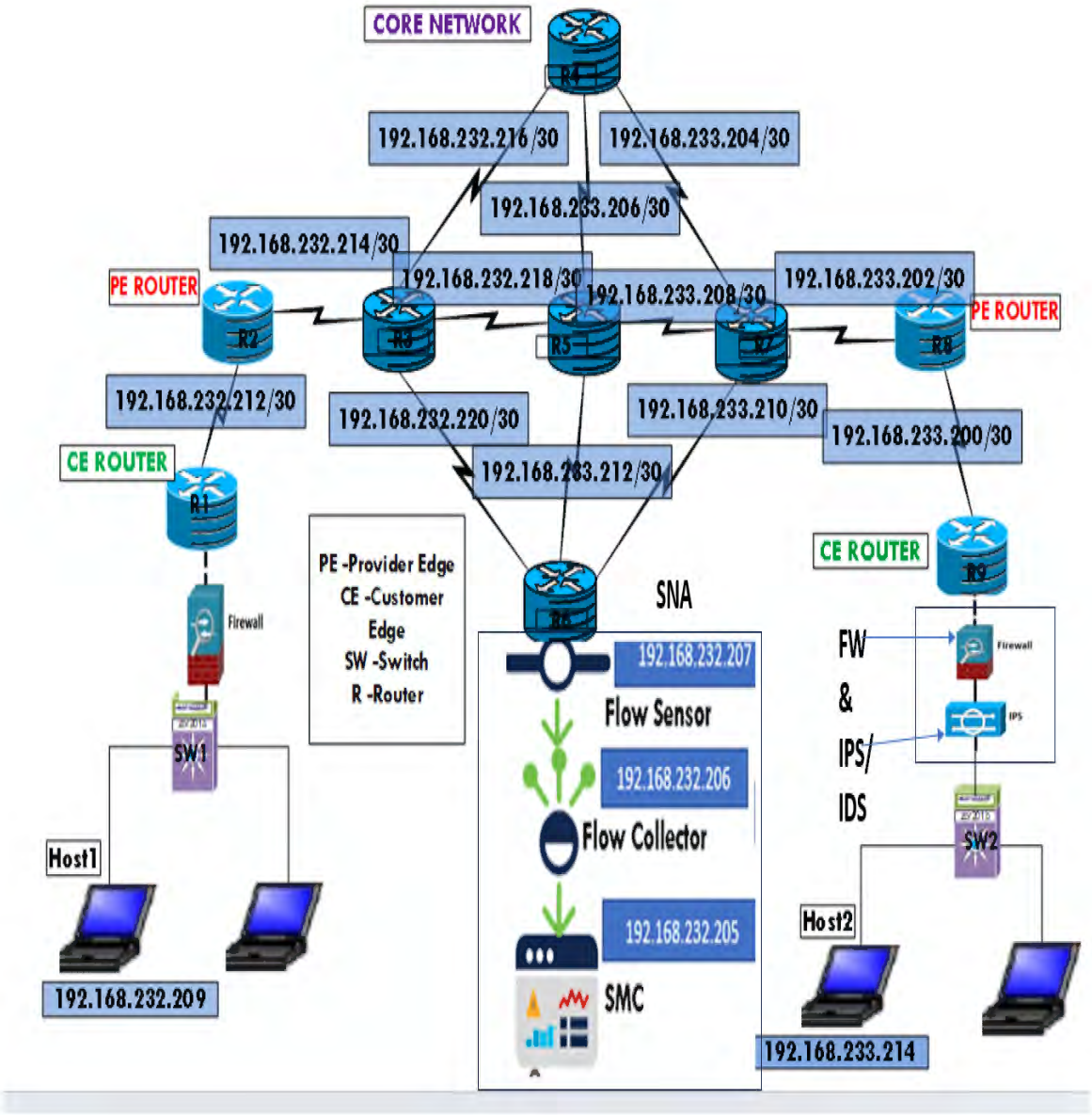


Fig. 24. SNA Tool-Proposed Smart Grid Communication Networks.

(6) Figs. 43 and 44 below illustrate the Firewall and IDS/IPS rules implemented in this research work. As part of the contributions, I added extra layers of detection by implementing firewall rules and IDS/IPS signatures, which were never included in the earlier research works.

The IPS signature rule can be used as another layer of security defense to block known attacks once they have been detected and mitigated as a form of remediation. From the SNA log, it can be seen that it captured the Sync Flood, port scan, and flow denied (which are indicators of a DDOS attack). The IPS can then be implemented once the signatures have been released by the vendor, as shown below.

ID	Source	Destination	Service	Action	Logging	Rule Name	Comment
Secure Network Analytics-Smart-Grid -LAB-Rules							
2171	h_192.168.232.209	host_192.168.233.214	ANY	Allow	Stored Connection Closing: No Log	@2227354.7	Secure Network Analytics-Smart-Grid -LAB-Rules
2172	host_192.168.233.214	h_192.168.232.209	ANY	Allow	Stored Connection Closing: No Log	@2227355.7	Secure Network Analytics-Smart-Grid -LAB-Rules
2173	FM_LAB_192.168.232.0_24	FM_LAB_192.168.233.0_24	ANY	Allow	Stored Connection Closing: No Log	@2227352.7	Secure Network Analytics-Smart-Grid -LAB-Rules
2174	FM_LAB_192.168.233.0_24	FM_LAB_192.168.232.0_24	ANY	Allow	Stored Connection Closing: No Log	@2228379.4	Secure Network Analytics-Smart-Grid -LAB-Rules
2175	ANY	FM_LAB_192.168.232.0_24 FM_LAB_192.168.233.0_24	ANY	Discard	Stored Connection Closing: No Log	@2228378.5	Secure Network Analytics-Smart-Grid -LAB-Rules

Fig. 43. SNA Smart Grid Firewall Rules Proposed.

Fig. 43. SNA Smart Grid Firewall in this section, the tools/devices/materials, codes, algorithms, and Lab apparatus simulation techniques used for the Detection and Mitigation of Distributed Denial of Service (DDOS) attack: Application to Smart Grid Communication Network have been discussed in detail.

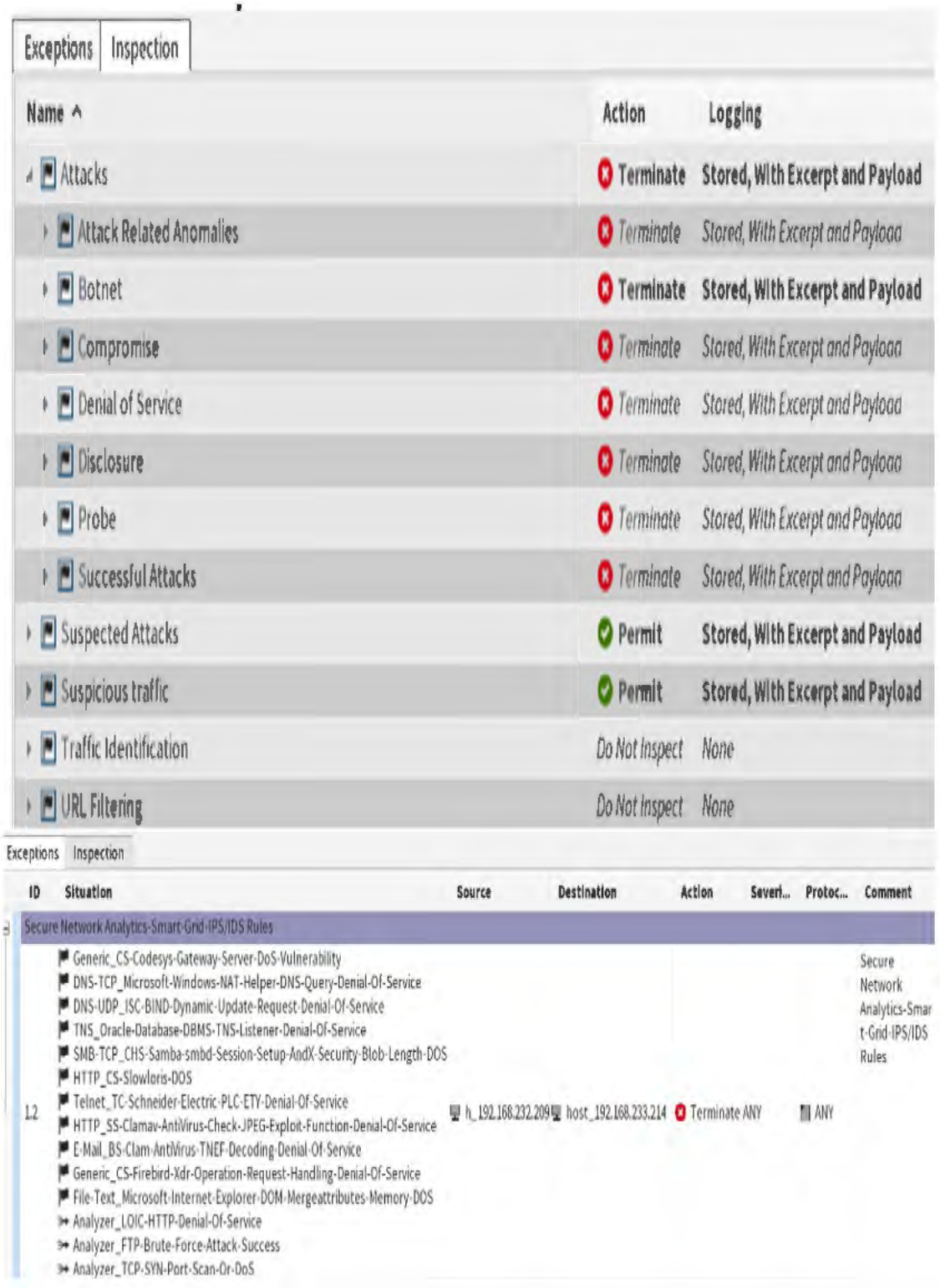


Fig. 44. SNA Smart Grid IDS/IPS Rules Proposed.

REFERENCES

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

[2] Y. Guo., C. W. Ten., S. Hu. and W. Weaver., "Modeling Distributed Denial of Service Attack in Advanced Metering Infrastructure," IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1-5, 2015.

[3] S. Asri. and B. Pranggono., "Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure," Wireless Personal Communications, vol. 83, no. 3, pp. 2211-2223, 2015.

[4] X. Xia. and J. Z. Xia., "Evaluation of Potential for Developing Renewable Sources of Energy to Facilitate Development in Developing Countries," Asia Pacific Power and Energy Engineering Conference (APPEEC), vol. 83, no. 3, pp. 2211-2223, 2010.

[5] P. Zhang., W. Xiao. and P. Choudhury., "Communication Systems for Grid Integration of Renewable Energy Resources," IEEE Network, vol. 25, pp. 22-29, 2011.

[6] H. Farhangi., "The Path of the Smart Grid ," IEEE Power and Energy Magazine, pp. 18-28, 2010.

[7] S. Amin. and B. F. Wollenberg., "Toward a Smart Grid : Power Delivery for the 21st Century," IEEE Power and Energy Magazine, vol. 3, pp. 34-41, 2005.

[8] D. Baimel., S. Tapuchi. and N. Baimel., "Smart Grid Communication Technologies," Journal of Power and Energy Engineering, vol. 4, pp. 1-8, 2016.

[9] K. Hannah. and B. Neil., "Hackers shut down Ukraine power grid," THE FINANCIAL TIMES LTD, 2016. [Online]. Available: www.ft.com/content/0cfffe1e-b3cd-11e5-8358-9a82b43f6b2f.

[10] B. Brian., "An Unprecedented Cyberattack Hit US Power Utilities," Wired, 2019. [Online]. Available: https://www.wired.com/story/power-grid-cyberattack-facebook-phone-numbers-security-news/.

[11] I. T. Report, "Communicatiob Networks and Systems in Sunstation Parts," IEC/TS, 2002-2005.

[12] IEC, "Communication Networks and Systems for Power Utility Automation," IEC, 2010.

[13] K. I. Sgouras., A. D. Birda. and D. P. Labridis., "Cyber Attack Impact on Critical Smart Grid Infrastructures," IEEE- ISGT 2014, vol. 2014, 1-5.

[14] P. Yi., T. Zhu., Q. Zhang., Y. Wu. and L. Pan., "Puppet Attack: A Denial-of-Service Attack in Advanced Metering Infrastructure Network," Network and Computer Applications, vol. 59, pp. 325-332, 2016.

[15] J. Wei. and D. Kondor., "A Flocking-Based Model for DoS-Resilient Communication Routing in Smart Grid ," 2012 IEEE Global Communications Conference (GLOBECOM), pp. 3519-3524, 2012.

[16] H. M. Shamina., J. R. Mattew., B. Russel. and C. Adrian., "Cybersecurity of Networked Microgrids: Challenges, Potential Solutions, and Future Directions," Los Alamos National Laboratory, 2020.

[17] W. RF., "Wireless Vendors and Resources," 2012, RF & Wireless Vendors and Resources, 2012. [Online]. Available: https://www.rfwireless-world.com/Articles/Smart-Grid-Architecture-basics-and-working.html.

[18] V. C. Gougor. and etal, "Smart Grid Technologies :Communication Technologies and Standards," IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 529-539, 2011.

[19] L. L. Grigsby., "Electric Power Engineering Handbook," CRC Press, Boca Raton, vol. 3rd edition, 2012.

[20] A. Pahwa., "Distribution Automation Fundamentals," IEEE/PES, 2008. [Online]. Available: http://wiki.powerdistributionresearch.com/index.php.

[21] U. D. o. Energy, "Benefits of Demand Response in Electricity Markets and Recommendations for Achieving Them," 2006.

[22] U. D. o. Energy, "Smart Grid System Report," washington, DC, 2009.

[23] B. Fang., X. Yin., Y. Tan., C. Li., Y. Gao., Y. Cao. and J. Li., "The contributions of cloud technologies to Smart Grid ," Renewable and Sustainable Energy Reviews, vol. 59, pp. 1326-1331, 2016.

[24] K. Demir., H. Ismail., T. Gurova. and N. Suri., "Securing the cloud-assisted Smart Grid ," International Journal of Critical Infrastructure Protection, pp. 100-111, 2018.

[25] O. A. Otuoze., W. M. Mustafa. and M. R. Larik., "Smart Grid security challenges: Classification by sources of threat," Journal of Electrical Systems and Information Technology, vol. 5, no. 3, pp. 468-483, 2018.

[26] M. Shrestha., C. Johansen., J. Noll. and D. Roverso., "A Methodology for Security Classification applied to Smart Grid Infrastructures," International Journal of Critical Infrastructure Protection,, vol. 28, 2020.

[27] E. N. Yilmaz., B. Ciylan., S. Gonne., E. Sindiren. and G. Karacayılmaz., "Cyber Security in Industrial Control Systems: Analysis of DoS Attacks Against PLCs and the Insider Effect," 2018 6th International Istanbul Smart Grid s and Cities Congress and Fair (ICSG), pp. 81-85, 2018.

[28] R. Liu., C. Vellaithurai., S. S. Biswas., T. T. Gamage. and K. A. Srivastava., "Analyzing the cyber-physical impact of cyber events on the power grid," IEEE Transactions on Smart Grid , vol. 6, no. 5, pp. 2444-2453, 2015.

[29] W. Brown. and L. Stallings., Computer Security: Principles and Practice 3rd ed, Pearson Education, Inc, 2015.

[30] K. Khanna., K. B. Panigrahi. and A. Joshi., "Feasibility and mitigation of false data injection attacks in Smart Grid ," 2016 IEEE 6th International Conference on Power Systems (ICPS), pp. 1-6, 2016.

[31] J. Ma., Y. Liu., L. Song. and Z. Han., "Multiact dynamic game strategy for jamming attack in electricity market," IEEE Transactions on Smart Grid , vol. 6, no. 5, pp. 2273-2282, 2015.

[32] N. Davis., "The Smart Grid : What's "The Grid" And How Is It "Smart?"," Powerelectronicsnews, 2017. [Online]. Available: https://www.powerelectronicsnews.com/the-smart-grid-whats-the-grid-and-how-is-it-smart/#:~:text=This%20growing%20network%20of%20communications,to%20be%20integrated%20into%20our.

[33] S. Landge., "mart Grid Communication.," International Journal of Engineering Research and General Science, vol. 3, no. 1, 2015.

[34] A. Naame. and N. K. Msirdii., "Towards a Smart Grid Communication.," Energy Procedia, vol. 83, pp. 428-433, 2015.

[35] V. A. Kharlamov., "The recovery of power relay systems after successful cyber-attacks," Relayer, vol. 2, p. 54, 2016.

[36] D. Kundur., X. Feng., P. P. Liu., T. Zourntos. and K. Butler-Purry., "Towards a framework for cyber-attack impact analysis of the electric Smart Grid ," Proc. 1st IEEE Int. Conf. Smart Grid Common, vol. 49, pp. 244-2, 2010.

[37] T. R. Sharafeev., V. J. Osokin. and A. L. Kulikov., "Cyber-Security Problems in Smart Grid . Cyber-attacks Detecting Methods and Modelling Attack Scenarios on Electric Power Systems," 2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), 2018.

[38] Z. JIZHONG., OPTIMIZATION OF POWER. Second Edition, IEEE Press Wiley, 2015.

[39] E. P. Mohajerin., M. Vrakopoulou., K. Margellos., J. Lygeros. and G. Andersson., "Cyber-attack in a two-area pow-er system: Impact identification using reachabilit," Proc. Amer. Control Conf, pp. 962-967, 2010.

[40] X. Jin., J. Bigham., J. Rodaway., G. Gamez. and C. Phillips., "Anomaly Detection in Electricity Cyber Infrastructures," Proc. Int. Workshop CNIP 2006, 2006.

[41] Y. Liu., P. Ning. and K. M. Reiter., "False data injection attacks against state estimation in electric power grids," ACM Transactions on Information and System Security, vol. 14, no. 1, 2011.

[42] V. A. Kharlamov., "The recovery of power relay systems after successful cyber-attacks," Relayer, vol. 2, p. 54, 2016.

[43] NERC, "Reliability Standards," NERC, 2023. [Online]. Available: https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx.

[44] R. Liu., C. Vellaithurai., S. S. Biswas., T. T. Gamage. and K. A. Srivastava., "Analyzing the cyber-physical impact of cyber events on the power grid," IEEE Transactions on Smart Grid , vol. 6, no. 5, pp. 2444-2453, 2015.

[45] U. D. o. Energy, "The Smart Grid ," U.S. Department of Energy, [Online]. Available: https://www.smartgrid.gov/the_smart_grid/smart_grid.html.

[46] W. S. a. L. Brown, Computer Security: Principles and Practice, 3rd ed, Nj: Upper Saddle River, 2015.

[47] F. Samie., L. Bauer. and J. Henkel., "Edge Computing for Smart Grid : An Overview on Architectures and Solutions," IoT for Smart Grid , vol. A247, pp. 21-42, 2018.

[48] O. Carvalho., M. Garcia., E. Roloff. and E. Diaz., "IoT Workload Distribution Impact between Edge and Cloud Computing in A Smart Grid Application," Latin America High-Performance Computing Conference, pp. 203-217, 2017.

[49] R. Brown., "Impact of Smart Grid on Distribution System Design," Power and Energy Society General Meeting Conversion and Delivery of Electrical Energy in the 21st Century, pp. 1-4, 2009.

[50] R. Buyya. and C. Yeo., "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing," Future Generation Computer Systems, pp. 599-616, 2009.

[51] A. Dattjerdi. and R. Buyya., "Fog Computing: Helping the Internet of Things Realize Its Potential," Cloud Cover, pp. 112-116, 2016.

[52] S. Chen., H. Wen., J. Wu., W. Lei., W. Hou., W. Liu. and A. Xu., "Internet of Things Based Smart Grid s Supported by Intelligent Edge Computing," IEEE Access, pp. 1-14, 2019.

[53] S. Bruske., D. G. Carne. and M. Liserre., "Multi-frequency power transfer ¨ in a smart transformer-based distribution grid,"," IECON 2014-40th Annual Conf. of the IEEE Ind. Electron. Society, pp. 4325-4331, 2014.

[54] A. Sandeep. and G. B. Fernandes., "Optimal voltage level for dc microgrids," in proc. IEEE 36th Annu. Conf. of the Ind. Electron. Soc. (IECON), pp. 3034-3039, 2010.

[55] D. Rajdip. and N. Shabari., "Architecture and power converter for multifrequency microgrid," in 2019 National Power Electron. Conf. (NPEC), pp. 1-6, 2019.

[56] F. Lau., H. S. Rubin., H. M. Smith. and L. Trajković., "Distributed denial of service attacks, in: Systems, Man, and Cybernetics," 2000 IEEE International Conference, vol. 3, pp. 2275-2280, 2000.

[57] S. Liu., P. X. Liu. and E. Saddik., "Denial-of-Service (DoS) attacks on load frequency control in Smart Grid s," In Innovative Smart Grid Technologies (ISGT)-IEEE, pp. 1-6, 2013.

[58] M. P. Esfahani., M. Vrakopoulou., J. L. Margelle's. and G. Andersson., "Cyber-attack in a two-area power system: Impact identification using reachability," In American Control Conference (ACC), pp. 962-967, 2010.

[59] T. S. Zargar., J. B. D. Joshi. and D. Tipper., "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," IEEE communications surveys & tutorials, vol. 15, no. 4, pp. 2046-2069, 2013.

[60] T. Sauter. and M. Lobashov., "End-to-End Communication Architecture for Smart Grid s," IEEE Transactions on Industrial Electronics, vol. 4, no. 58, p. 12181228, 2011.

[61] W. Wang., Y. Xu. and M. Khanna., "A survey on the communication architectures in Smart Grid .," Computer Networks, vol. 15, no. 55, pp. 3604-3629, 2011.

[62] S. Landge., "Smart Grid Communication.," International Journal of Engineering Research and General Science, vol. 3, no. 1, pp. 1-6, 2015.

[63] Y. Tarun. and M. R. Arvind., "Technical Aspects of Cyber Kill Chain," Springer International Publishing Switzerland, pp. 438-452, 2015.

[64] Cisco, "Cisco Models Specifications," Cisco Inc, [Online]. Available: cisco.com.

[65] D. Brett., "Trenton Systems," [Online]. Available: https://www.trentonsystems.com/en-us/resource-hub/blog/symmetric-vs-asymmetric-encryption.

[66] S. Premkumar. and V. Saminadan., "Impact of Denial of Service (DOS) attck i Smart Distribution Grid Communication Network," International Journal of Applied Engineering Research, vol. 12, no. 4, pp. 4443-4447, 2017.

CURRICULUM VITAE

EMMANUEL S KOLAWOLE

ekolawole@pvamu.edu

EDUCATION

- Ph.D. Electrical Engineering, Prairie View A&M University, Prairie View, Texas, 2025
- M.S. Electrical and Computer Engineering, Prairie View A&M University, Prairie View, Texas, 2014
- B.SC Electrical and Computer Engineering, Federal University and Technology, Akure, Ondo State, Nigeria, 2012

WORK EXPERIENCE

- Company: Intel Corporation
  Position: Info Security DevSecOps Engineer
  Job: Manage InfoSec Network Security Infrastructures/Cyber Operations

- Company: Prairie View A&M University, College of Engineering
  Position: Graduate Research Assistant
  Job: Research and innovations

- Company: Freeman & Curiel Engineers LLP
  Position: Network & Instrumentation Engineer
  Job: Network Instrumentations and control

- Company: GE Oil & GAS
  Position: Network Security & Validation Engineer
  Job: Network Testing and Validations

PROFESSIONAL, TECHNICAL AND WORK-RELATED EXPERIENCE AND SKILLS

Skills: Network Operations, Cyber Security, Intrusion and Detections, Security information & Event management monitoring, Troubleshooting, Firewalls, Smart Grid Technology.

Certifications: CCNA (Routing & Switching), CCNA (Security), CCNA (CyberOps),

CCNP, Palo Alto Firewall; PCNSA, PCNSE, CISA, CDPSE, CISM, CRISC, CGEIT, McAfee-Firewall, Checkpoint Firewall, CISSP-, Cisco Certified CyberOps Specialist (CyberOps Core), Cisco Certified Specialist (Security Core).

Publications & Presentations:

[1] **Kolawole, E.,** Cofie, P., Fuller, J., (**2017**) Practical Approaches to Securing an IT Environment. (A case study of WAN-LAN Environment). Communications and Network, 9,275-290.

[2] **Kolawole, E.,** etal (**2016**) Digital Signal Processing (DSP): (Fundamentals, Techniques and Applications). Nova Science Publishers, ISBN**:** 978-1-63485-168-8.

[3] **Kolawole, E.,** Ali, W., Obiomon, P., Fuller, J., Ali, S. and Cofie, P. (**2016**) Rapid Prototype with Field Gate (A Design and Implementation of Stepper Motor Using FPGA). Circuits and Systems, **7**, 1392-1403.

[4] **Kolawole, E.,** Ali, W., Cofie, P., Fuller, J., (**2016**) Optimization of FPGA Resource Usage in Today's Design and Application (AN FPGA IMPLEMENTATION). International Journal of Software & Hardware Research in Engineering, Volume 4 Issue 2, 99-106.

[5] **Kolawole, E.,** Ali, W., Cofie, P., Fuller, J., Tolliver, C. and Obiomon, P. (**2015**) Design and Implementation of Low pass, High-pass, and Band-pass Finite Impulse Response (FIR) Filter Using FPGA. Circuits and Systems, 6, 30-48.

[6] Olukayode A. Afolabi, **Kolawole, E.,** Warsame H. Ali, Penrose Cofie, John Fuller, Pamela Obiomon, (**2015**) Analysis of the Load Flow Problem in Power System Planning Studies. Energy and Power Engineering, Vol.7 No.10, 509-523.

[7] **Kolawole, E.,** etal., (**2019**) Security Issues, Threats, and Possible Solutions in Cloud Computing. American Journal of Information Science and Computer Engineering, Vol.5, No. 2, (**2019**), pp. 38-46, ISSN: 2381-7488; ISSN: 2381-7496

[8] Ali, W.H., Cofie, P., Fuller, J.H., Lokesh, S. and **Kolawole, E.S.** (**2017**) Performance and Efficiency Simulation Study of a Smart-Grid Connected Photovoltaic System. Energy and Power Engineering, 9, 71-85.

[9] Islam, N. Ali, W., **Kolawole, E** , Fuller, J. , Obiomon,P. , Attia, J. and Abood, S. (**2021**) Cost Optimization Modeling of Renewable Energy Sources in Smart-Grid Using SCADA. Communications and Network,13, 51 67.doi:10.4236/cn.2021/cn.2021.132005.

[10] **Kolawole, E. S**., Cofie, P., and Fuller, J. (**2022, March**), The Fast and Practical Approach to Effectively Securing a Cloud Computing System with Today's Technology Paper presented at 2022 ASEE Gulf Southwest Annual Conference, Prairie View, Texas. https://peer.asee.org/39209https.

[11] **Kolawole, E. S**., Cofie, P. S., Fuller, H. J., Akujuobi, C. M., Dada, E. A., Foreman, J. F., and Obiomon, H **(2024)**, Optimization of StealthWatch Network Security System for the Detection and Mitigation of Distributed Denial of Service (DDOS) attack: Application to Smart Grid System. Communications and Network, 2024, 108-134.