Advanced Techniques for Monitoring and Detecting Cyber-Physical Attacks on IEC 61850 Smart Grid Substations

Abdullah Albarakati

A Thesis

in

The Concordia Institute

For

Information Systems Engineering

Presented in Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy (Information and Systems Engineering) at

Concordia University

Montréal, Québec, Canada

September 2025

© Abdullah Albarakati, 2025

CONCORDIA UNIVERSITY

SCHOOL OF GRADUATE STUDIES

This is to certify that the thesis prepared

By: *Abdullah Albarakati*

Entitled: Advanced Techniques for Monitoring and Detecting Cyber-Physical Attacks on IEC 61850 Smart Grid Substations

and submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY (INFORMATION AND SYSTEMS ENGINEERING)

complies with the regulations of this University and meets the accepted standards with respect to originality and quality.

Signed by the Final Examining Committee:

_____ Chair
Dr. Otmane Ait Mohamed

_____ External Examiner
Dr. Tedjani Mesbahi

_____ Examiner
Dr. Chadi Assi

_____ Examiner
Dr. Mohsen Ghafouri

_____ Examiner
Dr. Mohammad Soleymani

_____ Co-supervisor
Dr. Mourad Debbabi

_____ Co-supervisor
Dr. Amr Youssef

Approved by _____
Dr. Andrea Schiffauerova, Graduate Program Director
Department of Information Systems Engineering

_____ 2025

_____
Dr. Mourad Debbabi, Dean
Gina Cody School of Engineering and Computer Science

Abstract

Advanced Techniques for Monitoring and Detecting Cyber-Physical Attacks on IEC 61850 Smart Grid Substations

Abdullah Albarakati, Ph.D.

Concordia University, 2025

The increasing digitization and interconnection of power systems has improved their operational efficiency and flexibility, but has also introduced critical cyber vulnerabilities. Ensuring the security of smart grid substations is therefore crucial for maintaining reliable grid operation and power delivery. In this thesis, we address the critical challenge of detecting attacks against IEC 61850 substations. The research encompasses the development and validation of advanced security monitoring frameworks using machine learning techniques and system simulations. We first introduce an OpenStack-based Hardware-in-the-Loop (HIL) framework that supports both emulation and co-simulation. This environment enables controlled evaluation of smart grid components' resilience to cyber threats and facilitates testing of the proposed security solutions. We then leverage Network and System Management (NSM) based on IEC 62351-7 and propose a hybrid anomaly detection platform that combines rule-based methods and deep learning to detect threats within IEC 61850 substations. To this end, we introduce a two-stage deep learning architecture that integrates LSTM, RNN, and GRU models to further enhance the accuracy of NSM-based anomaly detection. We then validate these approaches through simulations on various standard IEEE test grids. Finally, we implement a Deep Packet Inspection (DPI) mechanism, in compliance with the IEC 62351-90-2 standard, to identify malicious activity targeting IEC 61850 substations. This mechanism employs a two-level architecture to identify anomalies and then determine whether they were caused by faults or attacks. We then test this approach on a realistic IEC 61850 substation model implemented in our real-time co-simulation testbed. Collectively, the contributions discussed within this thesis offer a strategy, based on the IEC 62351 standard, to secure substations in a smart grid.

Acknowledgments

First and foremost, I extend my deepest gratitude to my supervisors, Dr. Mourad Debbabi and Dr. Amr Youssef, for their invaluable guidance, mentorship, and support throughout the duration of this research. Dr. Debbabi's expertise and insightful critiques have been crucial in shaping the research direction and execution of this thesis. His encouragement and high standards pushed me to refine my work to its highest quality.

I am also profoundly grateful to Dr. Amr Youssef, whose expertise in cybersecurity significantly enriched my understanding and approach to tackling the complex issues addressed in this thesis. Dr. Youssef's rigorous analytical techniques and thoughtful feedback were instrumental in refining my methodologies and enhancing the overall quality of my research.

I would also like to extend a heartfelt thanks to all my friends at Concordia University who have worked with me, advised me, or helped me throughout my thesis journey. Your camaraderie and support have made my time at Concordia not only productive but also enjoyable. Whether it was through late-night study sessions, insightful discussions, or simply sharing words of encouragement, your contributions have been invaluable. I am truly grateful for each one of you and cherish the strong bonds we have formed during our time together.

The journey through my academic research was not only shaped by academic guidance but also encouraged by the unwavering support and confidence of my mentors and peers. Their mentorship and friendship extended beyond academic knowledge, teaching me the value of perseverance and rigorous scientific inquiry. I am thankful for their willingness to share their expertise and for their assistance in helping me navigate through the challenges of my PhD journey. Their contributions have left a lasting impact on my professional and personal development.

Contents

List of Figures

List of Tables

Abbreviations

AI	Artificial Intelligence
APT	Advanced Persistent Threat
CB	Circuit Breaker
C37.118	IEEE Standard C37.118 for Synchrophasors
CPS	Cyber-Physical System
DO	Data Object
DoS	Denial-of-Service
DNP3	Distributed Network Protocol 3
DPI	Deep Packet Inspection
GNSS	Global Navigation Satellite System
GOOSE	Generic Object Oriented Substation Event
GPS	Global Positioning System
GRU	Gated Recurrent Units
GSE	Generic Substation Event
HIL	Hardware-In-the-Loop
HMI	Human–Machine Interface

IA	Information Assurance
ICS	Industrial Control System
ICT	Information and Communication Technologies
IED	Intelligent Electronic Device
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IoT	Internet of Things
IT	Information Technology
LSTM	Long Short-Term Memory
MIB	Management Information Base
Modbus	Modicon Bus
MMS	Manufacturing Message Specification
MU	Merging Unit
NSM	Network and System Management
OT	Operational Technology
PM	Prediction Model
PMU	Phasor Measurement Unit
PDC	Phasor Data Concentrator
PDU	Protocol Data Unit
PTP	Precision Time Protocol

R-GOOSE	Routable Generic Object Oriented Substation Event
R-SV	Routable Sampled Values
RMSE	Root-Mean-Square Error
RNN	Recurrent Neural Network
RTU	Remote Terminal Unit
SAS	Substation Automation System
SCADA	Supervisory Control and Data Acquisition
SEL	Schweitzer Engineering Laboratories
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SVM	Support Vector Machine
SV	Sampled Values
TAL	Time-Allowed-to-Live
TC57	Technical Committee 57
TLS	Transport Layer Security
UDP	User Datagram Protocol
VM	Virtual Machine
WAN	Wide Area Network
WAMS	Wide Area Measurement Systems

Chapter One

Introduction

1.1 Overview and Motivations

The Smart Grid represents a transformative evolution in traditional power systems, integrating advanced technologies to improve operational efficiency and strengthen the reliability of the system. The integration of cutting-edge communication and automation into the smart grid allows for the monitoring, controlling, and optimizing of power generation, distribution, and consumption. This evolution also facilitates the integration of renewable and distributed energy sources, enhancing consumer active participation and improving grid resilience.

At the heart of this transformation are electric power substations, which serve as critical nodes for stepping voltage levels up or down and routing power between transmission and distribution networks. These substations are increasingly digitalized, relying on intelligent electronic devices (IEDs) that monitor electrical conditions, execute protection and control logic, and communicate with one another over network infrastructures.

The communication between IEDs in digital substations is governed by a class of network protocols referred to as operational technology (OT) protocols. One of the most widely adopted standards in this domain is IEC 61850, which defines the architecture, data models, and services for substation automation systems. Within this standard, various protocols support different functions: Generic Object Oriented Substation Event (GOOSE) messages are used for the rapid exchange of protection and control signals; Manufacturing Message Specification (MMS) handles client-server

communications for supervisory control; and Sampled Values (SV) streams carry time-critical analog measurement data such as voltage and current samples.

To complement the communication framework of IEC 61850, the IEC 62351 series of standards provides cybersecurity mechanisms tailored to the smart grid context. These include recommendations for securing communication channels, ensuring data integrity and authentication, and enabling network and system monitoring. Additional supporting standards, such as IEEE C37.118 for phasor measurement and IEEE 1588 for time synchronization, further enhance the functionality and coordination of modern grid operations.

A notable example of the smart grid implementation is the North American Smart Grid, with 37 cross-border interconnections between Canada and the U.S.A. [2], accounting for approximately 16% of global electricity production [3]. It encompasses over 1.1 million kilometers of high-voltage transmission lines [4,5] with an installed generation capacity of approximately 1,340,499 MW [5,6], involving around 5,506 utility and control organizations [5,6]. This complex infrastructure supports more than 371 million customers [5, 7–9] and is valued at over US$1.3 trillion [10]. This scale underscores the critical importance of securing such infrastructures.

At the core of this modernization lies the integration of Information and Communication Technologies (ICT), which significantly enhances grid monitoring, protection, and control in real-time through Intelligent Electronic Devices (IEDs). These devices are meant to comply with standards such as IEC 61850, IEC 62351, IEEE C37.118, and IEEE 1588. However, despite adherence to these standards, the smart grid infrastructures remain vulnerable to cyberattacks [11, 12]. Notable incidents, such as the 2015, 2016, and 2022 cyberattacks on Ukraine [12, 13], demonstrate how adversaries can disrupt operations and cause outages by targeting communication protocols. This highlights the need for comprehensive security mechanisms that go beyond standard compliance.

1.2 Problem Statement

Smart grid substations based on the IEC 61850 standard play a key role in modern power systems, but remain exposed to serious cybersecurity threats. Although standards like IEC 61850 and IEC 62351 were created to improve communication and security, real-world attacks such as those in

Ukraine have shown that current protections are not enough [14]. These attacks can cause failures that move from the cyber systems to the physical infrastructure, leading to blackouts and risks to public safety. A major challenge is the lack of reliable and real-time methods to detect and respond to these threats in practice. There is also limited support for analyzing actual IEC 61850 traffic to spot advanced attack patterns. Therefore, there is a need for realistic testbed and advanced monitoring systems capable of detecting cyber-physical attacks, while remaining compatible with existing power grid standards.

1.3 Objectives

The main objectives of this thesis are:

- To investigate the cyber-physical impacts of cyberattacks targeting IEC 61850-based substations.
- To design and implement a real-time co-simulation testbed for evaluating cybersecurity frameworks in realistic substation environments.
- To develop a detection framework based on Network and System Management (NSM) data, leveraging IEC 62351-7 for identifying abnormal behavior in substations.
- To design a Deep Packet Inspection (DPI)-based detection system that enhances substation security by analyzing real-time IEC 61850 traffic.
- To validate the proposed frameworks through simulations and Hardware-in-the-Loop (HIL) experiments.

1.4 Thesis Contributions

This thesis contributes to the ongoing efforts to enhance the cybersecurity and resilience of smart grid infrastructures, with a particular focus on IEC 61850-based substations. The primary objective is to strengthen the security posture of communication protocols critical to substation operations, specifically targeting delay-based cyberattacks that threaten grid stability and reliability. The first

contribution of this thesis is a thorough review of the state-of-the-art related to cybersecurity within smart grid substations. This includes an in-depth examination of the IEC 61850 protocol suite, its associated cybersecurity recommendations, and known threat vectors. A brief overview of the remaining contributions is presented below.

1.4.1 Real-Time Co-Simulation

Simulating smart grid behavior in a real-time environment enables a comprehensive assessment of cyber-physical impacts resulting from cyberattacks. A key challenge lies in the seamless integration of real-time physical system simulation with the emulation of cyber infrastructure. In Chapter 3, we presents the design and implementation of a sophisticated real-time co-simulation testbed that accurately represents the multifaceted nature of smart grid operations.

This co-simulation environment facilitates the in-depth analysis of vulnerabilities in Wide Area Measurement Systems (WAMS), particularly in relation to attacks targeting their communication networks. It enables the emulation of realistic cyber-attack scenarios and the observation of their cascading physical consequences. Through this testbed, we demonstrate how cyber intrusions into WAMSs can lead to significant disruptions, highlighting the importance of integrated cyber-physical security assessments.

1.4.2 Leveraging IEC62351-7 Network and System Management to Enhance Substation Security

Chapter 4 investigates the role of ICT in modernizing the power grid infrastructure, particularly through their integration into digital substations and WAMSs. While ICT enhances real-time monitoring and control capabilities, it also introduces new cybersecurity risks that threaten grid reliability and operational stability.

To address these challenges, we focus on the application of the IEC 61850 and IEC 62351 standards, with an emphasis on IEC 62351-7 [15]. We propose a security monitoring framework based on Network and System Management (NSM) to detect anomalous behaviors indicative of cyberattacks within digital substations.

Our methodology and findings are validated on our real-time co-simulation testbed equipped

with Hardware-In-the-Loop (HIL) capabilities, demonstrating its practical effectiveness in enhancing the security and reliability of the smart grid infrastructure. In addition to the implementation and evaluation of the proposed detection system, the chapter also presents detailed system and threat modeling.

1.4.3 Leveraging Deep Packet Inspection to Enhance Substation Security

Chapter 5 addresses the critical issue of cybersecurity in smart grids, with a specific focus on the critical vulnerabilities in the IEC 61850 protocol. The IEC 62351 standard is explored as a solution, providing security recommendations to address the identified issues. Notably, the IEC 62351 encourages the use of NSM data for security purposes and advocates the deployment of Deep Packet Inspection (DPI) for security monitoring.

The main contributions presented this chapter is the design and implementation of a DPI-based security framework deployed at the substation level. Each substation is equipped with a DPI agent that monitors IEC 61850 traffic including control signals and measurement data—captured in real time. These data streams are processed using a multi-step deep learning architecture to detect anomalies, classify cyberattacks, distinguish physical faults, and identify faulty control signals. The proposed system is validated using a real-time co-simulation testbed with HIL capability, demonstrating its effectiveness in improving the detection of anomalous events within digital substations.

1.5 Publications Resulting from This Research

The work presented in this thesis has contributed to the following peer-reviewed publications:

(1) A. Albarakati, B. Moussa, M. Debbabi, A. Youssef, B. Agba, and M. Kassouf, "OpenStack-Based Evaluation Framework for Smart Grid CyberSecurity," in *Proc. of the IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2018 [16].

(2) A. Albarakati, C. Robillard, M. Karanfil, M. Kassouf, R. Hadjidj, M. Debbabi, and A. Youssef, "Security Monitoring of IEC 61850 Substations Using IEC 62351-7 Network and System Management," in *Proc. of the IEEE SmartGridComm*, 2019 [17].

(3) A. Albarakati, C. Robillard, M. Karanfil, M. Kassouf, M. Debbabi, A. Youssef, M. Ghafouri, and R. Hadjidj, "Security Monitoring of IEC 61850 Substations Using IEC 62351-7 Network and System Management," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1641–1653, 2021 [18].

The PhD candidate has also contributed to the following peer-reviewed publications (which are not part of the work presented in this thesis):

(1) R. Kateb, P. Akaber, M.H.K. Tushar, A. Albarakati, M. Debbabi, and C. Assi, "Enhancing WAMS Communication Network Against Delay Attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2738–2751, 2018 [19].

(2) B. Moussa, A. Albarakati, M. Kassouf, M. Debbabi, and C. Assi, "Exploiting the Vulnerability of Relative Data Alignment in Phasor Data Concentrators to Time Synchronization Attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2541–2551, 2019 [20].

1.6 Thesis Organization

The subsequent sections of this thesis are structured as follows. In Chapter 2, we provide a brief overview of threats targeting smart grids, particularly within substations. We also delve into the specifications and standards, with a focus on digital substations. Additionally, we present a comprehensive survey of existing literature addressing security concerns related to IEC 61850 substations.

In Chapter 3, we explore the design and implementation of our real-time co-simulation testbed for smart grids, providing a platform to study the cyber-physical behavior of smart grids. We then present in Chapter 4 our design and implementation of the security monitoring framework for IEC 61850 substations using IEC62351-7 Network and System Management (NSM). We also present our security monitoring framework for IEC 61850 substations using Deep Packet Inspection (DPI) as an additional component to the IEC 62351 standard in Chapter 5. Finally, Chapter 6 concludes this thesis and recaps its main contributions, as well as outlines potential future research directions.

Chapter Two

Background and Literature Review

In this chapter, we present an overview of the security of smart grids with a special focus on IEC 61850 substations. We start this chapter by presenting the components and architecture of IEC 61850 substations. We then provide a detailed review of the protocols responsible for measurement acquisition and control signal exchange. A security assessment of these protocols is presented to evaluate their exposure to cyber threats. Next, we discuss relevant standardization efforts that inform the cybersecurity landscape of digital substations, offering insights into the protective measures defined by international standards. The chapter concludes with a security gap analysis of the IEC 61850 protocol, identifying open research challenges and critical areas that require further investigation to enhance the resilience of smart grid substations.

2.1 Security in Cyber-Physical Systems

Cyber-Physical Systems (CPSs) have become integral to the operation of critical infrastructures, including energy, transportation, and healthcare systems. By tightly coupling computational and physical components, CPSs enable enhanced automation, real-time control, and system optimization. However, this integration also introduces complex cybersecurity challenges, making CPSs increasingly attractive targets for malicious actors. This section explores key security threats facing CPSs, with particular attention to notable attack vectors in Industrial Control Systems (ICSs) environments.

These systems are susceptible to a variety of cyber threats that can disrupt operations, compromise safety, and cause significant economic damage. One of the most critical threats is posed by Advanced Persistent Threats (APTs), which are highly targeted and prolonged cyber campaigns typically executed by well-resourced adversaries. APTs are designed to infiltrate systems without authorization and persist stealthily over long durations, allowing attackers to extract sensitive data, alter control operations, and interfere with critical services [21–23].

Another major concern is Distributed Denial-of-Services (DDoSs) attacks, which flood network resources with excessive traffic, rendering systems unavailable to legitimate users. In smart grids contexts, DDoS attacks can have critical consequences by impairing real-time monitoring, control, and protection mechanisms in electricity generation, transmission, and distribution [24, 25].

The proliferation of intelligent internet-connected devices further exacerbates the attack surface. These devices often lack standardized security properties such as availability, integrity, authentication, authorization, and confidentiality, introducing vulnerabilities that can be exploited by adversaries. Consequently, there is a growing need for robust, scalable, and adaptive security frameworks capable of addressing threats across heterogeneous CPS environments such as the smart grid. Moreover, the inherent complexity of CPS architectures demands advanced modeling techniques and fault-tolerant system designs to mitigate cascading failures caused by cyber or physical anomalies. The use of distributed and real-time sensing technologies introduces additional challenges in maintaining data availability, integrity, and confidentiality. Interoperability among subsystems amplifies these challenges, highlighting the need for holistic and layered security mechanisms [26].

2.1.1 Notable Cyberattacks on CPS

Cybersecurity has become a critical concern for modern CPS, with cyberattacks increasing in both frequency and sophistication. This section highlights a selection of significant cyberattacks that have targeted industrial control systems and smart grid environments. These attacks not only demonstrate the evolving threat landscape but also underscore the urgent need for proactive and adaptive security strategies.

In 2010, the Stuxnet malware [27] gained significant attention due to its sophisticated nature and targeted attack on Supervisory Control and Data Acquisition (SCADA) systems in Natanz,

Iran [28]. Stuxnet specifically aimed to damage centrifuges in Natanz nuclear facility. The attack demonstrated the potential for physical damage and disruption through cyber means, highlighting the vulnerabilities of ICSs [27].

Another notable attack is the Shamoon malware that targeted the oil and gas sector in Saudi Arabia in 2012. It was designed to destroy data and disrupt operations. The attack aimed to cause significant financial and operational losses by rendering the targeted systems inoperable. Shamoon raised concerns about the potential impact of cyber-physical attacks on critical infrastructure [29, 30].

The first major attack targeting the power grid was BlackEnergy in 2015 [31]. This is an attack on a power utility in western Ukraine, resulting in a widespread blackout. The attack highlighted the vulnerability of power grids and the potential for cyber-physical attacks to impact not only information systems but also physical infrastructure [32].

Another attack on the Ukrainian power grid is CrashOverride, discovered in 2016 [32], which targeted transmission substations in Ukraine. The malware demonstrated the potential to disrupt power grid operations by manipulating control systems. The attack emphasized the need for robust security measures to protect critical infrastructures [32].

In 2017, Shamoon 2 resurfaced with attacks targeting state agencies and private sector companies in Saudi Arabia. Similar to its predecessor, Shamoon 2 aimed to cause data destruction and disruption. The attack highlighted the persistent threat posed by cyber-physical attacks to critical infrastructure [33].

Another notable attack in 2017 was Trisis/Tritonthat targeted a petrochemical plant and aimed to sabotage operations, potentially triggering an explosion. This attack demonstrated the potential for cyber-physical attacks to cause physical harm and posed a significant risk to industrial facilities [32].

In addition to the earlier attacks, Ukraine has continued to face persistent cyber threats in recent years. In 2022, a new variant of the Industroyer malware, known as Industroyer2, was deployed against the power grid but was detected and contained before causing major disruption [34]. In 2023, a large-scale cyberattack targeted Kyivstar (Ukraine's largest mobile telecommunications), disrupting mobile and internet services and affecting emergency systems [35]. Similar attacks continued in 2024 and 2025, with thousands of incidents reported annually, mainly targeting critical

infrastructure [14].

2.2 IEC 61850 Substation Components and Architecture

IEC 61850 is a widely adopted international standard for the design and implementation of communication networks in electrical substations. It offers a standardized approach for integrating and ensuring interoperability among substation automation systems, enabling efficient and reliable monitoring and control of the smart grid's substations. This section presents an overview of the key architectural elements and components defined by IEC 61850, emphasizing their role in enhancing the functionality, reliability, and scalability of modern digital substations [36, 37].

2.2.1 Components of IEC 61850 Substations

This section introduces the main components in IEC 61850 Substations.

2.2.1.1 Intelligent Electronic Devices

Intelligent Electronic Devices (IEDs) are fundamental components in IEC 61850-based substations. IEDs, such as protection relays, controllers, and Merging Units (MUs), play a crucial role in acquiring, processing, and transmitting data within the substation. IEDs are equipped with standardized communication interfaces compliant with IEC 61850, ensuring seamless integration and interoperability among various substation elements. By enabling real-time monitoring, control, and protection functions, IEDs contribute significantly to the reliability, responsiveness, and overall efficiency of modern digital substations [36].

Protection IEDs are responsible for detecting and responding to faults and abnormal operating conditions within the grid. They continuously monitor parameters such as current, voltage, and frequency and compare them against predefined thresholds to determine the appropriate protective and remedial actions. Common protection functions include overcurrent protection, differential protection, distance protection, and transformer protection. These IEDs play a crucial role in ensuring the safety and stability of the smart grid by initiating timely control actions to isolate faulty components and prevent cascading failures [36, 38].

Control IEDs are responsible for executing control actions based on commands received from the station-level systems. They perform critical functions such as opening or closing circuit breakers, controlling tap changers in transformers, and adjusting power factor correction devices. Control IEDs enable remote control and automation capabilities, improving the operational efficiency of the substation, contributing to improved system responsiveness and reduced downtime [36, 39].

Measurement IEDs are responsible for acquiring voltage, current, power, energy, and harmonics measurements. this type of IEDs plays a vital role in assessing the operational state and condition of the electrical system, facilitating maintenance, planning, and system optimization [36, 39]. By delivering precise real-time measurements, measurement IEDs contribute to the overall reliability and efficiency of substation operations.

2.2.1.2 Communication Networks

IEC 61850 defines a standardized communication architecture that facilitates efficient and interoperable data exchange within substations. At its core, the protocol utilizes Manufacturing Message Specification (MMS) to enable structured and reliable communication between IEDs and other substation devices. The standard promotes the adoption of Ethernet-based communication networks, offering high-speed and reliable communication channels within the substation. The adoption of Ethernet-based networks enhances the scalability, flexibility, and interoperability of substation automation systems. Additionally, IEC 61850 supports the use of GOOSE messaging for fast and reliable transmission of status and control information between IEDs. GOOSE messaging is particularly suited for time-critical protection and control functions, significantly improving the responsiveness and robustness of substation communication infrastructure [36, 40].

2.2.2 Architectural Design of IEC 61850 Substations

The architecture defined in IEC 61850 provides a standardized hierarchical framework for the deployment and organization of substation components. It consists of multiple communication levels, i.e., station, bay, and process, each with its specific role and equipment [36, 41].

The station level is at the top of the hierarchy, it is responsible for various control and monitoring functions. The station level includes the Human–Machine Interface (HMI) systems, Substation

Automation System (SAS) servers, and interfaces to external systems such as SCADA systems. SAS servers collect and process data from IEDs and other devices, enabling advanced automation and control functions [36, 41].

The bay level comprises equipment grouped by functional sections or bays, such as control breakers, disconnectors, transformers, and measurement devices. IEC 61850 enables communication and interoperability between these devices using standardized protocols and data models. Each bay typically has a bay controller, which acts as a gateway for communication between the devices within the bay and the station level [36, 41].

At the lowest tier, the process level includes the primary equipment responsible for power transmission and distribution, such as switchgear sensors and actuators, trip coils, etc. These devices are controlled and monitored by the bay-level equipment and interact with the substation automation system through IEDs. IEC 61850 facilitates the exchange of measurement, status, and control information between the process level devices and other components within the substation [36, 41].

2.3 Standardization Efforts

In this section, we delve into some of the standards shaping the cyber-physical infrastructure of substations within the smart grid ecosystem, with a particular focus on the IEC 61850 [36] and IEC 62351 [42] standards, both of which are integral to enhancing cybersecurity and operational efficiency in substation automation.

2.3.1 IEC61850 Standard

The IEC 61850 standard [36] is a comprehensive framework for the design of electrical substation automation. It covers various aspects of substation automation and communication, including the following components.

2.3.1.1 Communication Networks in Substations

Communication networks in substations is a fundamental aspect of the IEC 61850 standard, primarily addressed in several parts of the standard. This component focuses on the protocols,

network architectures, and data exchange methods necessary for effective communication within electrical substations. We briefly present the details and relevant parts of IEC 61850 that pertain to this aspect in the section below.

- **IEC 61850-5 - Communication Requirements for Functions and Device Models [43]:** This part details the communication requirements for substation functions and the models of the involved devices. It defines how devices communicate, the types of exchanged data, and the performance requirements for these communications.
- **IEC 61850-7 - Basic Communication Structure for Substation and Feeder Equipment [44]:** Parts 7-1, 7-2, and 7-3 define the foundational communication and data modeling framework. Part 7-1 outlines the overall structure and principles, Part 7-2 specifies the abstract communication service interface (ACSI) used to facilitate interaction between applications and devices, and Part 7-3 describes the standardized data classes that represent the information exchanged within the substation automation system.
- **IEC 61850-8 - Specific Communication Service Mapping [45]:** The 8-x series, especially part 8-1, maps the abstract services defined in the 7-x series onto specific communication protocols like MMS. This part is critical for implementing the actual communication protocols that will be used in the substation networks.

2.3.1.2 Interoperability and System Integration:

IEC 61850 addresses the challenge of integrating heterogeneous systems and equipment from various vendors. It establishes a standardized set of protocols that ensure seamless interaction and functionality across diverse substation components. This interoperability is a key factor in maintaining system resilience and reducing vulnerabilities. In what follows, we briefly present the details and relevant parts of IEC 61850 that pertain to this aspect.

- **IEC 61850-6 - Configuration Language for Communication in Electrical Substations Related to IEDs [46]:** This part introduces the Substation Configuration Language (SCL), essential for defining and configuring the communication relationships and data flow between IEDs, ensuring interoperability.

- **IEC 61850-9-x - Sampled Values over Serial Unidirectional Multidrop Point-to-Point Link [47]:** Parts 9-1 and 9-2, which focus on the communication of sampled values, are crucial for integrating high-speed data exchange systems, such as those used in protection and measurement applications.

2.3.1.3 Real-Time Data Exchange:

IEC 61850 emphasizes the use of communication protocols that support rapid and deterministic data transmission, which is essential for real-time monitoring, control, and protection in substation environments. This capability is particularly critical for ensuring timely detection and response to operational anomalies and potential cyber threats. We briefly present the details and relevant parts of IEC 61850 that pertain to this aspect in the section below.

- **IEC 61850-7-2 - Basic Communication Structure - Abstract Communication Service Interface (ACSI) [48]:** This part defines the services used for data exchange between IEDs, including those needed for real-time data exchange and operation.

- **IEC 61850-8-1 - Specific Communication Service Mapping [45]:** This part is crucial for real-time data exchange as it specifies how the abstract services defined in part 7-2 are mapped onto actual network protocols, such as mappings to MMS, ISO/IEC 9506-1, ISO/IEC 9506-2, and to ISO/IEC 8802-3, enabling real-time communication.

- **IEC 61850-9-2 - Sampled Values over ISO/IEC 8802-3 [47]:** This part specifies the transmission of time-critical measurement data using Sampled Values (SV) in compliance with ISO/IEC 8802-3. It is particularly relevant for real-time applications that require high-speed, deterministic communication of digitized analog signals, such as current and voltage measurements, for protection, control, and monitoring functions in substations.

- **IEC 61850-90-5 - Use of IEC 61850 to transmit synchrophasor information according to IEEE Standard C37.118 for Synchrophasors (C37.118) [49]:** IEC 61850-90-5 is an extension of the IEC 61850 standard, focusing on integrating renewable energy sources and Distributed Energy Resources (DERs) into the power grid. It introduces Routable Sampled

Values (R-SV) and Routable Generic Object Oriented Substation Event (R-GOOSE) for efficient data exchange over Internet Protocol (IP) networks. These adaptations facilitate real-time monitoring and control across dispersed energy resources, ensuring interoperability and enhanced cybersecurity in the smart grid infrastructure. This part of the standard is crucial for the seamless integration of renewable energy, supporting a sustainable and resilient power system.

Each of these parts plays a vital role in ensuring that the communication networks in substations are robust and capable of handling complex data exchanges. These parts also ensure interoperability and efficient real-time operations. They collectively provide the guidelines and specifications necessary for the design, implementation, and integration of advanced communication systems in modern electrical substations.

2.3.2 IEC 61850 Communication Protocols

IEC 61850 standard aims to provide a comprehensive framework for the design and implementation of control, protection, and monitoring systems in substations. This standard encompasses numerous communication protocols to ensure the safe and efficient transfer of measurement and control signals.

2.3.2.1 Manufacturing Message Specification

The Manufacturing Message Specification (MMS) plays a central role in the IEC 61850 standard, enabling the transfer of real-time operational data and control signals between interconnected devices. MMS operates on the application layer of the OSI model, providing a mechanism for applications to exchange complex data structures [36, 50]. In the IEC 61850 context, MMS is employed for data exchange between power system automation devices, facilitating the communication of measurement and control signals. It provides a standardized means of communication, ensuring the accurate and timely transfer of data, crucial for the management and operation of electrical substations.

2.3.2.2 Generic Object Oriented Substation Event

Generic Object Oriented Substation Event (GOOSE) is a novel mechanism introduced in IEC 61850, designed to replace traditional hardwired control logic with more flexible, software-based solutions. Operating directly on the Ethernet level, GOOSE enables real-time peer-to-peer communication between IEDs [36, 50].

GOOSE messages are used for fast transfer of event-triggered status data and control commands. These messages, unlike client-server communication, are broadcast directly to all devices in a substation network. This mechanism significantly reduces the latency in control command execution, making it suitable for critical applications that require real-time performance.

2.3.2.3 Sampled Values

The Sampled Values (SV) protocol is a core component of the IEC 61850 standard, designed for high-speed transfer of digitized analog data, primarily used for protection and measurement applications [36, 50]. The Sampled Values (SV) protocol enables the digitization and distribution of current and voltage measurements. This mechanism enables the replacement of conventional copper wiring with fiber-optic links, reducing costs and improving flexibility and reliability. The SV protocol supports multicast communication to ensure that multiple devices can receive the sampled data simultaneously. This capability is essential for synchronized protection schemes and power quality monitoring.

2.3.2.4 Routable GOOSE

Routable GOOSE (R-GOOSE) is an extension of the conventional GOOSE protocol, designed for the transmission of GOOSE messages beyond the local substation network. This capability enables Wide Area Network (WAN) communication, facilitating protection, control, and monitoring applications on geographically dispersed substations [49].

R-GOOSE achieves this extended functionality by encapsulating GOOSE datasets within IP/User Datagram Protocol (UDP) packets, allowing the messages to be routed across multi-hop network paths. By leveraging standard IP-based infrastructure, R-GOOSE offers a scalable and cost-effective

solution for wide-area substation communication.

2.3.2.5 Routable Sampled Values

Routable Sampled Values (R-SV) is an extension of the SV protocol, which allows for the transmission of SV messages over a WAN. R-SV is primarily used for wide area monitoring applications, where high-resolution measurements from multiple substations need to be centralized for data analysis and system monitoring [49]. Like R-GOOSE, R-SV utilizes IP/UDP encapsulation to route SV datasets over a WAN.

2.3.3 IEC 62351 Standard

The IEC 62351 standard [42] addresses the cybersecurity requirements of communication protocols used in power system operations. It provides security enhancements for the IEC 61850 standard for substation automation, in addition to IEC 60870-5 series. IEC 62351 is organized into multiple parts, each targeting a specific aspect of communication security within power systems, such as authentication, encryption, access control, and secure data exchange. We discuss below the parts that are particularly relevant to the scope of this thesis.

- **IEC 62351-6 - Security for IEC 61850:** IEC 62351-6 is an integral part of the IEC 62351 series [51], specifically designed to bolster the security of IEC 61850, which is central to substation automation and power utility communications. This segment of the standard is focused on mitigating cybersecurity vulnerabilities inherent in the communication protocols encompassed by IEC 61850, such as MMS, GOOSE, and SV. It plays a pivotal role in ensuring the secure operation of IEDs within substations.

  A key emphasis of IEC 62351-6 is on ensuring the authentication and integrity of data exchanged between IEDs. It defines mechanisms to verify that transmitted data originates from a legitimate source and remains unaltered during transmission, which is crucial for the reliable functioning of power systems. Additionally, the standard outlines the use of encryption technologies to protect sensitive data in transit within substation networks. This measure is particularly important for preventing unauthorized access and eavesdropping in network

environments that may not be properly secured.

Another critical aspect of IEC 62351-6 is the effective management of cryptographic keys used for encryption and authentication. The standard provides protocols for key generation, distribution, rotation, and revocation, all of which are vital for ensuring the integrity and confidentiality of encrypted communications over time. In addition, it provides guidelines for establishing secure communication channels between components of the substation automation system. These guidelines emphasize the use of secure transport protocols and robust authorization mechanisms to prevent unauthorized access, data interception, and other cyber threats within substation networks.

IEC 62351-6 also integrates established cybersecurity best practices into substation automation systems. This includes carrying out periodic security reviews, performing vulnerability assessments, and implementing a well-defined security guidelines and protocols. A key feature of the standard is its emphasis on ensuring that the recommended security enhancements are compatible with existing IEC 61850-based infrastructures. This compatibility enables the gradual and non-disruptive integration of advanced security measures, allowing utilities to strengthen their cybersecurity posture without requiring major architectural changes to current systems.

The standard is designed to bolster the resilience of substation automation systems against a wide array of cyber threats, including both external attacks and internal vulnerabilities. This resilience is achieved through a combination of technological solutions and procedural guidelines. Recognizing the dynamic nature of cybersecurity threats, IEC 62351-6 is adaptable, allowing for updates and revisions in response to new types of cyber threats and vulnerabilities as they emerge.

- **IEC 62351-7 - Network and System Management (NSM) Data Object Models:** IEC 62351-7 is an essential part of the IEC 62351 series [52]. It is dedicated to enhancing the security of NSM within power systems. This part of the standard is particularly focused on establishing robust security protocols and practices for the management of networks and systems in power utility environments. It encompasses the security of devices, communication infrastructure,

and the software applications that operate within these networks.

A key feature of IEC 62351-7 is the definition of data object models specifically designed for NSM. These models provide a standardized framework for representing various elements involved in network and system management. This standardization is essential for enabling secure, consistent, and interoperable monitoring and control of network elements. By ensuring the integrity, availability, and confidentiality of critical operational data, these object models support enhanced visibility, diagnostics, and threat detection across utility communication networks.

The standard also addresses the security of protocols used for monitoring and control of power system networks. It emphasizes the protection of data involved in critical network management functions—such as performance monitoring, fault diagnosis, and configuration management—against unauthorized access, tampering, and other forms of cyber intrusion. Securing these protocols is essential to maintaining the operational integrity, reliability, and resilience of power system communications and infrastructure.

Authentication and authorization mechanisms also receive significant attention in IEC 62351-7. The standard underscores the importance of robust procedures to prevent unauthorized access to network management tools and resources. This is a critical measure to protect against potential cybersecurity threats that could disrupt power system operations.

Furthermore, IEC 62351-7 provides guidelines for securing the communication channels used for NSM activities. It advocates for the use of encryption and secure protocols to protect data exchanges between network management systems and the devices they manage. This protection is essential for preventing eavesdropping and data breaches in communication networks.

The standard also delves into the detection of security incidents and anomalies within the network management context. This aspect is crucial for identifying potential cybersecurity threats and enabling prompt and effective responses to mitigate these risks.

Another important consideration in IEC 62351-7 is the integration of security measures with existing power system communication infrastructure. The standard is designed to enhance the security of existing systems without necessitating complete system overhauls, thereby

allowing for a more practical and cost-effective approach to improving cybersecurity. Finally, IEC 62351-7 includes provisions for compliance with established security policies and for the auditing of network management activities. These provisions help ensure that NSM activities are aligned with defined cybersecurity policies, and that they can be systematically audited and evaluated for effectiveness and regulatory compliance.

- **IEC 62351-10 - Security Architecture Guidelines:** IEC 62351-10 [53], is dedicated to establishing a security architecture for power system communication networks. This part of the standard plays a pivotal role in guiding the development and implementation of security measures to protect the critical infrastructure of power utilities.

  The primary focus of IEC 62351-10 is to provide a structured methodology for designing and implementing security architectures within power system communication networks. It outlines a detailed process for identifying critical assets, assessing potential threats and vulnerabilities, and defining security requirements to mitigate associated risks. The standard emphasizes that effective security strategies must consider the unique operational constraints of power system communication networks, such as real-time performance requirements, deterministic communication behavior, and the critical nature of uninterrupted service.

  A central component of IEC 62351-10 is its emphasis on risk assessment and management. The standard provides guidance for evaluating the risks posed to various network components and communication protocols. This risk evaluation serves as a foundation for determining the most appropriate and cost-effective security controls. By systematically identifying and prioritizing risks, utilities can allocate resources more efficiently and focus their efforts where they are most needed.

  IEC 62351-10 advocates for a layered security strategy. This strategy involves implementing multiple layers of security controls throughout the network. This ensures redundancy in protection, i.e, if one layer fails, the others continue to provide the necessary protection. This layered approach enhances the overall resilience of the system against various types of cyber threats.

The development and enforcement of security policies and procedures are also key components of IEC 62351-10. These policies cover various security domains, such as access control, data protection, incident response, and recovery planning. Establishing clear security policies is essential for maintaining consistent security practices across the organization and for responding effectively to security incidents.

IEC 62351-10 also highlights the requirement of regular security audits and compliance checks. These audits are essential for ensuring that the network adheres to the established security policies. Regular audits help in identifying security gaps and areas for improvement, ensuring that the security measures remain effective over time.

Lastly, IEC 62351-10 emphasizes the need for adaptability of the security architecture to the evolving cybersecurity landscape. The standard promotes flexible frameworks that incorporate new security technologies and best practices as threats evolve. This adaptability is critical for maintaining a proactive defense posture and for ensuring long-term protection against emerging vulnerabilities and threat vectors.

2.4 Security Assessment of IEC 61850 Protocols

The IEC61850 standard primarily focuses on performance requirements to ensure real-time communication in substation automation systems. However, it does not include specific provisions for security requirements. This section explores the security of the IEC 61850 protocol and the gaps in substation security.

2.4.1 Security Assessment of IEC 61850

While the IEC 61850 standard prioritizes high-performance and real-time communication for substation automation systems, this emphasis has come at the cost of integrated cybersecurity mechanisms. Specifically, IEC 61850 does not natively support critical security features such as encryption, authentication, or intrusion detection systems. The absence of these built-in protections introduces notable vulnerabilities, leaving systems susceptible to a wide range of cyber threats [54].

The security implications of these vulnerabilities are significant, particularly in terms of the

fundamental cybersecurity principles of availability, integrity, confidentiality, and non-repudiation. Various types of cyberattacks can exploit these weaknesses, potentially compromising the reliability and safety of power system operations. Common categories of attacks targeting IEC 61850-based systems include, but are not limited to [42]:

- **Denial of Service (DoS):** These attacks can disrupt the availability of the system, hindering its ability to perform critical functions in real-time.
- **Unauthorized Access to Information:** Attackers may gain unauthorized access to sensitive data, compromising the confidentiality and integrity of the system.
- **Unauthorized Modification or Theft of Information:** The integrity of data can be compromised through unauthorized changes or theft, leading to operational disruptions and misinformation.

To address these security gaps in IEC61850, the IEC62351 standard provides a suite of security recommendations specifically designed to enhance the protection of substation automation systems [42]. These recommendations are designed to fill the gaps in the IEC 61850 standard. However, the effectiveness of these recommendations depends on their proper evaluation and implementation. Ensuring end-to-end security in IEC 61850 systems requires a thorough assessment of how these security controls interact with system components and how resilient they are against advanced and evolving cyber threats.

2.4.2 Substation Security Gap Analysis

Analyzing the cyber-physical impacts of cyberattacks on critical infrastructure, including smart grids, remains a significant challenge. This difficulty arises primarily from the high costs, safety concerns, and difficulty of conducting such assessments on operational systems. The high cost and logistic challenges of such testing are driven by the need for specialized equipment and the potential damage to sensitive physical components if testing is performed on real systems. To effectively understand the interdependencies between the cyber and physical systems of a smart grid, it is essential to replicate cyberattack scenarios within a real-time emulated or simulated testbed environments that accurately capture the behavior of realistic systems.

Table 2.1 summarizes existing work in this area. However, many of the proposed solutions face limitations in terms of real-time applicability, scalability, and practical deployment. Therefore, there is a clear need for the development of advanced testbeds capable of accurately emulating smart grid operations in the presence of cyberattacks.

As smart grid architectures continue to evolve, the security landscape grows increasingly complex due to the integration of new elements, protocols, and services. While the IEC 62351 standard introduces a set of security recommendations aimed at detecting and mitigating cyberattacks, ensuring end-to-end protection requires rigorous analysis and systematic implementation. Although substantial research has been undertaken to strengthen the security posture of IEC61850, enumerated in Table 2.1, further investigation is essential to address unresolved challenges in achieving robust cyber-physical security.

One critical area requiring deeper exploration is the standard's recommendation for the use of NSM. Although IEC 62351 promotes the use of NSM for security monitoring, it provides limited guidance on how these NSM objects can be effectively utilized to generate actionable insights. This gap underscores the need for further research to operationalize NSM capabilities for real-time threat detection and system diagnostics.

Another key recommendation is the adoption of Deep Packet Inspection (DPI) technologies. DPI offers the potential to monitor various types of data, including access to physical data such as measurement and control signals. This capability could significantly enhance security monitoring within substations, providing a more granular and comprehensive view of network traffic and activities.

2.5 Related Work

This section presents related studies relevant to the scope of this thesis.

2.5.1 Smart Grid Co-simulation

Smart grid co-simulation using HIL has gained significant popularity in recent years. The literature is rich with approaches that combine various simulation techniques to analyze different aspects

Table 2.1: Comparative examination of IEC 61850 substation related literature.

Testbed														
Ref	**Year**	**Co-Sim**	**HIL**	**Real-Time**	**Network Simulator**	**Network Emulator**	**Virtual IEDs**	**Physical IEDs**	**GPS**	**Power Simulator**	**IEC 61850 Emulation**	**Time-Sync Traffic**	**Real-World Attack Scenarios**	**Scalable**
[55]	2025	•	•	•	•	•	•		•	Multiple	•	•	•	•
[56]	2012	•			•		•		•	PSLF	•	•		
[57]	2015	•	•	•	•		•			OPAL-RT				
[58]	2025	•	•	•	•		•	•	•	RTDS	•	•	•	•
Our testbed	2018	•	•	•		•	•	•	•	OPAL-RT	•	•	•	•

Intrusion Detection Systems (IDS)															
Ref	**Year**	**NSM**	**DPI**	**Rule-Based**	**ML**	**DL**	**Targeted Protocols**	**Distributed**	**Centralized**	**Attack Surface**	**Adaptability to-New Threats**	**Real-Time Testbed Validation**	**Accuracy / Metrics**	**Scalability**	**Targeted System**
[59]	2013		•	•	•		IEC 61850	•		Limited	•	•	98.30%		Synchrophasor
[60]	2014		•	•	•		IEC 61850		•	Limited			90%		Substation
[61]	2017		•			•	ICS Protocols		•	Large	•	•	not reported	•	ICS Network
[62]	2016		•	•	•		IEC 61850		•	Limited		•	not reported		Substation
[63]	2016		•			•	IEC 61850		•	Limited		•	87%		Substation
[64]	2015		•	•	•		IEC 61850		•	Limited			93.21%		Substation
[65]	2014		•		•		ICS Events		•	Limited			not reported		Substation
[66]	2014		•	•			IEC 61850		•	Limited			not reported		Substation
[67]	2014		•	•			IEC 61850		•	Limited			not reported		Substation
[68]	2015		•	•	•		GOOSE		•	Limited			not reported		Substation
[69]	2012		•	•			IEC 61850			None			not reported		Substation
[70]	2016		•	•			IEC 61850		•	Limited			not reported		Substation
[71]	2025		•			•	GOOSE	•		Limited	•		99.80%		Substation
[72]	2008	•			•		General IT		•	Limited			not reported		General
[73]	2013	•			•		General IT		•	Limited			98%		General
[74]	2014	•			•		General IT		•	Limited			97.30%		General
[75]	2015	•		•			General IT		•	Limited			higher acc	•	General
[76]	2012	•		•	•		General IT		•	Limited			100%		Substation
[77]	2009	•		•			General IT		•	Limited			90%		General
Our system	2025	•	•	•		•	IEC 61850	•	•	Large	•	•	99.9%	•	Substation

of the smart grid. A comprehensive overview of such efforts can be found in a recent survey on smart grid cyber-physical testbeds [78]. One of the earliest contributions in this domain was presented by Lin et al. in [56], where the authors integrate a software-based power system simulator (PSLF) with a network simulator (NS2). Similar approaches include the work by Bian et al. in [57], where a co-simulation framework connects a real-time power system simulator (OPAL-RT) with a software network simulator using Riverbed Modeler.

A notable contribution is the BUTENET testbed proposed in [55], which introduces a modular and extensible co-simulation environment combining physical, virtual, and emulated components to assess security, interoperability, and training scenarios in smart grid transmission networks. The testbed supports a variety of protocols, such as IEC 61850, IEC 60870, DNP3, Modbus, and OPC UA, and features integration with a Digital Twin and Cyber Arena for attack modeling. However, the use of resource-constrained hardware like the Raspberry Pi 3B+ for high-speed protocol simulation poses performance limitations under heavy traffic loads. Another testbed was introduced in [58] to emulate a realistic IEC 61850 substation environment through the integration of industry-grade hardware components. The hardware setup includes both real and simulated IEDs, Remote Terminal Units (RTUs), GPS-synchronized time sources, and circuit breakers. It incorporates a real-time digital simulator to facilitate HIL operation, enabling accurate modeling of both electrical and communication layers. The architecture supports experimentation with cyber-physical interactions under time-critical conditions and provides a programmable attacker module to inject GOOSE and SV-based attack scenarios. Unlike simulation-only frameworks, this testbed enables the evaluation of protection schemes, timing behavior, and system resilience with high fidelity. The modular design and detailed instrumentation allow researchers to monitor end-to-end latencies and evaluate the performance of substation automation functions under attack or fault conditions. While currently used with a rule-based NIDS for initial testing, the primary strength of this testbed lies in its hardware realism, timing precision, and capacity for in-depth CPS experimentation. However, it lacks integrated virtual network emulation or scalable co-simulation capabilities, which limits its suitability for large-scale smart grid communication scenarios.

In contrast, our approach is distinguished by the capabilities of its virtualization environment for communication network emulation. The proposed virtualized environment offers a scalable and

flexible framework to simulate realistic smart grid communication networks. Leveraging OpenStack, we are able to define networks with varying levels of complexity to meet the requirements of diverse smart grid simulation scenarios. Furthermore, the virtualization platform enables the manipulation of communication traffic and supports the execution of various tests and cyberattacks on that traffic. Unlike simulation tools such as Riverbed Modeler—which restrict communication across different virtual local area networks and lack support for multiple gateways interfacing with physical hardware—our environment supports Ethernet-based integration with real power hardware while overcoming these limitations.

2.5.2 Network Monitoring in CPS

Simple Network Management Protocol (SNMP) is among the most recommended protocols for implementing DOs in NSM [15]. Similar to TCP/UDP Management Information Bases (MIBs), the NSM DOs are deployed as SNMP MIBs in [79].

Though some techniques in the literature utilize SNMP MIBs to detect cyberattacks, they often overlook the NSM data objects defined by IEC 62351-7 as a valuable data source for attack detection. This gap leaves room for further research on the suitability and effectiveness of these NSM data objects for enhancing security monitoring in power systems. A machine learning-based algorithm using Support Vector Machine (SVM) is presented in [72], where the collected data is employed to detect flooding attacks. This work suggests incorporating SNMP MIBs into an intrusion detection system (IDS), though the proposed techniques were not adequately integrated to achieve a comprehensive solution. In a subsequent study [73], the same authors use the C4.5 algorithm in place of SVM to improve the detection performance for flooding attacks. Rule mining techniques are also applied to extract classification rules. Additionally, a Protocol Independent Detection and Classification (PIDC) system is introduced in [74], which uses SNMP MIB data to identify Distributed Reflection Denial of Service (DRDoS) attacks—similar in scope to the attacks studied in [72].

In another study, Choi et al. [76] demonstrate the use of NSM data for detecting cyberattacks in substations. They develop a decision tree to identify two attack types using attributes extracted from NSM data. The attacks had clearly observable impacts on NSM data objects, allowing some

algorithms to achieve a 100% detection rate. However, their method does not address more sophisticated attacks whose signatures are not reflected in NSM data objects. Other studies, such as [80,81], have analyzed or implemented attacks targeting IEC 61850 substation protection systems but did not evaluate real-time detection capabilities.

On the other hand, Yoo and Shon [60] apply a combination of Expectation Maximization, Local Outlier Factor (LOF), and SVM for anomaly detection on IEC 61850 GOOSE and MMS messages. They use SVM to learn the normal behaviour of IEC 61850 packets gathered from a real IEC 61850 substation, using a single packet model as a proof of concept. After learning normal behaviour, packets that are found to deviate significantly from the established normal behaviour are considered anomalous. However, Yoo and Shon believe the false positive rate of the proposed approach to be too high. They also lacked sample attack packets for use in their experiments, preventing them from evaluating the false negative rate of their approach.

Feng, Li, and Chana [61] propose an anomaly detection method for ICS digital communication networks that uses a combined signature identification scheme and Long Short-Term Memory (LSTM) model for traffic anomaly classification. The trained LSTM takes advantage of the predictable and regular nature of communication traffic in ICS domains, which improves the likelihood of accurate predictions by the LSTM. Packet signatures that fail the acceptable signature identification check or that fall outside the most probable signatures predicted by the LSTM are considered anomalies. The experimental dataset used by Feng et al. includes both real operation of a gas pipeline system and simulated cyberattack data consisting of malicious ICS protocol payloads and DoS. The results show a better F1 score for the proposed anomaly detection method when noise data is intentionally introduced into the training dataset, with the reduction in false positives making up for the rise in false negatives. Their work highlights the advantage of deep learning approaches such as LSTM in ICS contexts, where traffic behaviour is less varied compared to traditional Information Technology (IT) environments.

Cui-Mei [77] proposes an approach to detect traffic flooding attacks using a two-level SVM approach applied on SNMP MIB data. The first level identifies attack traffic from normal traffic with a one-class SVM. The second level uses a multi-class SVM to classify the type of attack as either TCP-SYN flooding, UDP flooding, or ICMP flooding. The SVM was trained on 13 MIB

objects across the IP, TCP, UDP, and ICMP MIB groups that are part of standard SNMP. This work shows promise in using SNMP MIB data for cyberattack detection, although it does not consider ICS protocols and only detects flooding attacks.

Cerroni et al. [75] propose a Network Intrusion Detection system (NIDS) that uses peer-to-peer unsupervised data clustering of SNMP data that is collected from multiple monitoring stations. The proposed NIDS has a central monitor that collects standard SNMP MIB object values from distributed monitor nodes that each perform their own clustering based on data they observe, then separates the data into cluster partitions via k-means clustering. Simulated HTTP traffic, designed to match real network during normal and attack scenarios, is transmitted across their experimental test network, to be observed by the central monitor over SNMP at regular intervals. The experimental results of the NIDS proposed by Cerroni et al. show that the distributed clustering approach has higher accuracy than a purely centralized clustering approach and a much lower false positive rate compared to the centralized approach. Though the work of Cerroni et al. does not consider a smart grid network environment, it does show the potential for analytics performed on SNMP data to be useful for cyberattack detection.

Despite these contributions, the existing works on IEC 61850 digital substation security have several gaps which we aim to address. The gaps we seek to address can be summarized in three points: (i) the absence of a study on the use of NSM as specified by IEC 62351-7, to detect cyberattacks targeting the communication network of the IEC 61850 digital substation, (ii) a need of a comprehensive and realistic cyber-physical study on the impact analysis of cyber-physical attacks targeting the IEC 61850 substation, and (iii) the lack of experimental evaluations on real-time performance of proposed substation attack detection systems to ensure that they meet IEC 61850 operational performance requirements.

2.5.3 Deep Packet Inspection in CPS

Several studies have proposed the design of Intrusion Detection Systems (IDS) for substations based on the IEC 61850 standard. In [62], Yang et al. introduced a multidimensional IDS framework capable of analyzing physical, behavioral, and access control aspects of IEC 61850 substations. Their design relied on predefined rules and protocol-based detection techniques, achieving

full detection of 23 predefined rule-based attacks on a cyber-physical testbed. However, their approach is limited to these predefined attacks and fails against unknown or novel anomalies, as it lacks adaptability beyond the static rule sets.

In a similar context, Kwon et al. [64] proposed a behavior-based IDS that analyzed statistical network features and metrics extracted from IEC 61850 GOOSE and MMS traffic. Their system achieved a high detection accuracy of 99% across 27 scenarios but was primarily evaluated in static environments and cannot be generalized beyond the observed attack signatures. Yang et al. in [59] extended this idea to the C37.118 protocol, focusing on Man-in-the-Middle and Denial-of-Service attacks. Their approach combined access control and protocol-based whitelisting with Deep Packet Inspection (DPI) to define behavior-based rules. While their method effectively detected known threats, its generalization to new or distributed attacks was limited.

Behavioral analysis-based IDS approaches have also been explored by Hink et al. [65], where they evaluated several classifiers across five cyber-physical disturbance scenarios. While they reported strong classification accuracy, their approach does not incorporate substation-wide cooperation, which is essential for detecting coordinated attacks across distributed infrastructure.

Hong et al. [66] proposed an integrated anomaly detection framework for multiple IEC 61850 communication protocols. However, their approach mainly relied on protocol behavior and packet filtering, ignoring packet content. In an extension to their first work [67], they proposed detecting anomalies in multicast messages, such as GOOSE and SV, but their approach focused on packet characteristics without using payload data during detection. Yoo et al. [68] employed SVMs to detect anomalies by analyzing IEC 61850 packet behavior, achieving high accuracy, but face challenges in differentiating between genuine system faults and coordinated cyberattacks.

DPI solutions have emerged to address limitations in packet-level visibility. Lee et al. [69] developed a DPI-based packet analyzer for GOOSE, SV, and MMS traffic, capable of outperforming Wireshark in analysis speed. However, their framework was limited to inspection and did not support anomaly detection. On the other hand, Formby et al. [70] employed fingerprinting techniques and DPI to detect tampering in substations with 99% fingerprinting accuracy. However, their system lacked integration with real-time detection logic.

Valdes et al. [63] applied unsupervised learning for anomaly detection in IEC 61850 substations,

reaching 92.06% detection accuracy. However, when tested on larger datasets, performance dropped to 71.11%, indicating limited scalability. These approaches largely focus on single-substation scenarios and lack mechanisms for verifying whether anomalies are widespread or localized.

Beyond detection, mitigation strategies such as the "Active Command Mediation Defense (A*CMD)" proposed in [82] aim to delay suspicious commands at substations, buying time for external monitoring systems to intervene. While this technique effectively reduces the physical impact of cyberattacks, it is reactive in nature and assumes the presence of a prior detection mechanism. Moreover, it relies on static time thresholds, which may not be optimal for all scenarios.

More recently, Dawli [71] proposed a lightweight IDS framework using DPI and hybrid deep learning models (CNN and TCN) for IEC 61850 GOOSE traffic. The approach emphasizes real-time detection with low-resource deployment on edge devices. Although the model demonstrates high detection accuracy, it lacks validation in real-time environments.

In this thesis, we present an integrated IDS framework that builds upon these earlier approaches by combining IEC 62351-90-2 compliant DPI with deep learning-based temporal anomaly detection and inter-substation fault propagation analysis. Our system is deployed across a real-time HIL co-simulation testbed. Our proposed framework detects delay-based and message-level anomalies in GOOSE and SV traffic by extracting timestamp, alivetime, and inter-arrival time features. Each substation agent employs deep learning models (GRU, LSTM, or Simple-RNN) to perform local detection. We then introduce a novel graph-based verification mechanism that analyzes fault propagation across substations. By verifying whether anomalies follow expected propagation sequences, the system distinguishes between actual system disturbances and cyberattacks with improved accuracy. Compared to earlier works, our approach is proactive, scalable, and capable of distributed detection and coordinated verification, addressing key gaps in current state-of-the-art IDS frameworks for smart grid substations.

Chapter Three

OpenStack-Based Evaluation Framework for Smart Grid Cybersecurity

The rapid evolution of traditional power systems into smart grids necessitates innovative platforms for evaluating new expansions and analyzing system behavior under both normal and adversarial conditions. Real-time HIL co-simulation environments have emerged as a powerful approach to study smart grid component interactions, assess functionality, and evaluate system security against a variety of cyber threats.

In this chapter, we present a HIL co-simulation testbed designed for smart grid security assessment. Our framework integrates OPAL-RT's Hypersim real-time power simulator with a virtualized communication network built using OpenStack [83, 84]. This architecture allows us to emulate realistic smart grid operations, simulate cyberattacks targeting both power and communication layers, and observe the resulting system responses.

Unlike traditional event-driven models, this setup provides a flexible and scalable environment capable of emulating large-scale systems such as WAMSs. It supports the simulation of various cyberattacks, including those targeting communication protocols, and facilitates a detailed security assessment of critical smart grid functions, including time synchronization and data integrity.

The main contributions of this chapter can be summarized as:

(1) The development of a cybersecurity-oriented smart grid HIL co-simulation framework.

(2) The coupling of real-time power grid simulation with a virtualized communication network using OpenStack.

(3) The evaluation of the presented testbed under different cybersecurity use cases.

The rest of this chapter is organized as follows. Section 3.1 introduces the co-simulation testbed. Section 3.2 presents our experimentation setup. Finally, cybersecurity case studies are presented in Section 3.3 and Section 3.4 concludes this chapter.

3.1 Smart Grid Testbed

The evolution of the smart grid requires new techniques for simulation and testing. Being composed of two main components: power and communication, there is a need to simulate both components and their interaction. The main challenge facing such a simulation is the different nature of the power grid and the communication network, and the absence of any simulation environments available that integrate both aspects of the smart grid. To perform this simulation, we follow a layered approach where we simulate different smart grid functionalities in parallel and integrate them into the same testbed. The bottom layer encompasses HIL simulation of the power grid real-time dynamics. On top of this layer, using network virtualization, we built the communication network to transmit power measurements and communicate control commands issued by the control centre. The control centre is located at the top layer and controls the smart grid through the virtual communication layer. Using this testbed, we are capable of performing our security assessments and performing the simulation of cyberattacks on the communication layer, which will impact both cyber and physical systems.

Figure 3.1 provides an overview of the co-simulation testbed architecture, which serves as the foundation for the experimental scenarios and attack use cases presented in this chapter.

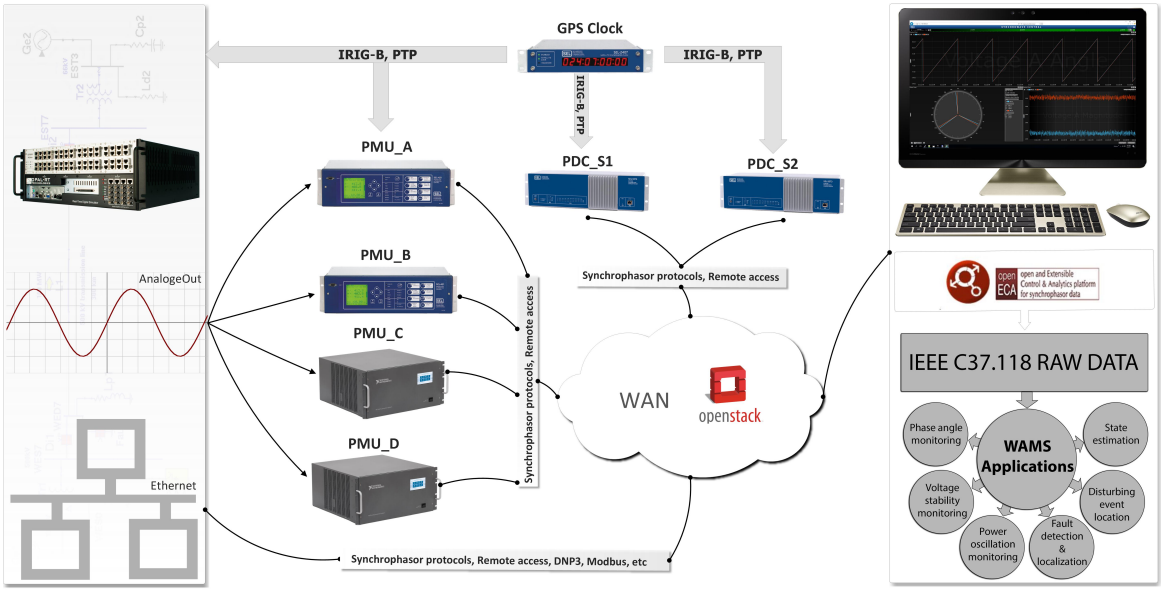


Figure 3.1: Smart grid HIL co-simulation framework.

3.1.1 Power Grid Simulator

3.1.1.1 OPAL-RT Simulator

The main component in our co-simulation environment is an OPAL-RT [83] digital runtime simulator that simulates the power grid in real time. The underlying Hypersim framework provides the user with capabilities to assign sensors to various components of the power model. Through those sensors, the user can gather measurements representing the current state of the power system. Using pre-specified communication protocols, we are capable of monitoring the power grid status through various measurements from different power buses in the simulated power model. The allocated sensors, on different components, enable the control of those components through external remote commands to trip a circuit breaker, increase/decrease generation, or disconnect a power load from the system. Moreover, the analog signals of the different components represent the current and voltage measurements at the different buses selected by the user. Such measurements are collected and sampled using C37.118 [85] traffic, emulating the behavior of real Phasor Measurement Units (PMUs). In addition, Hypersim is capable of simulating faults targeting the grid and enables studying their effects on voltage and current stability.

3.1.1.2 Available Hardware

The developed HIL testbed includes four phasor measurement units (PMUs) sourced from different vendors. These devices receive analog signals from the Hypersim simulator and convert them into digital synchrophasor data formatted according to the C37.118 standard. This data is sent to two physical phasor data concentrators (Phasor Data Concentrators (PDCs)): one serving as a local aggregator and the other as a regional collector. The local PDC consolidates PMUs measurements and forwards them upstream, while the regional PDC integrates data from multiple local PDCs and transmits it to the control centre. Additionally, two protective relays capable of operating in PMU mode are included. All devices are time-synchronized via a Global Positioning System (GPS)-based clock.

3.1.2 Communication Network Emulation

To emulate the communication network of the smart grid, we leverage OpenStack cloud computing platform [84]. OpenStack delivers various functionalities that enable us to establish a complex and scalable communication network suitable for addressing the communication requirements of the smart grid. Using OpenStack, we implemented a virtual network capable of interacting with the PMUs, PDCs, and control infrastructure. The virtualization environment provides flexibility in designing communication networks needed for testing a wide range of smart grid scenarios. The virtualization environment is connected to the power grid simulator and the available hardware using Ethernet. The transfer of PMU measurements along with different control commands takes place in a virtual environment. The collected measurements, obtained form the power grid simulator, are transmitted over the communication network to the PDCs and then to the control centre. This network can be subjected to various constraints regarding the architecture, delay, throughput, and routes traversed by the traffic. Thus, this environment provides the capability to complement the power grid simulator to produce a smart grid co-simulation environment.

The virtualization of the communication network represents a novel approach in smart grid simulation. Using virtualization, we are creating instances of the communication network without any performance losses. Traditional network simulators replicate the core functions of network devices

but lack their full range of characteristics, whereas through virtualization, the communication network behaves exactly like a real-life system through emulation. Using this approach, we overcome the limitations associated with network simulators when coupled with real-time power simulators. In contrast to network simulation, we are able to divide our network into several private networks with different address domains, and manage traffic over those domains from and to the power system simulation environment. Furthermore, through virtualization, the inconsistency between the continuous real-time nature of power simulation and event-driven nature of communication simulation is no longer a problem. Both systems are simulated and interact in real-time. Finally, OpenStack allows for a seamless and real-time coupling of the emulated cyber systems with the real-time power system simulator.

3.1.3 Control Centre

The control centre consists of different software components that track grid conditions and execute decision-making using analytical algorithms that process and visualize the measurements collected by different sensors. Our control centre consists of software from Schweitzer Engineering Laboratories (SEL) [86], Synchrowave Central. Synchrowave Central provides power system situational awareness by translating data into visual information. It is a powerful solution for the display and analysis of synchrophasor data and relaying of event reports. Moreover, using the publicly available openECA project [87], we are capable of developing several smart grid applications to estimate the state of the grid and take corrective measures in response to faults, alerts, and attacks.

3.1.4 Testbed Capabilities

The developed Hardware-in-the-Loop (HIL) co-simulation testbed shares key characteristics with the emerging Digital Twin paradigm, which involves creating virtual replicas of physical systems for real-time monitoring, analysis, and control. Our testbed continuously mirrors the behavior of the physical power grid, enabling the simulation of cyber-physical attacks, evaluation of defense mechanisms, and assessment of system resilience under realistic conditions. Similar to a Digital Twin, it provides a synchronized virtual environment where operational data and cyber-physical

models interact in real time, facilitating predictive analytics, anomaly detection, and decision support for substation cybersecurity. In this section, we discuss the capabilities of the testbed and explore their ability to provide a real-time simulation of the smart grid.

3.1.4.1 Communication Protocols

A range of communication protocols and standards are currently used in power system communications. Those protocols include Modbus, DNP3, C37.118, and IEC 61850 for communications inside the substation, and between a substation and the control centre. Our interest in simulating those protocols stems from a cybersecurity perspective. Using our testbed, we are capable of simulating smart grid traffic using the implemented protocols. We are capable of receiving measurements from the power simulation model using C37.118, IEC 61850 GOOSE, and SV, along with the status of circuit breakers using IEC 61850, DNP3, and Modbus. The simulation environment is capable of receiving signals using those protocols to control the power model under investigation. Moreover, traffic from and to the power grid components can be targeted by attacks against the protocols or general attacks targeting the communication infrastructure. This allows us to study the system behavior and response to such malicious actions, and develop strategies to harden the system security and increase its resilience to attacks.

3.1.4.2 Wide Area Measurement System

The need for a WAMSs emerged as an outcome of the analysis of blackouts experienced by the smart grid. WAMSs evolved to become the main monitoring mechanism within the power grid. However, the deployment of such a system is associated with a high cost due to the number of needed PMUs and the underlying communication network. Thus, there is a need to study the performance and reliability of WAMSs ahead of large-scale deployment. Our testbed, with its integrated PMUs and the vast capabilities of the virtualization environment, is capable of accurately and realistically testing WAMSs networks of various dimensions. Moreover, simulating WAMSs in a controlled environment enables us to assess WAMSs security concerns, and evaluate its robustness to attacks. Such an assessment is of extreme importance to utilities.

3.1.4.3 Time Synchronization

Precise time synchronization is essential for the reliable operation of the smart grid. The synchronization of grid devices is essential for various smart grid applications (voltage stability, fault localization, etc). The smart grid relies on two major mechanisms for time synchronization, Global Navigation Satellite System (GNSS) and Precision Time Protocol (PTP) [88, 89]. Those time distribution mechanisms are subject to a variety of attacks that threaten their availability and usage in the smart grid [90]. Thus, there is a need to quantify the impact of threats stemming from the security of time synchronization mechanisms for the smart grid. Through our testbed, we are able to synchronize the available hardware using GPS and PTP, and thus simulate attacks targeting both these time synchronization services. This capability of our testbed makes it possible to study the impact of those attacks and test solutions to harden the security of those synchronization mechanisms.

3.2 Experimental Setup

Our experimental setup consists of the IEEE 24-Bus test grid and its corresponding communication network. This test grid is also known as the IEEE Reliability Test System, and is widely used in power systems research. The size and relative low complexity of this grid make it suitable for real-time co-simulation setups without the need of extensive computational resources. Through this setup, we study the impact of cyberattacks on WAMSs. To enable this study, we added two PMUs to the IEEE 24-Bus system as shown in Fig. 3.2. PMU_A monitors Bus 3 and records the three-phase voltage magnitude, phase angle, frequency, and rate of change of frequency (ROCOF). PMU_B, installed at Bus 9, captures the same set of measurements. Both PMUs transmit their data to a local PDC (PDC1) using the IEEE C37.118 protocol [85]. PDC1 synchronizes and aggregates the received measurements based on their timestamps and forwards the compiled data to a higher-level PDC (PDC2), which subsequently transmits the information to the control centre for processing. The control centre visualizes the status of the transmission line connecting Bus-3 and Bus-9 using the reported measurements. The communication network used for this setup is virtualized using OpenStack and depicted in Fig. 3.3. We simulate cyberattacks using a transparent bridge deployed in our testbed, which is capable of intercepting and controlling the traffic transmitted by PDC1. This

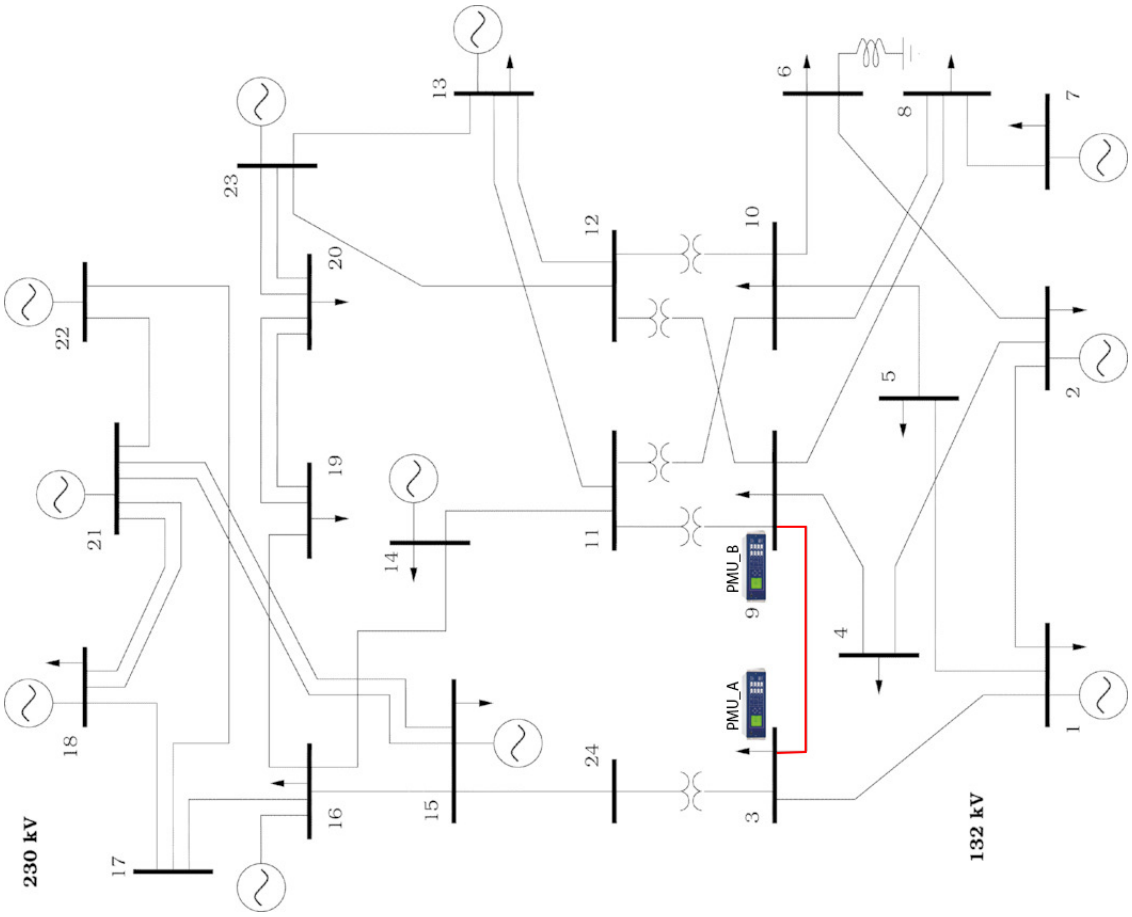


Figure 3.2: IEEE 24 bus test system

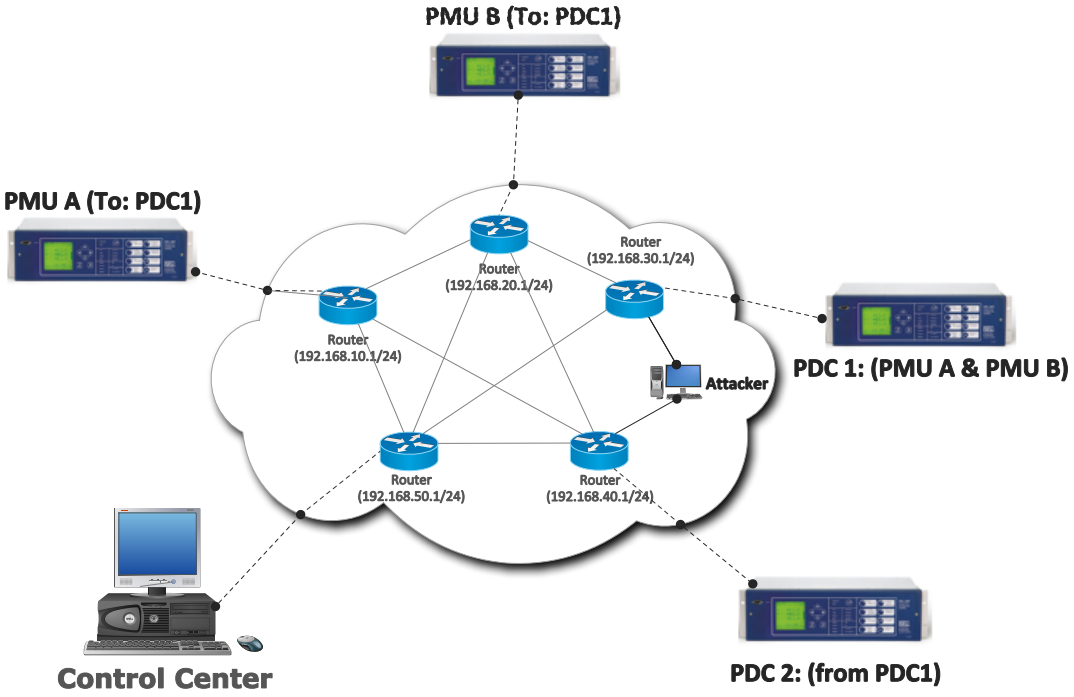


Figure 3.3: Virtual network topology created on openstack

setup enables the evaluation of various attack scenarios on WAMSs using PMU measurements. This setup enables the study of different types of attacks targeting the measurement system, along with their impact on the power system behavior.

3.3 CyberSecurity Use Cases

In this section, we describe the performed attack scenarios and the collected results. Using the attacker capabilities in the transparent bridge, we performed a DoS attack, data replay attack, and on-the-fly traffic manipulation attack.

3.3.1 DoS Attack

A DoS attack can be launched to target PMU measurements and WAMSs. The first method of launching this attack is by delaying the data during transmission, rendering it useless for the power system. Once the delayed data arrives at the PDC, the PDC will drop the traffic due to violation of its timer limits [56]. Another method is to simply drop the PMU traffic and prevent it from reaching

the PDC. In our case, we intercepted and dropped all the measurements collected by the two PMUs for a few seconds to prevent its collection by the PDC.

The attack was performed for three seconds, and Fig. 3.4 depicts the measurements collected at the control centre. Fig. 3.4 demonstrates the attacker's success in denying the control centre the ability to monitor the transmission line between Bus-3 and Bus-9. The impact of the loss of these measurements on state estimation was demonstrated in previous studies [56]. However, their attack hinders state estimation for a few milliseconds, while our attack can last for a prolonged time. It is worth noting that the same attack can target PDC functionality through compromising an intermediate network node. This demonstrates WAMSs vulnerability to DoS attacks.

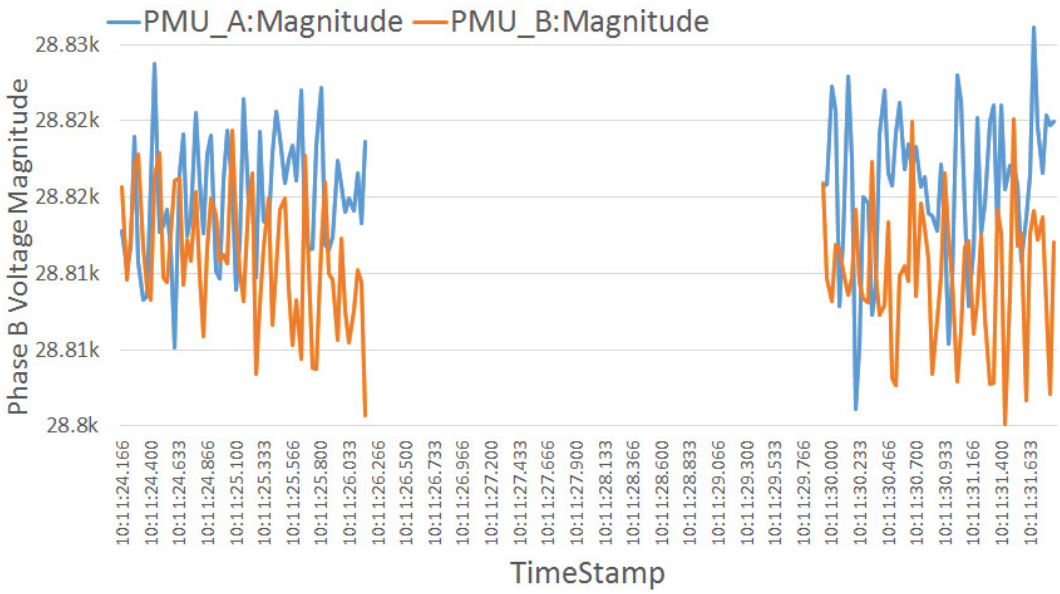


Figure 3.4: Impact of a DoS attack

3.3.2 Replay Attack

To perform a replay attack, an attacker has to collect measurements and then replay them to the PDC at a later time of their choosing. However, to prevent the PDC from detecting the attack and successfully replaying the saved measurements, the attacker has to update the traffic timestamp before injecting the data back into the network. Moreover, the attacker has to update the following fields in the packets: Second-Of-Century (SOC), the fraction of second (FRACSEC), and

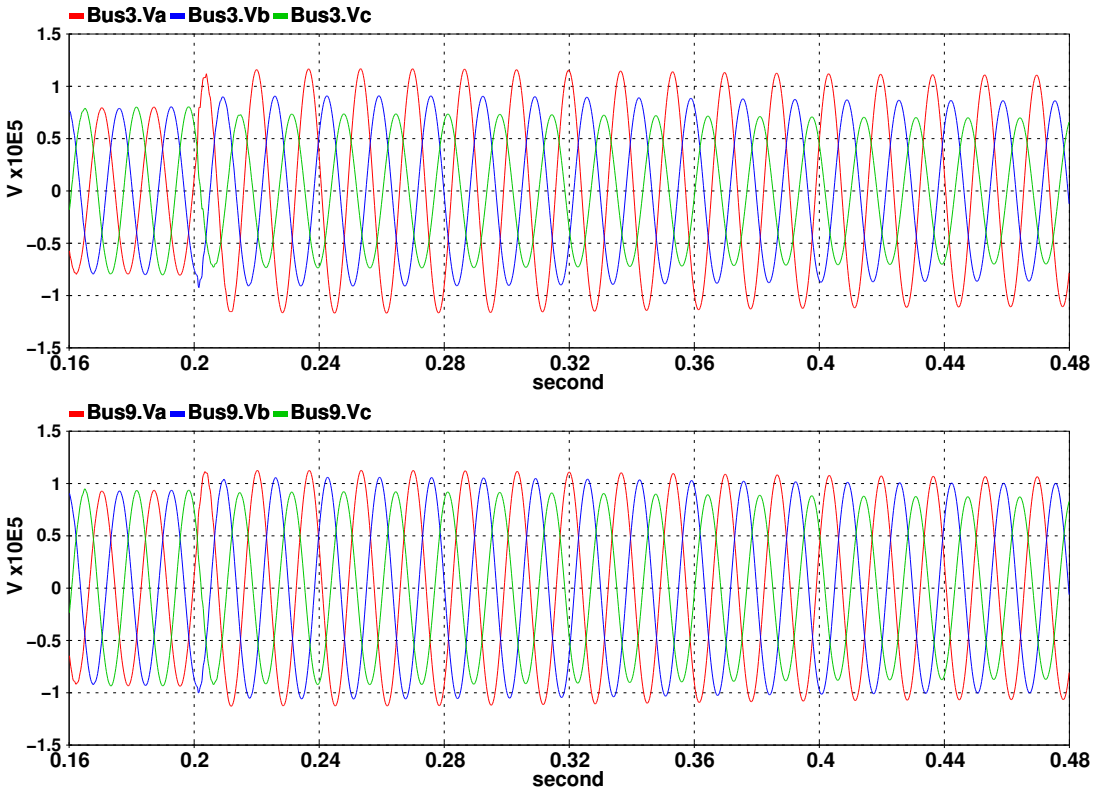


Figure 3.5: Voltage oscillations at bus-3 (top) and bus-9 (bottom) during replay attack.

CRC-CCITT (CHK). Due to the lack of security measures in C37.118, such modifications are undetectable. Indeed, the virtual communication network empowers us with the capability to intercept, modify, and inject traffic into the network. To perform the attack, the C37.118 traffic sent from PDC1 is intercepted. The traffic is analyzed, and data referring to PMU_A is modified to introduce changes into the header as indicated above.

The modified packets are then injected into the network and successfully collected by PDC2. The attacker can use this attack to hide the actual system state. To demonstrate the impact of such attacks, we created a fault on phase A of the transmission line monitored by the two PMUs. The effect of this failure can be seen in Fig. 3.5, which shows voltage oscillations at Bus-3 and Bus-9. The instability in the voltage is masked by the attacker through a data replay attack. As a result, the control centre can only see the waveforms plotted in Fig. 3.6. Indeed, Fig. 3.6 shows normal

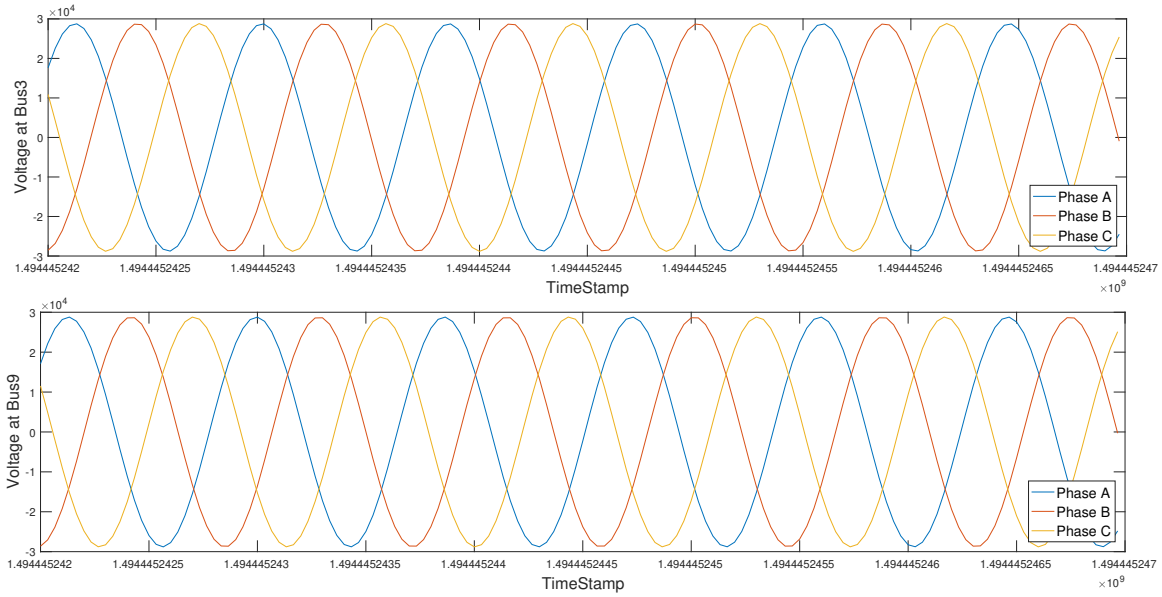


Figure 3.6: Voltage monitoring at bus-3 and bus-9 during replay attack.

working conditions in the system without any alerts regarding the phase angles at the monitored transmission line. Those experiments confirm that an attacker can induce a failure on the monitored transmission line and replay normal data to hinder the control centre's visibility of the actual system state. This attack demonstrates the vulnerability of WAMSs to replay attacks.

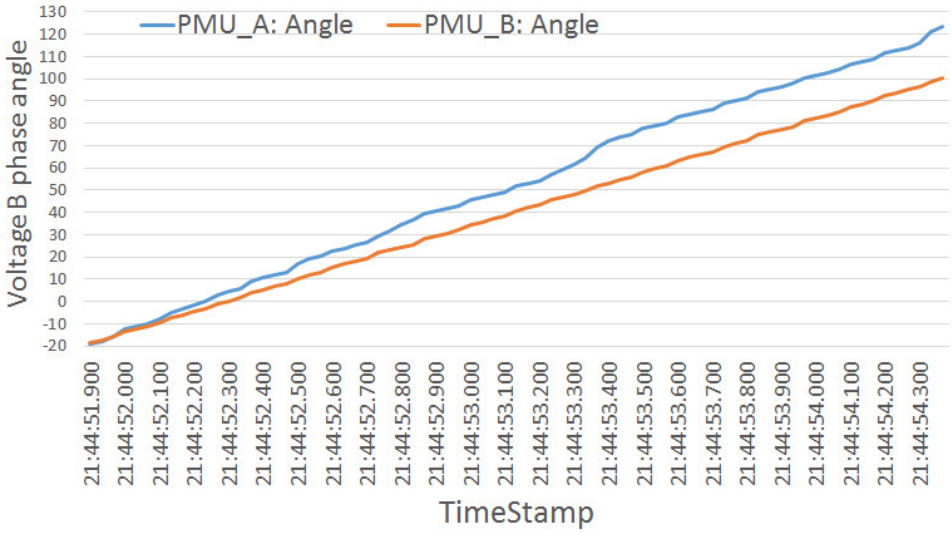


Figure 3.7: Impact of traffic manipulation attack on the phase angle monitoring

3.3.3 Traffic Manipulation Attack

In this scenario, the attacker aims to deceive the control centre through online modification of WAMSs traffic. As a result of this modification, the control centre will make a decision based on the manipulated data. To demonstrate this attack, we target a power system application that uses WAMSs traffic to monitor phase angle difference from selected PMUs, and detect faults in the system [91].

Monitoring phase angle differences gained more significance as an important tool after the August 2003 Northeast outage and the September 2011 Pacific Southwest outage [92]. Phase angle difference can be used to understand system stability [92] by comparing to a pre-determined reference. The acceptable phase angle difference is set at 14 degrees [91], and any violation of this limit indicates a fault in the system and necessitates corrective actions from the control centre.

To carry this attack out, the attacker manipulates the PDC traffic to introduce a phase angle difference between the PMUs at both ends of the transmission line that exceeds the acceptable limit. The synchrophasors traffic is altered to change the phase angle of PMU_A, and the resulting traffic is injected back into the network. The attack impact on the phase angle difference of phase B is illustrated in Figure 3.7. As Figure 3.7 shows, the attacker succeeded in introducing a difference in phase angles by modifying the data during transmission. This manipulation raised a false alarm at the control centre since the phase angle difference reached 21 degrees as demonstrated in Figure 3.8.

3.4 Conclusion

In this chapter, we presented the architecture of our smart grid real-time HIL co-simulation testbed. The testbed's power grid, cyber, and communication systems, and their capabilities were introduced. Using OpenStack we built the virtual communication network, allowing us to simulate smart grid networks of different sizes. Moreover, our co-simulation framework is capable of simulating different smart grid protocols such as GOOSE, SV, PTP, IEEE C37.118, IEC 61850-90-5, DNP3, and Modbus. Finally, we presented the vulnerability of WAMSs to a variety of cyberattacks targeting its communication network. Using the co-simulation environment, we demonstrated the

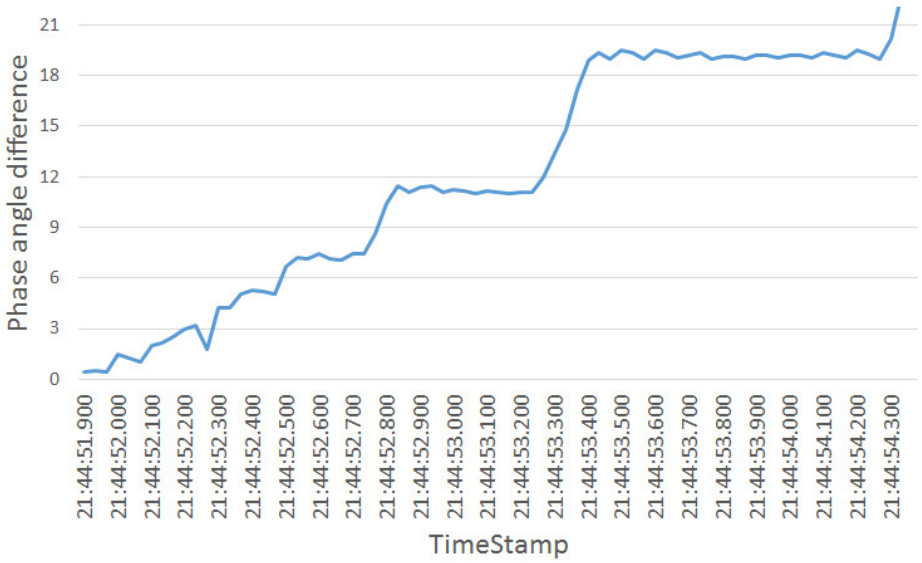


Figure 3.8: Phase angle difference caused by traffic manipulation attack

real-world impacts these attacks can have on the power grid. To this end, we presented the impact of three attack types, and discussed how attackers can extend them to cause large-scale failure in the grid.

Chapter Four

Security Monitoring of IEC 61850 Substations Using IEC 62351-7 Network and System Management

The IEC 62351-7 standard, outlines data collection through Network and System Management (NSM) and supports security monitoring of smart grid environments. However, while the standard defines a set of NSM data objects essential for managing the grid's information infrastructure, it does not elaborate on how these objects can be effectively utilized to assess system security or detect cyber threats [15, 93]. This lack of operational guidance leaves a gap in translating the standard's specifications into actionable security measures.

In this chapter, we address this gap by developing an NSM-based security monitoring platform tailored to a realistic IEC 61850 substation model, using the specifications outlined in IEC 62351-7. The proposed model integrates essential smart grid elements, including power equipment (e.g., transformers, transmission lines, generators), control schemes (e.g., voltage regulation), protection devices (e.g., overcurrent, distance, differential, and under/overvoltage relays), and communication protocols (e.g., GOOSE, SV). Finally, NSM agents and managers are incorporated to enable systematic data collection across the system.

To detect anomalies and identify cyberattacks, a two-step deep learning framework is introduced. The first step applies multiple deep learning architectures, i.e., LSTM, Recurrent Neural Network (RNN), and Gated Recurrent Units (GRU). Each of these models is paired with an autoencoder to enhance feature extraction. In the second step, an ensemble learning technique is employed to combine the outputs of the individual models and improve detection accuracy. The framework is validated using the co-simulation testbed in chapter 3, where several cyberattack scenarios are simulated on the IEEE 9-bus system to evaluate the platform's effectiveness.

Our findings demonstrate that leveraging NSM data for real-time security monitoring can significantly enhance the visibility and resilience of smart grid infrastructures. Based on these results, we propose cybersecurity recommendations aligned with IEC 62351-7, emphasizing the need for more practical guidance on utilizing NSM objects to detect and mitigate cyber threats. The chapter underscores the importance of securing the grid's information infrastructure and contributes a concrete implementation model that bridges the gap between theoretical standards and operational security.

The main contributions of this chapter can be summarized as follows:

(1) Employing a detailed substation model to demonstrate the physical impact of cyberattacks targeting the IEC 61850 communication protocols.

(2) Designing and implementing an IEC 62351-7 compliant NSM monitoring and data collection platform.

(3) Proposing and implementing a two-step deep learning cyber attack detection framework.

(4) Assessing the limitations of the current cybersecurity guidelines of IEC 62351-7 and providing additional recommendations.

The remainder of the chapter is organized as follows. Section 4.1 describes the developed physical model, cyber model, and co-simulation environment. Section 4.2 presents the Threat Model and the cyberattacks on IEC 61850 substation protocols. The proposed anomaly detection solution is introduced in Section 4.3.2. We then present the experimental results, including the detection performance and cyber-physical impact in Section 4.4. Finally, in Section 4.5, we provide an assessment

of IEC 62351-7, including limitations and recommendations, and 4.6 concludes this chapter.

4.1 System Modeling and Co-simulation Testbed

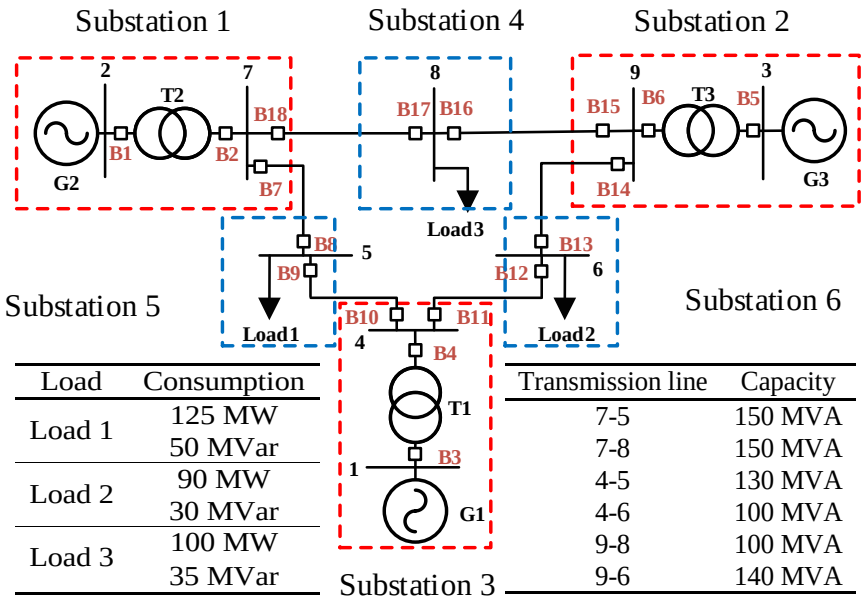
This chapter examines the security mechanisms in place in IEC 61850 substations [36] based on IEC 62351, especially IEC 62351-7 [15]. The IEC 62351-7 standard specifies the data that needs to be collected and monitored through NSM, to ensure the integrity of IEDs digital communications.

This monitoring, however, is considered inadequate, as existing SCADA systems do not provide the complete information required to help diagnose anomalies in the network layer or at edge devices [15]. In this research, we consider well-defined and standardized NSM data objects, specifically tailored to power systems, that represent information about the devices being monitored. IEDs present in the substation can populate the NSM data objects with the necessary data for a remote management system to retrieve using the SNMP. These NSM data objects can then provide a wealth of new information to oversee the reliability of the communication system and edge devices, to identify problems such as degraded performance or system failures, and raise alerts associated with cyber threats.

The section below discusses the system model considered for this research.

4.1.1 Physical Layer

In this chapter, we evaluate our methodology using the IEEE 9-bus test system, which serves as a simplified representation of the 230 kV Western System Coordinating Council (WSCC) power grid. It includes three generators (at buses 1, 2, and 3) and three load substations (at buses 4, 5, and 6) that are interconnected by six transmission lines. The total load of the grid is 315 MW and 115 MVAr. The single-line diagram of the system and its detailed parameters are illustrated in Fig.5.1. The physical and cyber layers discussed in the following subsections are constructed on top of this grid.



Load	Consumption
Load 1	125 MW 50 MVar
Load 2	90 MW 30 MVar
Load 3	100 MW 35 MVar

Transmission line	Capacity
7-5	150 MVA
7-8	150 MVA
4-5	130 MVA
4-6	100 MVA
9-8	100 MVA
9-6	140 MVA

Figure 4.1: IEEE 9-Bus system scheme.

4.1.1.1 IEC 61850 Digital Substation

The physical side of IEC 61850 substation includes various components, such as Current Transformers (CTs), merging units, circuit breakers, transformers, control rooms, etc. For instance, CTs are used to reduce the current magnitude to a level compatible with the control/protection system. The merging unit is used to receive the measurements of CT and convert them to SV messages compatible with the digital protection system [94]. The control and protection systems are built on top of the physical system to regulate the grid's parameters and protect it.

- Protection scheme: The main objective of the protection system and its corresponding IEDs is to detect electrical faults and isolate affected systems without significant performance degradation of the remaining sections of the grid. The relays receive and process the measurements and send tripping commands to their associated circuit breakers. In the developed substation model, three different relays are deployed, namely, overcurrent relays (50/51), distance relays (21), and differential relays (87). The sampling frequency of these relays is 2-3KHz [80], and they are distinguished using their ANSI codes between parentheses. The numbers associated with each protective relay are assigned according to the ANSI/IEEE C37.2 standard [95]. The overcurrent relay in Substation 1 of Fig. 5.1, protects the buses and transmission line using a time-inverse curve that ensures faster

clearing of a fault when its magnitude is larger. The guidelines for the computation of this curve are presented in [96]. The Distance relay, which is used as a backup for overcurrent, identifies the drop in the system impedance following the fault. The differential relay is also deployed to protect the transformer, benefiting from the difference between its input and output currents. Furthermore, the loads are protected by overvoltage and undervoltage relays, which are designed to disconnect them during emergency voltage conditions. To optimize the operation of the designed protection system, the relay settings are carefully coordinated to ensure that, upon fault detection, only the minimal necessary portion of the grid is disconnected by the protective IEDs, thereby preserving overall system stability and continuity of service.

- Control scheme: The main aim of the control scheme is to ensure that the system parameters, e.g., voltage, are within the acceptable limits. To this end, we developed a voltage regulation scheme using an on-load tap changer for the substation transformer. In this control scheme, the voltage is measured at the secondary side of the transformer, and the tap of the transformer is calculated so that the voltage remains within the acceptable range. Following any change in the system operation point, the control system is delayed by 1.25s to ensure that the voltage reaches steady state before deciding on the magnitude of the regulation. The tap changer is has 23 taps activated in steps of 1.25% per unit to keep the voltage within acceptable limits. It is worth mentioning that the generators are also equipped with automatic voltage regulators and power system stabilizers.

4.1.2 Cyber Layer

In this subsection, we describe the cyber infrastructure implemented in our IEC 61850 substation model illustrated in. Fig. 4.2.

4.1.2.1 Protocols

IEC 61850 is a standard issued by IEC to define the communication protocols for IEDs in the substation [36]. In this research, we implement SV, GOOSE and R-GOOSE protocols. SV is used to transfer measurements from MU to other Intelligent Electronic Devices (IEDs) such as relays. GOOSE is used to transfer control signals from IEDs to circuit breakers within the same substation.

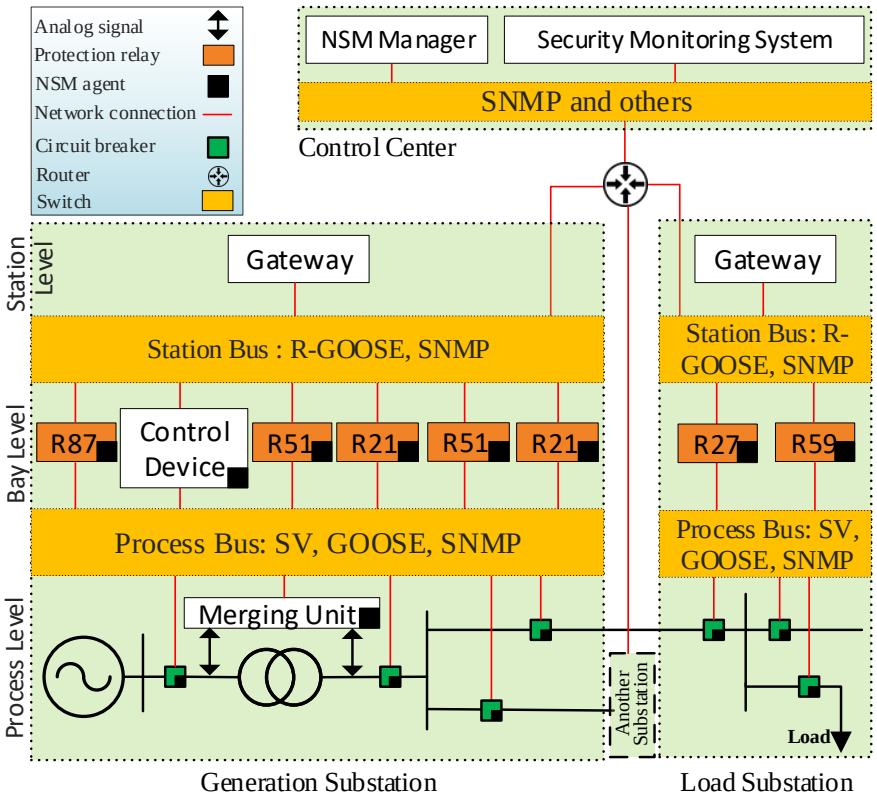


Figure 4.2: IEC 61580 substation model.

R-GOOSE is used to transfer control signals between substations. IEC 61850 does not discuss the security measures for these protocols. Thus, the security recommendations provided by IEC 62351 are considered. Among the main IEC 62351-7 security recommendations is the utilization of NSM for security purposes [15].

It should be noted that some security measures that fall outside NSM are specified in other parts of IEC 62351. Specifically, IEC 62351-6 covers the security of GOOSE and SV. IEC 62351-6 specifies that encryption should be used for IEC 61850 protocol communications in cases where the strict operational timing requirements are not a concern. It specifies the use of AES 128 for encryption and SHA256 for generating a Message Authentication Code (MAC). These cryptographic techniques ensure the integrity and confidentiality of IEC 61850 messages. For applications where strict timing requirements must be met, the standard emphasizes the importance of securing the local communication channels used to exchange messages. Our work considers the IEC 61850 substation network with strict operational timing restrictions, where computational overhead for cryptographic

operations may be too large to be considered feasible. The implementation of IEC 62351-6 is outside the scope of this chapter. Throughout this chapter, we use GOOSE Protocol Data Unit (PDU) field names regularly, so Table 4.1 lists GOOSE PDU fields and describes the purpose of each field.

Table 4.1: GOOSE PDU structure [1]

GOOSE PDU Field	Description
gocbRef	The name of the control block that represents the publisher-subscriber relation
timeAllowedtoLive	The amount of time within which the next GOOSE packet is expected to arrive
datSet	The name assigned to the data and commands being transferred
goID	The name assigned to the source IED of the GOOSE PDU
t (timestamp)	the timestamp corresponding to the date and time that the PDU was transmitted
stNum	A counter that increments by one every time the value of the data being transmitted is changed, resetting the sqNum field to 0 upon incrementing
sqNum	A counter that increments by one every time a GOOSE PDU is transmitted that contains the same information as the previous packet and is reset to 0 when the stNum field is increased to signal new data values being transmitted
test	An indicator for whether the GOOSE PDU is a test message
confRev	A counter that increments every time the GOOSE control block is reconfigured
ndsCom	An indicator for whether the GOOSE control block needs to be reconfigured
numDatSetEntries	A count of the number of data entries contained in the GOOSE PDU
allData	The data payload of the GOOSE PDU, where data and commands are written

4.1.2.2 Communication Network

Fig. 4.2 shows the IEC 61850 substation communication schema. There are three levels in the substation schema: process, bay, and station level. There is a network switch between the levels. Equipment in the process and bay levels is connected to the process bus or switch, while equipment in the bay and station level is connected to the station bus or switch. All the IEDs and controllers have NSM capabilities. The substation network provides a connection between IEDs inside and outside the substation, as well as one between the controller and the utilities. The substation network

is emulated using our co-simulation testbed.

4.1.3 Network and System Management (NSM)

NSM is developed to gather the statistical data from different IEDs deployed on the substation model. The measurements of those IEDs and the NSM collected data are used to take operational decisions and ensure the security of the substation, respectively. In the NSM platform, agents collect the MIB object values and send them to the manager using SNMP [97] for security monitoring purposes. Fig. 4.3 shows the general scheme of NSM, where the manager queries all agents for the collected MIB object values based on IEC 62351-7.

NSM DOs can be collected either through polling or using traps. Polling involves the NSM manager requesting the DO values from the NSM agent at regular intervals [97]. On the other hand, traps are event-driven unsolicited messages sent by the NSM agent to the NSM manager upon generating a DO that corresponds to a security event. The proposed testbed uses polling to retrieve the latest DO values from the NSM agents corresponding to the relays. Ideally, the polling rate matches the DO value update rate of the NSM agents. The effective anomaly detection speed using NSM can be increased by having the measurement tools update the values of the polled DOs on the agent more frequently.

The agents and the manager are implemented on VMs in our co-simulation testbed. Each agent Virtual Machine (VM) is deployed as a proxy to collect the information from the corresponding IED. Fig 4.2 demonstrates the agents that are attached to the IEDs in the substation model.

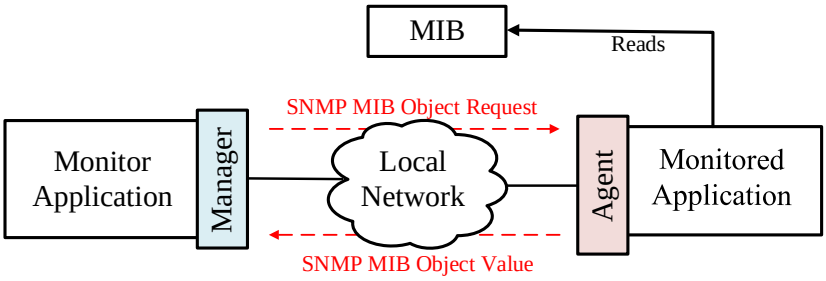


Figure 4.3: The general scheme of NSM platform.

4.1.4 Co-simulation Testbed

All simulations are performed on the testbed developed in Chapter 3. After incorporating all the communication, control, and NSM functionalities discussed in this section, the testbed accurately replicates the architecture and operational behavior of a realistic IEC 61850 substation with NSM capabilities, in accordance with the IEC 62351 standard. This co-simulation testbed is capable of performing our security assessment and simulating cyberattacks to validate the impact on the physical system. The first part of this testbed is an OPAL-RT Hypersim [83] digital simulator, which simulates the power grid in real-time. Hypersim also provides I/O for digital and analog communication, which can be used to connect the power system to physical IEDs. Moreover, it provides protocol drivers for IEC 61580, Modbus, DNP3, C37.118, and more. These drivers can be connected to virtual components such as protection relays or circuit breakers. The traffic generated by these drivers is used to evaluate and assess the effects of the security attacks on the smart grid. An example of a IEC 61850 GOOSE packet generated by Hypersim is shown in the Wireshark packet file presented in Figure 4.4.

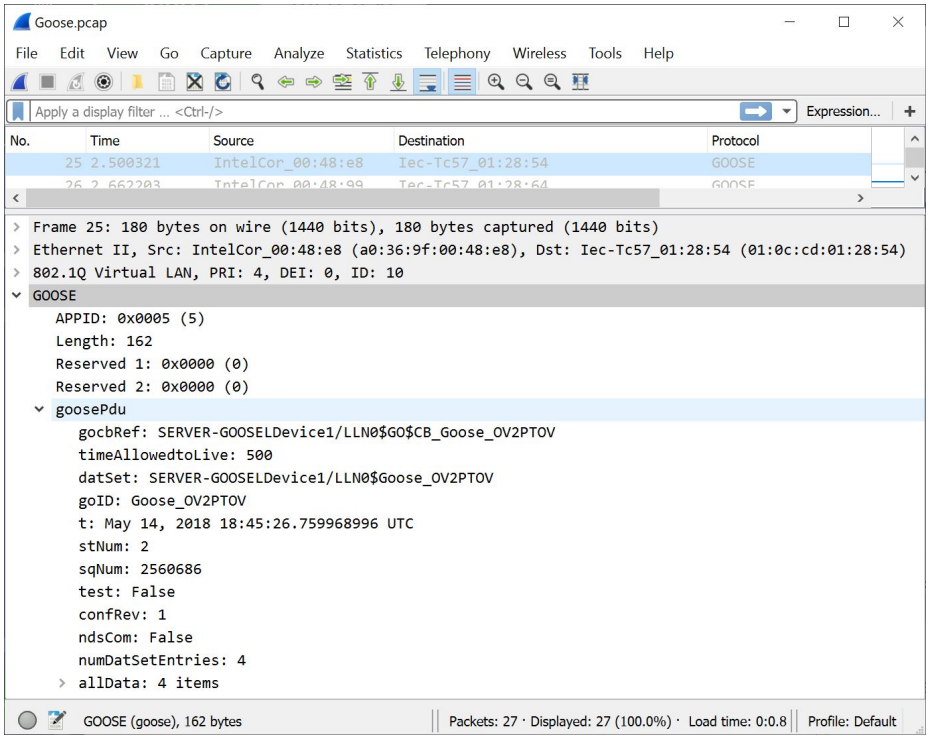


Figure 4.4: Wireshark packet trace for Generic Object Oriented Substation Event communication.

The second part of this testbed is OpenStack [84], which emulates the smart grid's cyber layer. Furthermore, Hypersim's I/O ports are connected to the OpenStack network, and the messages transmitted between IEC 61850 GOOSE and SV publishers and subscribers must pass through the OpenStack network. Actions that control the quality-of-service network parameters of our testbed communication network, such as packet delay, are implemented within our custom transparent bridges deployed on OpenStack. These bridges are used to control the traffic flow between the substation publishers and subscribers.

4.2 Threat Model

In this chapter, we consider that the attacker gains access to the substation network and is able to target its communication protocols. However, the attacker cannot compromise the IEDs themselves. Furthermore, the following assumptions are made. The attacker is knowledgeable about the information and operational infrastructures. Moreover, the attacker can persist in the system as long as required to achieve their malicious objectives. Also, the attacker can inject, capture, replay, modify, drop, and delay any communicated messages. We consider straightforward and sophisticated attack scenarios to test them against our detection system.

For our attacker model, we consider an insider case in which an attacker infiltrates the substation under the guise of a worker performing scheduled maintenance on a network switch. The attacker then secretly connects a rogue device to the network switch being updated. The rogue device reconfigures the network to pass traffic of a specific GOOSE publisher through the rogue device. In this way, the rogue device acts as a man-in-the-middle, launching the attacks studied in this chapter.

We identify the variables that can be used to discard messages or degrade their quality. For instance, undelivered GOOSE messages that carry a critical trip command could have adverse effects on substation operation. The identified variables are used to generate a list of cyberattacks that can target ICS protocols, which are presented in Table 4.2. Attacks G2 and G7 have been explored in [81, 98] and [99] respectively.

Our work considers an attacker capable of injecting malicious GOOSE packets and delaying legitimate packets. The GOOSE protocol is used to transfer the command from the protection relay

Table 4.2: List of cyberattacks on ICS protocols

ID	Attack
G1	Modify PDU length (malformed PDU)
G2	Modify, inject or replay PDU with higher stNum
G3	Modify PDU t to outside skew period
G4	Delay PDUs until they are outside skew period
G5	Modify, inject or replay PDU with smaller Time-Allowed-to-Live (TAL) to force TAL expiration
G6	Drop PDUs until TAL expiration
G7	Delay PDU until TAL expiration
G8	Modify PDU confRev field
G9	Modify, inject or replay PDU with test flag on
G10	Invalidate digital signature

to the circuit breaker. These commands can be 0 (open) or 1 (close). The GOOSE injection attack issues false commands that open or close circuit breakers and, in our experiments, can be executed in two ways. One way is to fake a new packet carrying that command, and the other is to interrupt and modify the transferred packet. We simulate the GOOSE injection attacks through a Python script on the VM configured as a transparent bridge with two network interface cards, placed between the GOOSE publisher and subscriber.

As for GOOSE delay attacks, the legitimate GOOSE traffic can be delayed in two ways. One way is to introduce a fixed and abrupt delay to the transferred command, which can cause a cascading failure. The second way is to introduce a minimal delay between packets arriving in the attacker's packet queue. This minimal delay accumulates over multiple consecutive packets into a significant delay. This delay causes critical commands to be held within the attacker queue long enough to cause operation failures, possibly leading to a cascading failure. We simulate the delay attacks on a transparent bridge VM placed between the GOOSE publisher and subscriber.

In the GOOSE poisoning attack, for example, the attacker can set the stNum field of a packet during GOOSE communication to a new value to desynchronize the publisher and subscriber, thereby poisoning the GOOSE communication. The attacker can achieve this goal by either injecting a new fake message containing a higher stNum value or modifying the stNum of one of the transmitting messages with a higher value.

As a man-in-the-middle, the attacker can launch the GOOSE poisoning, GOOSE delay, and GOOSE injection attacks. This research aims to detect those attacks through our proposed security

monitoring framework based on NSM. The NSM agents deployed in our system report MIB object data related to traffic statistics to the NSM manager, which can help identify the attacker's activities.

4.3 Anomaly Detection

In the following section, we describe how we leverage the collected NSM data to build anomaly detection models capable of detecting and localizing cyberattacks in a substation.

4.3.1 Machine Learning-Based Anomaly Detection

Our Proposed machine learning-based anomaly detection approach is described below.

4.3.1.1 Data Collection and Preprocessing

To collect the required data, we deploy the NSM architecture presented in section 4.1.3 on the co-simulation testbed and use it to collect the required NSM data. This data is then visualized and analyzed using statistical tools to detect trends and correlations. This analysis allows us to select the models best suited for the detection of anomalies resulting from cyberattacks on the substation.

This data consists of vectors of more than 300 MIB values periodically collected at 10-second intervals from all devices in the substation. We consider the collected vector as a snapshot of the state of the substation under study. A sequence of snapshots is stored in a database during a period of 24 hours of normal operations. The objective of this is to learn the normal behavior of the substation and use it as a reference to detect anomalies. This data is preprocessed in a sequence of four steps: filtering, encoding, regularization, and normalization.

In the filtering step, all MIB objects identified as static or with no relevance to anomaly detection are discarded. These objects are carefully selected based on their semantics as described in the IEC standard. An example of such objects includes MAC address and IP address of the IEDs. In the second step, MIB objects belonging to categorical types are encoded into numerical values using one-hot encoding. These include MIB objects that report the time synchronization status (e.g. "cLKEClockIssue") and MIB object has boolean value (e.g. "gSESL2ConfRevMis"). For the third step, MIB objects showing an increasing trend are individually regularized using differencing and

turned into a rate. The data is then normalized to scale each numerical MIB object to the range [0,1]. At the end of this stage, the data is ready for analysis, followed by training the machine learning models.

4.3.1.2 Data Analysis

The first step of our analysis is conducting statistical analysis to examine the correlation and autocorrelation that exists within our collected MIB objects. Autocorrelation is the correlation between a signal and a delayed version of itself. The correlation between two MIB objects X and Y is calculated as:

$$\rho_{XY} = \frac{cov(X,Y)}{\sigma_X \sigma_Y} \tag{4.1}$$

where cov denotes the covariance, σ_X and σ_Y represent the standard deviations of X and Y respectively.

Figure 4.5 reveals a high correlation between some of the MIB objects we have associated with the state of the substation network. This demonstrates how a change that appears in one part of the substation can be associated with or triggered by some change in another part of the substation.

On the other hand, Figure 4.6 reveals a high autocorrelation within the MIB objects. This suggests that the current state of the substation is highly correlated with its previous states. The figure shows the strength and type of relationship between values and their delayed counterpats. However, we observe that the correlation becomes weaker as the lag increases. The autocorrelation function (ACF) presented in Eq. (4.2) is used to observe the correlation within the same MIB object with different delay times (lags).

$$r_k = \frac{\sum_{i=1}^{N-k}(Y_i - \bar{Y})(Y_{i+k} - \bar{Y})}{\sum_{i=1}^{N}(Y_i - \bar{Y})^2} \tag{4.2}$$

where k is the lag; k = (1, 2, ...), Y_i is the value of Y at time step i, $\bar{Y}$ is the mean of Y, and N is the number of observations.

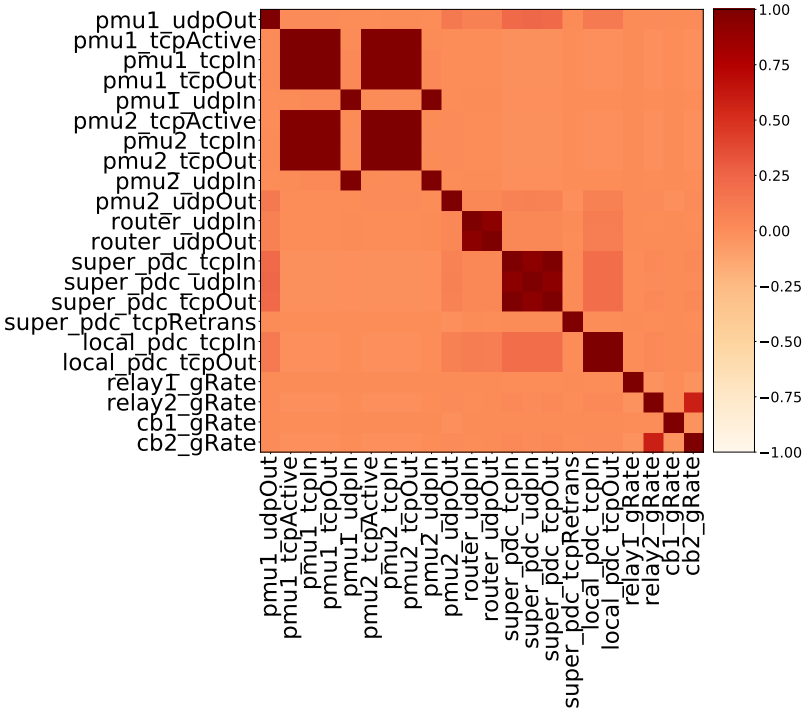


Figure 4.5: Linear correlations between MIB objects reflecting the substation network state.

4.3.1.3 Anomaly Detection Approach

The correlation results presented above motivated us to adopt an anomaly detection approach based on predicting the substation status and comparing it to the observed behavior. The idea is to collect SNMP snapshots from the substation during its normal operation. This data is used to build a machine learning prediction model that captures the normal substation behavior. This model will be used later to predict the future state of the substation from a sliding window of previous states and compare it with the current observed state. Anomalies will be flagged if the difference between these 2 states exceeds a certain threshold TH.

More formally, raw data D_t=$(d_{1,t}, d_{2,t}, \ldots, d_{m,t})$ is collected during normal operations of the substation where $d_{i,t}$ is the value collected from MIB object i at time t. t is the time falling the period $[T_1, T_2]$ where T_1<t<T_2. D_t is then preprocessed into a multivariate time series $X_t = (x_{1,t}, x_{2_t}, \ldots, x_{n,t})$. X_t is considered as the snapshot of the substation's state at time t. A machine learning prediction model is thrn trained to predict X_t from the previous states $X_{t-1}, X_{t-2}, ..., X_{t-p}$, where p is the prediction time window size. The maximum learning error for the training data is

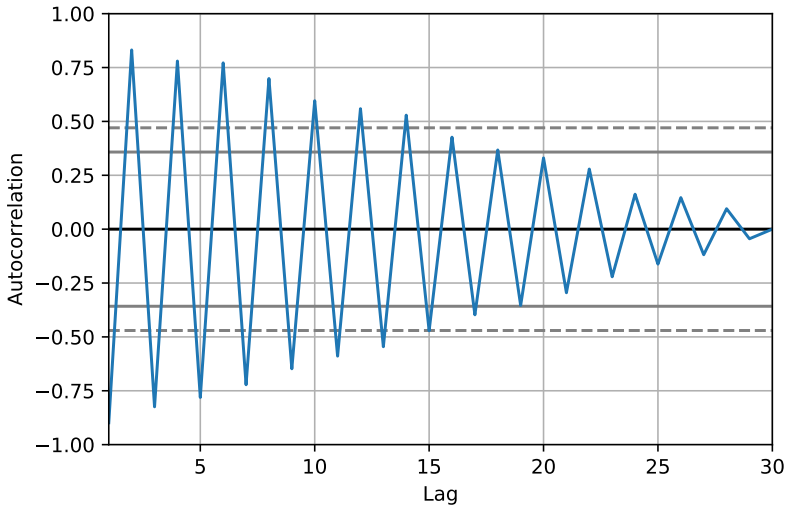


Figure 4.6: Auto correlations in MIB objects reflecting the substation network state.

used as the threshold TH.

Given that our data is shaped in the form of a multivariate time series, using models such RNN, GRU, and LSTM for our prediction model is expected to achieve the best results [100]. Neural networks achieve similar if not better performance when competed with classical statistical models, such as ARIMA [101, 102] [103, 104]. A recent study also shows that neural networks outperform classical statistical models by comparing the prediction accuracy of LSTM model and ARIMA forecast model [105].

Our anomaly detection model is constructed at the level of each MIB object to maintain the ability to identify the MIB experiencing the anomalous behavior. One way to achieve this goal is to create a separate prediction model PM_i for each MIB object i. The final model $PM{=}(PM_1, PM_2, ..., PM_n)$ which is a combination of all individual prediction models.

4.3.2 Anomaly Detection Models

In this chapter, we propose the use of LSTM, GRU, and RNN as our prediction models. Each of the proposed three deep learning models is combined with an autoencoder to improve the prediction results. In addition, using the ensemble learning method, we combine the results of the three models to further improve the overall results. Ensemble learning [106], is a method used to enhance the prediction results by combining outputs of separate and unique models to improve the overall

accuracy of the prediction.

After data is collected and preprocessed as described above, we split it into training and validation sets for each feature. In the training phase, the prediction model is trained using the preprocessed NSM data collected during normal operation. The normal operation involves conditions in the presence and absence of faults. The faults are simulated on different transmission lines and within different transformers. These faults are detected and isolated by various relays (87, 51, 21, 27 and 59), as shown in Fig. 4.2. These relays send trip commands to circuit breakers using the GOOSE communication protocol. Table 4.3 shows the locations of the simulated faults, as well as the normal events caused by the faults. In the validation phase, we compute the threshold through three step: (1) use the validation set in each model to predict the next timestep value, (2) enhance the prediction by using an ensemble learning method on the three developed models per feature, and (3) compute the differences between the predicted values and the ground-truth ones.

Table 4.3: Fault location and events under normal operation

ID	Fault	Location	Fault Detected	CB tripped
Tr0	Faulty transformer	T2	Sub1 Relay 87	B1, B2
Tr1	Faulty transformer	T3	Sub2 Relay 87	B5, B6
Tr2	Faulty transformer	T1	Sub3 Relay 87	B3, B4
L0	fault in Line	Bus 7-8	Sub1 Relay 51, 21	B18, B17
L1	fault in Line	Bus 8-9	Sub2 Relay 51, 21	B15, B16
L2	fault in Line	Bus 9-6	Sub2 Relay 51, 21	B13, B14
L3	fault in Line	Bus 6-4	Sub3 Relay 51, 21	B11, B12
L4	fault in Line	Bus 4-5	Sub3 Relay 51, 21	B9, B10
L5	fault in Line	Bus 5-7	Sub1 Relay 51, 21	B7, B8

The fully trained prediction models are used to flag anomalies in real-time. This process is depicted in Fig. 4.7. Fig. 4.7 presents two demonstrative scenarios, i.e., an anomaly scenario (in red) and a normal operation (in green). When an anomaly is detected, we replace the anomaly data with the predicted one, and we send an alert. This is performed to avoid adversely affecting future predictions by the anomalous values that were observed. The example shows a sliding window equal to 3 time steps for simplicity. However, the actual wondow size used in this research is 10 time steps.

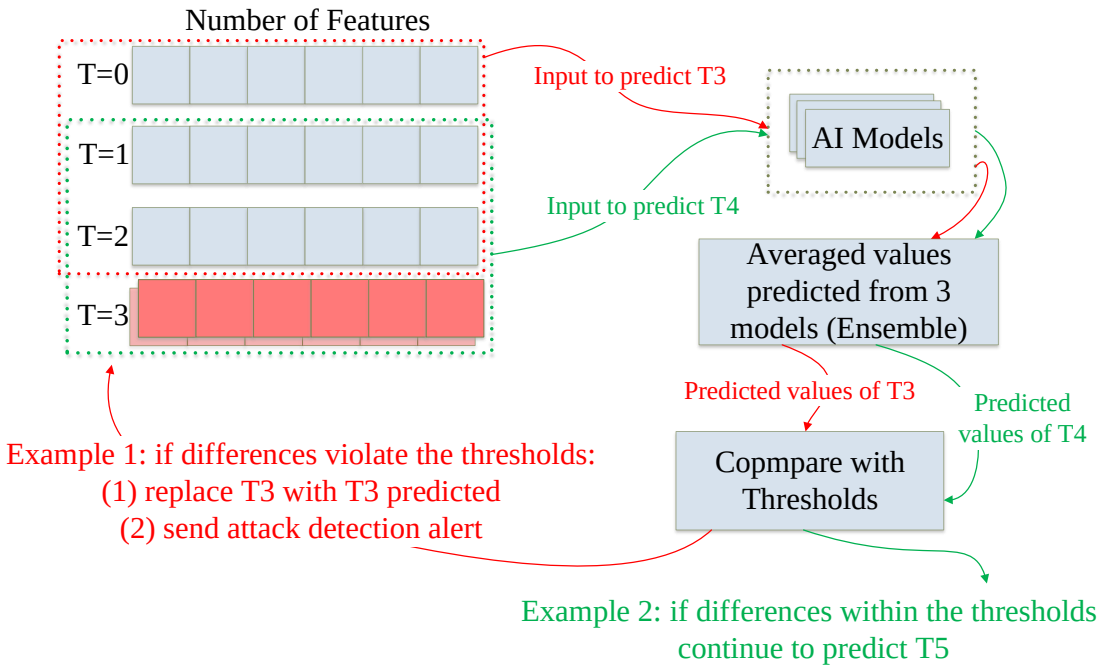


Figure 4.7: AI model training and detection processes.

4.4 Experimental Results

In the next two sections, we discuss the performance of our security monitoring system, its impact on cyber-physical systems, and our proposed improvements to IEC 62351-7. We experimentally evaluate our detection approach using a balanced dataset. Then, we calculate the true positive (TP), false negative (FN), true negative (TN), false positive (FP), recall, precision, and F1-score metrics to comprehensively evaluate the detection performance. We considered the normal behavior as the negative class and the malicious behavior as the positive class. The TP measures the number of malicious samples that are detected by our detection approach, while the FP measures the number of normal samples that are falsely detected as malicious samples. The TN measures the number of normal samples that are detected as normal by our detection approach, where the FN measures the number of malicious samples that are falsely detected as normal samples. According to [107, 108], the recall, precision and F1-score are calculated as follows:

$$Recall = \frac{TP}{TP + FN} \tag{4.3}$$

$$Precision = \frac{TP}{TP + FP} \tag{4.4}$$

$$F1\ -score = \frac{2 \times (Recall \times Precision)}{Recall + Precision} \tag{4.5}$$

As a result, data from two different experiments are collected to measure the performance and accuracy of our detection approach. The first one consist of: (1) 500 samples collected during normal operation in the absence of physical faults, (2) 250 samples collected during the GOOSE injection attack, and (3) 250 samples collected during the GOOSE delay attack. The detection performance results for this experiment are reported in Table 4.4. The second experiment consist of: (1) 500 samples collected during normal operation in the presence of physical faults, (2) 250 samples collected during the GOOSE injection attack, and (3) 250 samples collected during the GOOSE delay attack. The detection performance results for this experiment are reported in Table 4.5.

Table 4.4: Detection performance in the absence of a physical fault

TP	FN	FP	TN	Recall	Precision	F1-score	Threshold
477	23	2	498	0.954	0.9958	0.9745	$\alpha = 1$
489	11	20	480	0.978	0.9607	0.9693	$\alpha = 0.9$
497	3	111	389	0.994	0.8174	0.8971	$\alpha = 0.8$

Table 4.5: Detection performance in the presence of faults

TP	FN	FP	TN	Recall	Precision	F1-score	Threshold
481	19	12	488	0.962	0.9757	0.9688	$\alpha = 1$
492	8	27	473	0.984	0.9480	0.9657	$\alpha = 0.9$
499	1	131	369	0.998	0.7921	0.8832	$\alpha = 0.8$

Our anomaly detection determines if an observed MIB object is anomalous by comparing the deviation between the observed value and the predicted value with the anomaly threshold. MIB objects with deviations exceeding the threshold are considered anomalies. The threshold is equal to $\alpha \times losses$, where α is a constant multiplicative factor of our choosing, and $losses$ is the maximum amount of prediction loss reported during the validation step of the training process. The detection

performance results of our experiments across different choices for α are reported in Table 4.4 and Table 4.5.

To validate the detection time performance, we recorded the execution time for 1000 runs. The experimental validation was carried out on Intel core i7-7700k CPU. The average time was 0.64 ms. This performance is compliant with IEC 61850 time requirements for the deployed protocols. The 0.64 ms average time for our anomaly detection suggests that it is feasible for our proposed detection approach. There is, however, the additional challenge of ensuring that the NSM MIB objects being observed are updated and sent to the NSM manager shortly after the attack is launched. In cases where specific security events must be reported, NSM agents can use unsolicited SNMP trap messages to inform the central NSM manager of key events in the system. Fast detection based on traffic rate anomalies also depends on NSM agents updating the values of the traffic rate MIB objects over a very short interval.

It should be noted that since we trained multiple deep learning models, specifically one model for each MIB object under consideration, our detection system can point to the exact set of MIB objects that is anomalous, as well as identify the affected devices. Details of the anomaly are logged, and the gathered information of the detected anomaly is used to distinguish between different attacks. For example, when the attacker injects a fake GOOSE message into the network, the NSM agent of the GOOSE subscriber will report the fake message and assign it to a specific MIB object. Our deep learning models detect the anomaly and provide the details such as the increased value, the affected device, and the time of the event. This allows our detection system to distinguish between different attacks. Table 4.4 and Table 4.5 show the detection performance of our technique against cyberattacks in the absence of faults and during faults, respectively.

4.4.1 Detection of Cyberattacks Targeting The Protection System

4.4.1.1 Injecting GOOSE PDU with Higher stNum

This attack aims to interrupt the communication between the publisher (e.g., relay) and the subscriber (e.g., circuit breaker) to prevent the subscriber from processing legitimate messages sent by the publisher. To interrupt publisher-subscriber communication, the attacker injects a fake GOOSE

Table 4.6: Cyber-physical impacts and consequences

Scenario ID	Fault ID	Attack ID	Target	Impact	Consequences [Relay, CB]
S0	Tr0	G2, G4, G6, G7	Relay's 87 subscribers (B1, B2)	Cascading failure	[51, (B17, B18)], [51, (B7, B8)]
S1	Tr0	G2, G4, G6, G7	Relays' (87, 51) subscribers ((B1, B2), (B17, B18))	Cascading failure, Blackout	[51, (B7, B8)], [(51, 21), (B15, B16)], [27, Load3 CB]
S2	L0	G2, G4, G6, G7	Relay's 51 subscribers (B18, B17)	None	None
S3	L0	G2, G4, G6, G7	Relay's 21 subscribers (B18, B17)	None	None
S4	L0	G2, G4, G6, G7	Relays' (51, 21) subscribers (B18, B17)	Cascading failure, Blackout	[87, (B1, B2)], [(51, 21), (B15, B16)], [51, (B7, B8)], [27, Load3 CB]
S5	Tr2	G2	Tap changer control at Substation 1	Blackout	[59, Load1 CB], [59, Load2 CB], [59, Load3 CB]
S6	Tr2	G1	Tap changer control at Substation 1	Blackout	[27, Load1 CB], [27, Load2 CB], [27, Load3 CB]

message carrying stNum larger than that stored at the publisher (attack ID G2 at Table 4.6). To illustrate the impact of this attack on various locations of the implemented model, we consider the fault conditions in Table 4.3. When the fault is detected, the corresponding protection relays should trip the circuit breakers to isolate it. However, when the attacker poisons the publisher-subscriber communication, the subscriber is forced to drop the legitimate trip message. In Table 4.6, we summarize the cyber-physical impacts and their consequences on some targeted subscribers. As the attack's impact escalates, the fault cascades to another area, causing other relays to trip and isolate the fault. The findings from scenario (S1) indicate that the cascading failure can cause the disconnection of Load 3 as shown in Fig. 4.8. It is possible to detect this attack by analyzing the NSM data using the proposed two-step deep learning approach. This approach monitors the communication (including the GOOSE messaging rate) between the IEDs/RTUs. When the GOOSE messaging rate is abnormal, the approach raises an alert that indicates the detection of a GOOSE poisoning attack. Furthermore, this attack is simulated multiple times, and the proposed detection approach detects these attempts every time.

4.4.1.2 Modifying GOOSE PDU with Higher stNum

In this attack, the adversary has the same objectives as in the GOOSE injection, but in this attack, the attacker modifies a communicated PDU by changing its stNum to a higher value (attack ID: G2). The injection attack is detected since the PDU per-second rate changes. Since the modification attack does not affect the per-second rate, it remains undetected. As a result, our two-step detection approach is unable to detect this attack as its activity does not reflect on any considered MIB objects. This limitation is discussed in Section 4.5.

4.4.1.3 Delaying GOOSE PDU Until Time Allowed to Live (TAL) Expiration

The GOOSE delay attack (attack ID: G7) remains feasible even when message encryption and authentication are in place. This attack results in physical impacts comparable to those caused by injection and modification attacks, as shown in Table 4.6. However, in this attack, the targeted subscriber is not forced to drop the critical tripping command and, instead, responds late to the publisher. To apply this delay, the attacker introduces a 100 ms delay between each packet to reach a total delay of 4 seconds. As a result of this delay, the system experiences a cascading failure that, in some cases, leads to a blackout. Nevertheless, our detection approach identifies this attack based on the change of the MIB object "gSESL2RxPduPerSecond" that reports the rate per second. This attack is simulated multiple times, and the proposed detection approach can detect the attack every time.

4.4.1.4 Delaying GOOSE PDUs Until They are Outside Skew Period

Unlike in the delay attack that causes TAL violations, the goal of this attack (attack ID: G4) is to avoid detection by slowly shifting the arrival time of the GOOSE packets until a certain amount of timing shift, or skew, is achieved. Once the intended skew is achieved, the received GOOSE packets are older than they should be for safe operation, yet this would be viewed as normal. The attacker achieves this skew by introducing a very small delay between each packet sent to the GOOSE subscriber, gradually building up a queue of delayed packets in the process. Compared to the TAL violation delay attack, the delay between consecutive packets in this attack is not large enough to be

reliably distinguished as anomalous.

As result, the attack generates the same physical impact as the delayed GOOSE PDU, but it is undetectable due to the normal variation in the network delay. This limitation is discussed in Section 4.5.

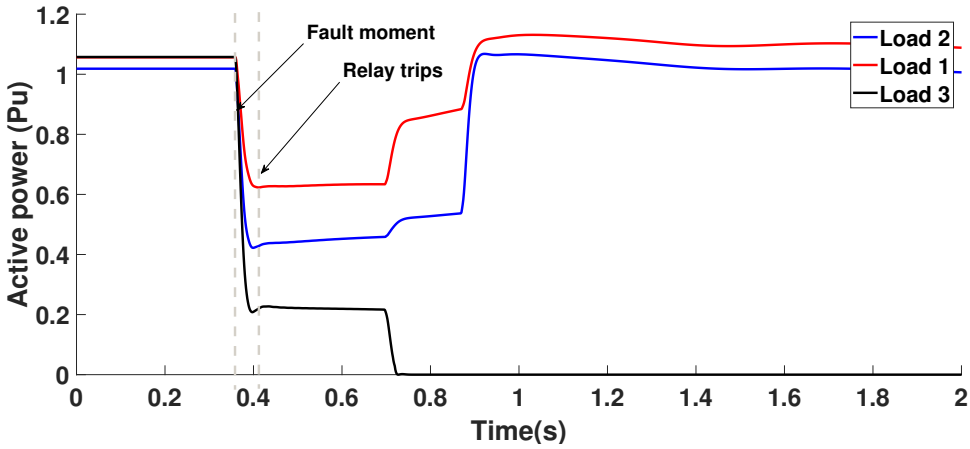


Figure 4.8: Scenario (S1) VRMS at each load.

4.4.2 Detection of Cyberattacks Targeting The Control System

The voltage regulation scheme of transformers is also a target for the attacker. It is also worth mentioning that the impact of the tap changer on the instability is dependent on the loading of the system. For instance, in a heavy load condition, reducing the tap changer can significantly decrease the voltage and force the protection systems to respond. Thus, the adversary can leverage the heavy loading condition of the system to target the voltage control scheme of the transformer when it can induce the largest instability.

4.4.2.1 Injecting GOOSE PDU with higher stNum

This attack (attack ID: G2) is similar to the GOOSE injection attack on the protection system, but instead targets the substation control. The attacker poisons the publisher-subscriber communication immediately after a fault. The attack occurs post-fault this time to make sure the tap changer

controller sends the "up-command" to increase the voltage to a safe level. As a result, the attacker causes the other commands to drop. Thus, the subscriber continues executing the "up-command," causing it to reach an over voltage scenario. Therefore, as demonstrated in S5 (see Table 4.6), the overvoltage relay detects the high voltage, trips the circuit breaker at the load, leading to a blackout as seen in Fig. 4.9. This attack can be detected on the protection system and the control system.

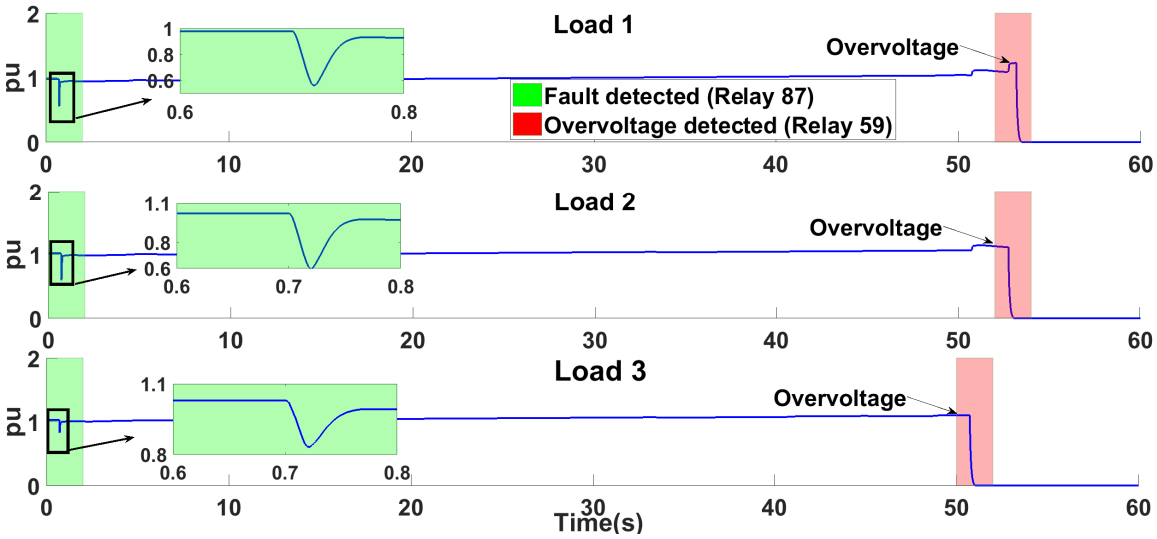


Figure 4.9: Scenario (S5) VRMS at each load.

4.4.2.2 Modify GOOSE PDU (Malformed PDU)

This attack (attack ID: G1) reduces the tap position to decrease the voltage to unsafe levels. To achieve this goal, the attacker modifies the transmitted message to change the "down-command" from 0 to 1. When the voltage reaches an unsafe level, the undervoltage relay detects the low voltage and trips the circuit breaker at the load. This scenario (S6) leads to a blackout, as presented in Table 4.6. In this case, since no MIB object can report this activity, the proposed detection approach is unable to recognize this attack. This limitation is discussed in Section 4.5.

Table 4.7: Effect of attacks on Network and System Management data objects

Attack	NSM DO changes
GOOSE injection: stNum poisoning	gSESL2RxPduPerSecond is higher during the injection attack than during normal operation.
GOOSE modification: stNum poisoning	There is no observable change on NSM DOs explored in this work. gSESL2MessageIntegrityFailCnt, if implemented using IEC 62351-6 specifications, increases by one for each modified packet that fails integrity checks.
GOOSE delay: TAL violation	gSESL2RxPduPerSecond during delay attack is lower than during normal operation. gSESL2TalExpCount increases by one for each packet that arrives after TAL of previous packet
GOOSE delay: skew	No change on NSM DOs explored in this work.

4.4.3 Results and Discussion

The impact of the attacks on the NSM data objects (DOs), in comparison with the behaviour of the DOs under normal conditions, is summarized in Table 4.7. Attacks that target the stNum GOOSE packet field in the injection attack are reflected on the "gSESL2RxPduPerSecond" NSM DO, which measures the number of GOOSE packets received by the subscriber over Ethernet. The "gSESL2RxPduPerSecond" DO will have a larger value during the injection attack compared to what is expected during normal operation. However, during the modification attack that does not introduce any additional fabricated packets, there are no NSM DOs explored in this chapter that will be affected, meaning they do not help detect the attack. This attack can still be detected if integrity checks are in place, where the "gSESL2MessageIntegrityFailCnt" DO would increment by one for each modified packet that fails the integrity check.

The GOOSE delay attack that causes TAL violations will be reflected on the "gSESL2RxPduPerSecond" DO. During this attack, the "gSESL2RxPduPerSecond" DO values will be lower than they are during normal operation. Also, the "gSESL2TalExpCount" counter will increment by one for each TAL violation.

On the other hand, GOOSE delay attacks that skew the packets over time without causing any TAL violations will not be reflected on any considered NSM DOs. The "gSESL2TalExpCount" will not increase, since the delayed packets are still within the bounds of the TAL. Also, the "gSESL2RxPduPerSecond" is unlikely to take on values that deviate significantly from those seen

during normal operation, since the delay at each moment is very small. Finally, Table 4.8 summarizes the vulnerabilities of each GOOSE PDU field.

Table 4.8: Vulnerabilities of each GOOSE PDU field

GOOSE PDU Field	Potential Attacks	Associated NSM DOs
gocbRef	Modify	gSESL2CBRef, gSEPL2CBRef
timeAllowedtoLive	Delay	gSESL2TalExpCnt
t (timestamp)	Delay	gSESL2TalExpCnt, gSESL2RxPduPerSecond, and gSEPL2TxPduPerSecond
stNum	Modify	None
sqNum	Modify	None
confRev	Modify	gSESL2ConfRevMis
ndsCom	Modify	gSESL2RxPduPerSecond

4.5 Security Assessment

In general, the NSM DOs defined in IEC 62351-7 can help detect various attacks targeting IEC 61850 substations. Yet, there are some cases where those DOs can only offer partial detection capabilities. The detection capabilities of NSM can be enhanced by defining existing NSM DOs more precisely or by adding new NSM DOs. When using data gathered from the communication network using NSM, it is important to detect attacks that cannot be identified from physical system measurements, such as DoS attacks. Our assessment includes both cases with and without the application of security extensions from other parts of IEC 62351

4.5.1 NSM and GOOSE/SV Protocols

NSM DOs in the Generic Substation Event (GSE) agent can assist in detecting many attacks against the GOOSE protocol as many of them track information related to potentially vulnerable fields in the PDUs. These are InErrCnt (malformed PDUs), DecryptFailCnt and MessageIntegrityFailCnt (AuthenticationValue from IEC 62351-6 [109]), TalExpCnt (TAL) and ConfRevMis (confRev) [15]. Any changes to these NSM DOs usually indicate a potential issue. Attacks that do not target these fields, such as the known attacks on the value of stNum, cannot be tracked in this manner. The remaining vulnerable fields are stNum, t, and the test flag. According to [15], the NSM DOs `TxPduPerSecond` and `RxPduPerSecond` track the rate at which PDUs are sent

and received each second. These DOs can be altered by flooding, injection, replay, delay, and drop attacks, and are used for attack detection. However, excluding flooding, we find that the attacker can perform such an attack and cause a change in these rates that is too small to distinguish normal system behavior from a cyberattack. Examples of such attacks include the injection or replay of a single PDU with a higher stNum, or introducing a very small delay between PDUs. Additionally, it is not specified how this rate must be calculated (e.g., whether it is an instantaneous rate or an average over many seconds). Thus, the rate of PDUs by itself is not sufficient to accurately detect such attacks. The NSM DOs RxPduPerSecond, TxPduPerSecond, and MessageIntegrityFailCnt, are also used for SV [15] and have the same detection capabilities for both protocols. In contrast to GOOSE, the NSM DOs for SV do not track information related to fields found in PDUs, possibly due to the high rate of SV traffic found in typical substations. This prevents NSM from being reliable for detecting attacks on fields other than AuthenticationValue, such as the timestamp from IEC 62351-6 [109] or smpCnt.

4.5.2 NSM and MMS Protocols

NSM DOs defined for MMS are effective at detecting several classes of attacks. As the NSM DOs track the total count for every kind of PDU sent and received [15], flooding, injection, replay, delay, and drop attacks are likely to leave attack traces. Attempts to tamper with authenticated PDUs are tracked by counters for PDUs that are erroneous or that cause decryption failure [15]. However, NSM cannot detect attacks that involve sniffing MMS PDUs or modifying them, though it should be noted that both of these are addressed by using Transport Layer Security (TLS) with MMS as per IEC 62351-4 [110].

4.5.3 Limitations of The NSM Solution

4.5.3.1 Legacy Equipment

Legacy IEDs produced prior to the release of IEC 62351-7 in 2017 [15] do not support the NSM DOs nor, in many cases, the SNMP protocol. Additional effort is required to implement IEC 62351-7 compatibility in either the IED itself or in a proxy [111]. The resulting implementation is likely to

differ across IED models due to their different characteristics and can be incomplete for IEDs that do not provide sufficient information [111].

4.5.3.2 Compromised Agents or Manager

The NSM system itself can be targeted by cyberattacks. As it relies on SNMP, vulnerabilities in this protocol can be potentially exploited. A monitored device that is compromised by an attacker can be modified to report false values for its NSM DOs. The data collected prior to the compromise and the data coming from unaffected hosts remain correct, and it might still indicate the presence of an attack. A compromise or a cyber attack aimed at the NSM manager renders the NSM solution ineffective. Hence, it is critically important to have a redundant NSM manager, to isolate the managers behind firewalls, to use the encryption and authentication features offered by SNMP version 3, and to deploy security countermeasures to complement the capabilities of NSM.

4.5.4 Recommendations

To enhance NSM capabilities and the security of the substation, we recommend a number of possible additions to the existing IEC 62351 standards.

4.5.4.1 GSE and SV NSM DOs

The following changes can enrich the data provided by NSM and ensure consistency across implementations: (1) Add a NSM DO for the total count of PDUs sent (publisher) and received (subscriber), similarly to the NSM DOs for MMS; (2) Add a NSM DO for the total count of received valid PDUs discarded for any reason (e.g., lower stNum) to locate potential cyberattacks.

4.5.4.2 GSE NSM DOs

We make the following recommendations: (1) Track the synchronization of publisher and subscriber by monitoring their latest stNum and t values, which can be accomplished by introducing new NSM DOs. Our suggestion is to add new NSM DOs to track last stNum, last t, time of last stNum change (based on host's local clock), a counter for the number of stNum resets, and the time

of last stNum reset; (2) Add an NSM DO to track the status of the test flag, similarly to the needs commissioning (ndsCom: indicates if the GOOSE control block needs more configuration) NSM DO that tracks the ndsCom flag.

4.5.4.3 SV NSM DOs

New NSM DOs can track statistics concerning the "skew" of PDUs to help detect potential attacks involving delays. In this context, we define the skew as the absolute difference between the timestamp in a PDU and the subscriber's local time, i.e., $|time_{local} - timestamp|$. Our suggestions for NSM DOs are: average, maximum, and minimum skew across many PDUs within a defined period, and count the PDUs with a skew exceeding a preset threshold.

4.6 Conclusion

Security monitoring for the IEC 61850 substations was of paramount importance given their role as a major component of the smart grid. The use of NSM enabled data collection, as specified in IEC 62351-7, to provide an additional layer of security. In this regard, this chapter presented the implementation of an NSM platform for a realistic IEC 61850 substation to enhance its resilience against cyberattacks. We deployed the substation model in a HIL framework with detailed modeling of power dynamics, protection measures, control schemes, communication, and NSM. We then proposed an anomaly detection solution on top of this model to identify cyberattacks using the statistical data and the values reported by the NSM data objects. We used the IEEE 9-bus system, including six substations, to show the effectiveness of the proposed ensemble machine learning-based cyber attack detection approach.

Chapter Five

Security Monitoring of IEC 61850 Substations Using IEC 62351-90-2 Deep Packet Inspection

This chapter introduces an anomaly detection system based on DPI that aims to strengthen the security of IEC 61850 communication networks in a power grid's substations. Given the increasing sophistication of cyberattacks that have been proven to be capable of bypassing detection through NSM data, our approach extends the principles outlined in IEC 62351-90-2 by implementing a DPI-driven anomaly detection framework specifically adapted for GOOSE traffic patterns.

The detection framework integrates local decision making, where an ensemble of two neural network models is used per relay to report anomalies, with a centralized validation technique used to collaboratively verify anomalies across other substations. The DPI agents deployed at each relay in the substation collect and inspect GOOSE packets, extracting critical features such as control signals and physical measurements. These features are then processed through a multi-step deep learning framework for anomaly detection. Once anomalies are detected, a centralized graph-based verification mechanism is used to collaboratively validate whether the detected anomalies are induced by a naturally occurring fault or a malicious action. The proposed system is validated using the testbed presented in chapter 3, demonstrating the importance of DPI deployment in alignment

with IEC 62351-90-2 recommendations.

The main contributions of this chapter can be summarized as follows.

(1) Designing DPI agents and integrating them into each substation to enhance monitoring and strengthen network security.

(2) Designing a deep learning-based detection framework to identify anomalies and cyber threats in substation communication.

(3) Implementing a graph-based verification mechanism to enable collaborative anomaly validation across substations and distinguish genuine faults from malicious activities.

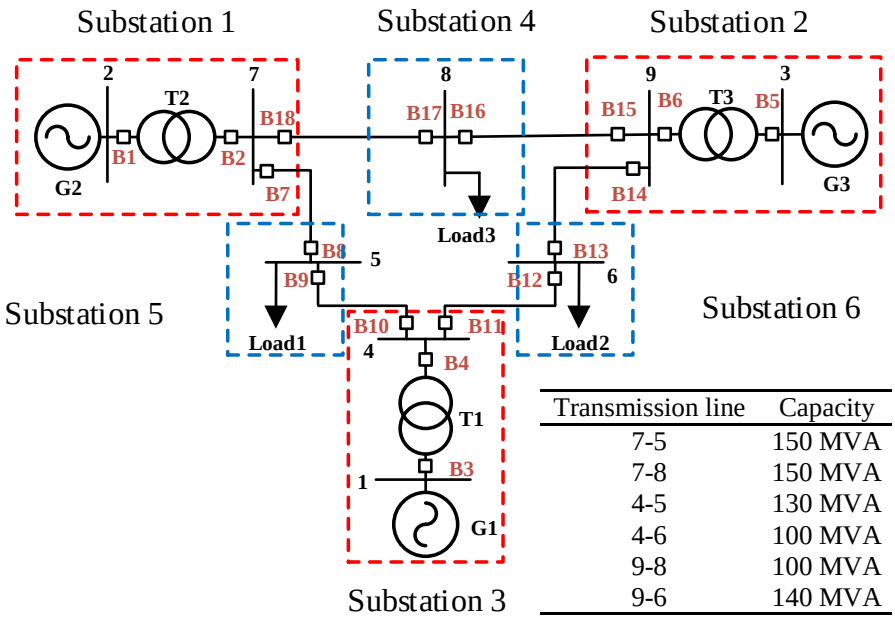
The remainder of the chapter is organized as follows. Related work is reviewed in Section 2.5.3. Section 5.1 presents the system model. The architecture and design of the proposed detection system are detailed in Section 5.2, while the anomaly detection scheme is described in Section 5.3. Section 5.4 introduces the graph-based verification technique used to validate anomalies. Experimental results and evaluations are discussed in Section 5.5, followed by concluding remarks along with directions for future research are provided in Section 5.6.

5.1 System Model

This section provides an overview of the smart-grid substation environment and the components of our DPI-based monitoring framework. We first describe the IEC 61850 communication architecture and the role and functionality of DPI agents deployed at each substation. We then present our threat model, detailing the types of cyber-physical disturbances and attack vectors considered in this work.

5.1.1 Power Layer

Our testbed uses the IEEE 9-Bus system shown in Fig. 5.1, consisting of three generation substations, three load substations, and interconnecting transmission lines. This layer simulates real-world power system behavior using dynamic 24-hour load profiles that reflect changes in reactive



Transmission line	Capacity
7-5	150 MVA
7-8	150 MVA
4-5	130 MVA
4-6	100 MVA
9-8	100 MVA
9-6	140 MVA

Figure 5.1: IEEE 9-Bus system scheme.

and active power demands. Voltage stability is ensured through voltage regulators that adjust tap changers in response to substation-level measurements.

5.1.2 Protection Layer

The protection layer includes circuit breakers and protection relays configured according to IEEE standards. Generation substations use distance (R21) and overcurrent (R51) relays. Load substations feature a combination of distance (R21), overcurrent (R51), overvoltage (R59), and undervoltage (R27) relays. These devices isolate faults and protect assets from abnormal operating conditions. Their performance depends on timely and accurate measurement data delivered via the communication layer.

5.1.3 Control Layer

The control layer comprises intelligent electronic devices (IEDs) and control logic responsible for maintaining normal operations. It includes local automation functions and supervisory control elements interacting with protection systems and measurement devices. Voltage regulation and

switching operations are handled based on control signals and state of the system derived from measurements at this layer.

5.1.4 Communication Layer

The communication layer facilitates data exchange between IEDs, controllers, and substations using IEC 61850 protocols. Our implementation uses Sampled Values (SV) for measurements, GOOSE for local control signals, and Routable GOOSE (R-GOOSE) for inter-substation communication. This layer operates on a virtualized network created using OpenStack, which mimics real-world traffic conditions and topologies.

5.1.5 Cybersecurity Layer

Since IEC 61850 lacks built-in security, we implement a cybersecurity layer that adheres to IEC 62351-90-2 recommendations. This layer includes Deep Packet Inspection (DPI) agents deployed across substations to monitor traffic and detect anomalies. The DPI agent inspects SV, GOOSE, and R-GOOSE traffic to identify malicious manipulation or delay attacks, enhancing the resilience of the control and protection systems. These agents enable localized detection at each substation while also working collaboratively to distinguish between cyberattacks and physical faults. This distributed detection approach improves the overall security, reliability, and resilience of the substation by allowing coordinated threat detection.

5.1.6 Co-simulation Testbed

The co-simulation testbed integrates the Hypersim real-time power grid simulator from OPAL-RT for simulating the behavior of our physical power grid layer with OpenStack to emulate its communication infrastructure. OPAL-RT enables real-time simulation of grid dynamics and interaction with physical IEDs using protocols like IEC 61850, Modbus, and DNP3, while OpenStack virtualizes the communication network and manages traffic via transparent bridges. DPI agents are deployed at each substation within the IEEE 9-bus system to monitor GOOSE, SV, and R-GOOSE traffic, extracting key data for a deep learning-based, multi-step intrusion detection system.

5.1.7 Threat Modeling

Our detection strategy relies on deploying DPI agents at each substation to monitor IEC 61850 traffic and extract key data such as control signals and physical measurements. We assume attackers may gain access to one or more substations, potentially compromising IEDs, but without full control over the entire network. The threat model is based on the following assumptions:

(1) The attacker has detailed knowledge of both the IT and operational infrastructure.

(2) They can remain undetected for extended periods to achieve their objectives.

(3) They are capable of injecting, capturing, replaying, modifying, dropping, and delaying messages within compromised substations.

Our system is tested against both simple and advanced attack scenarios, particularly those undetected in our previous work [112]. Two specific advanced attacks are modeled:

(1) GOOSE PDU modification with elevated state number (stNum): The attacker modifies the stNum in a GOOSE message to a higher value, causing the subscriber to reject legitimate future messages from the original publisher, as they appear outdated.

(2) GOOSE PDU delay beyond skew period: The attacker gradually delays each GOOSE packet to avoid detection, eventually violating the `timeAllowedtoLive` threshold, causing the subscriber to reject the expired packets.

The lack of existing mechanisms of detecting such attacks emphasizes the need for a detection mechanism capable of identifying cyberattack targeting IEC 61850-based substations.

5.2 Architecture of the Multi-Step Detection System

This section outlines the strategies behind the multi-step detection system. Key challenges include the potential compromise of IEDs or substation devices, limited time for attack detection depicted in Fig. 5.3, and handling diverse data from IEC 61850 protocols. However, the interconnected nature of substations provides a valuable advantage, i.e., real faults often affect multiple substations, creating redundant data points, enhancing detection reliability.

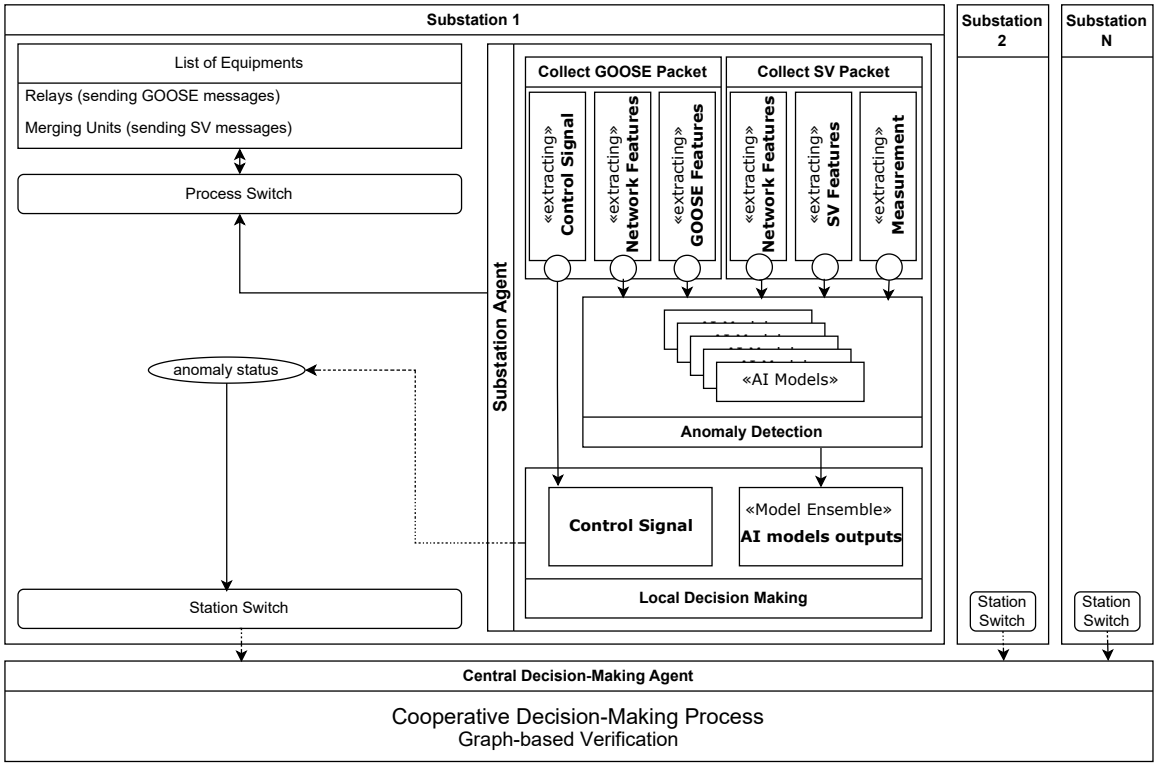


Figure 5.2: Architecture of the proposed multi-step detection

To address these challenges, the system employs the following strategies:

(1) Protocol-specific focus: The system is designed to work with GOOSE protocols with the compatibility needed to extend the approach to SV, ensuring it meets the specific needs of substation networks.

(2) Multi-model approach: Using different models for analyzing network measurements, PDU fields, and payload data improves detection accuracy by covering a wider range of issues.

(3) Robust anomaly detection with deep learning: Incorporating deep learning enhances the system's ability to detect subtle changes and patterns in large datasets, aiding in threat detection.

(4) Ensemble-driven detection at each substation: Every relay runs two AI models and combines their results. A substation is flagged as anomalous if any of its relays report an anomaly.

(5) Central cooperative verification and decision making: The central system analyzes data from

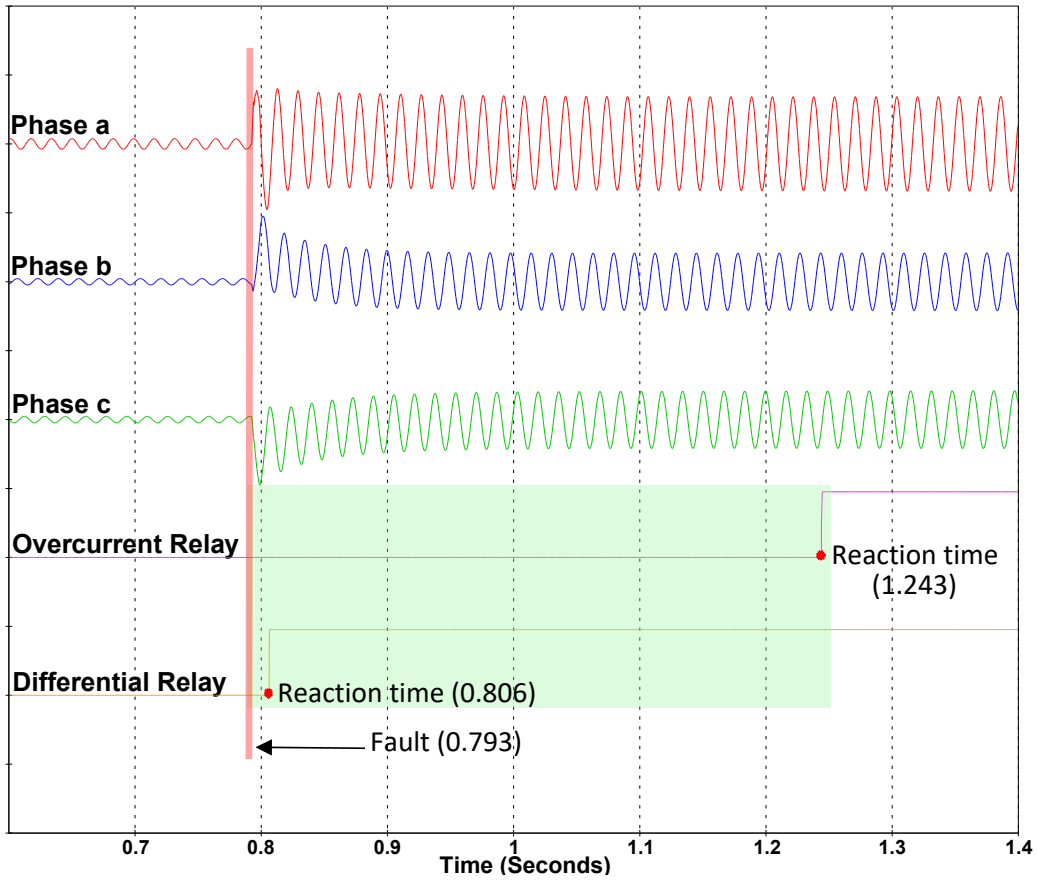


Figure 5.3: Reaction time of the protection system to a fault.

multiple substations to improve detection accuracy and reduce false alarms, ensuring a coordinated response to anomalies.

Based on the outlined strategies, our multi-step detection system is designed for secure and efficient monitoring of substations by leveraging DPI agents to analyze data from SV and GOOSE protocols. This architecture is illustrated in Fig. 5.2. While the system supports both SV and GOOSE protocols to ensure the reliability of substation operations, this work focuses on detecting anomalies in GOOSE communications.

5.2.1 Data Extraction and Organization

In the first phase, the DPI agents extract data from the GOOSE packets. The extracted data are then organized into specific categories for further analysis:

(1) Network statistics: Measurements that provide information on network activity and performance.

(2) GOOSE PDU fields: Data from GOOSE PDUs, including key protocol parameters.

(3) Control signals: Important payload signals that are essential for substation control operations.

5.2.2 Anomaly Detection Using Specialized Models

In this step, each relay runs two AI prediction models to boost detection accuracy. These models, trained on historical "normal" behavior, continuously monitor live GOOSE traffic and flag anomalous behaviour by:

- Learning typical packet travel times and flagging unusual delays.
- Learning normal intervals between packets and flagging irregular gaps.

By learning these two features, the models can learn the long-term and short-term patterns, trends, and statistical properties of normal packet delays.

5.2.3 Local Decision Making

This step of the detection process, performed by each DPI agent at the substation, takes the outputs of two models at each relay, computes a combined error score for each relay, and then aggregates across all relays in the substation. Each relay runs two AI models, one that learns normal packet latency and one that learns normal inter-arrival times. We then combine the results of these two models into a single error score by calculating the Root-Mean-Square Error (RMSE) between the predicted and observed latency and inter-arrival time for each relay. A relay is flagged as anomalous whenever its RMSE exceeds a threshold, th, determined empirically during training. This indicates that the observed latency and interarrival time deviate significantly from their predicted values. At the substation level, if any relay is flagged as anomalous, the substation reports an anomaly to the central decision-making mechanism discussed below.

5.2.4 Central Cooperative Decision Making

Centralized decision-making is essential for ensuring the consistency and reliability of fault detection in power substations. In the proposed multi-stage detection framework, each substation performs local anomaly detection and transmits its results to a central unit. This unit leverages a graph-based verification process to improve decision accuracy, which considers the physical topology of the network. The power grid is represented as a graph where the power lines are edges and the buses are the graph nodes. The edge weights are then assigned based on the line parameters and the propagation time of errors from one node to the other. This allows the graph to capture the normal fault propagation behavior in the power grid. This graph is then divided into communities based on the strength of the relation between the connected nodes. Finally, when an anomaly is flagged at a given substation, the propagation of this anomaly is verified within each community it appears in and a majority vote is then taken to determine whether it follows the expected fault propagation pattern. This graph-based approach is used to classify whether the detected anomalies are naturally occurring faults or malicious attacks.

5.3 Anomaly Detection

In what follows, we describe how we leverage the extracted data to build anomaly detection models capable of detecting anomalies at the relay and substation levels.

5.3.1 Data Preprocessing and Feature Engineering

To enable our model training, we collect data from the smart-grid testbed via the DPI architecture. Two raw time fields (the GOOSE PDU send time and the packet received time) are validated and used to compute additional timing features required to generate a data set suitable for detecting modification and delay attacks. All measurements are then normalized (Z-score and Min–Max) to ensure consistent feature scaling. We then enrich this timing information with a suite of derived features: rolling statistics, inter-arrival and timestamp deltas, and lag values that capture both short-term variability and longer-term temporal patterns in the traffic [113–115]. This combination of raw timing and engineered statistics produces a structured input set optimized for our AI-based anomaly

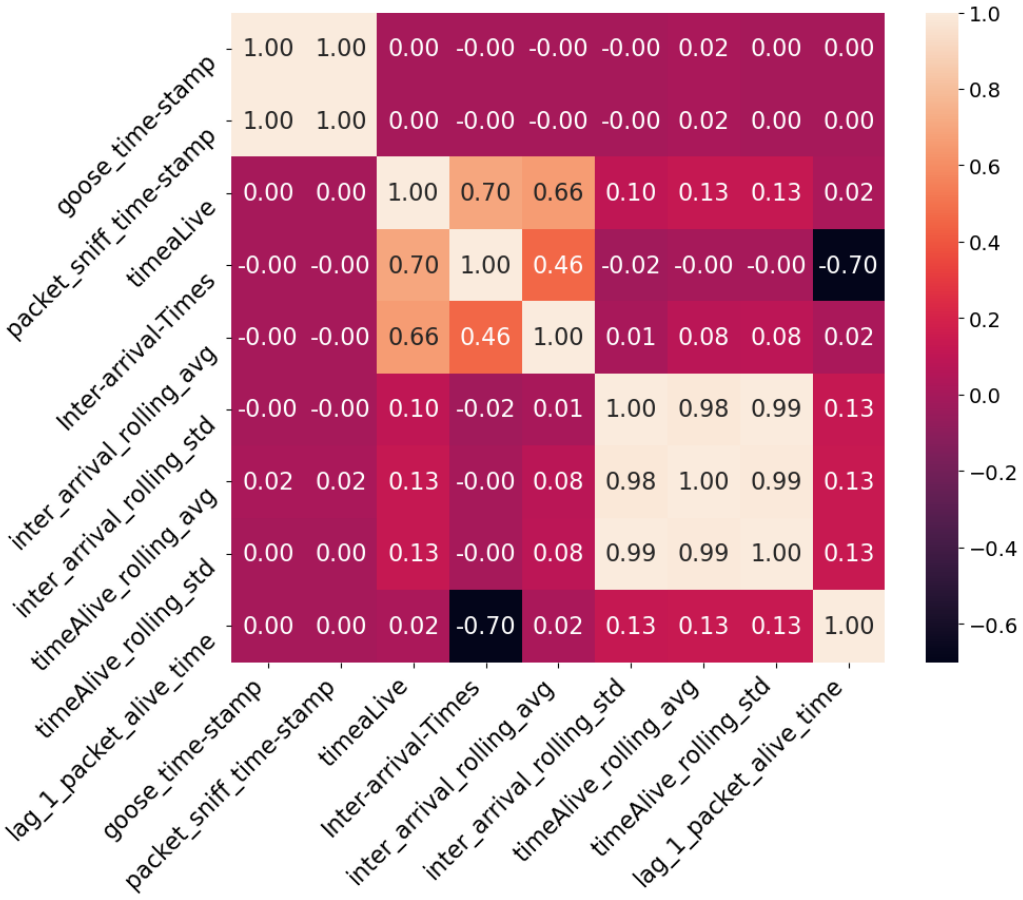


Figure 5.4: Correlation heatmap of engineered features.

detectors.

5.3.2 Feature Correlation and Selection

To gain a better understanding of the relationships among the extracted/engineered features, we computed the Pearson correlation matrix illustrated in Fig. 5.4. The analysis reveals that the features "timealive" and "Inter-arrival-Times" exhibit strong correlations with several others. Notably, the "timeaLive" feature, which represents the time difference between packet sniffing and GOOSE message timestamps, shows a strong positive correlation with both the "Inter-arrival-Times" (0.70) and the "rolling average of inter-arrival times" (0.66). It also maintains a loose correlation with three additional statistical features of the alive time and inter-arrival time. Similarly, the "Inter-arrival-Times" feature shows strong correlations with the "timealive" and the "rolling average of

inter-arrival times". It also exhibits a strong negative correlation (-0.70) with the "lagged value of timeaLive". This inverse relationship indicates that shorter inter-arrival times are often associated with increased timing discrepancies in consecutive packets. Given their strong correlations with other key features, we select "timealive" and "Inter-arrival-Times" as the primary features to be predicted by our local anomaly detection models. These predicted values are then compared to the observed values to identify potential anomalies. This approach ensures that the most informative features are prioritized, while less relevant features are excluded from the prediction process. As a result, the model maintains a compact size without compromising its performance. We note that the first two raw data features exhibit no correlation to the remaining engineered features. Raw features are not meaningful before useful information (the engineered features) is extracted from them.

5.3.3 Anomaly Detection Model Construction Approach

The central idea is to learn the normal operational behavior of each substation by extracting time-series features from consecutive GOOSE packets and training predictive models on this data. During a normal operating period, a set of feature vectors is extracted, where each vector at time t is denoted as D_t in (1), where d_{it} represents the value of feature i at time t, and m is the total number of features.

$$D_t = (d_{1t}, d_{2t}, \ldots, d_{mt}) \tag{5.1}$$

A prediction model (PM) is then trained to forecast the next feature vector based on a sliding window of previous vectors:

$$X_t = (D_{t-p}, D_{t-p+1}, \ldots, D_{t-1},) \tag{5.2}$$

where p is the prediction window size. There are two models per relay. Each model is trained to predict a single feature at time t, and the resulting prediction error (the difference between predicted and observed values). One model forecasts packet-alive latency, while the other forecasts inter-packet arrival time. The difference between predicted and observed values is used to calculate RMSE for each model and the RMSE of the combined model per relay.

$$E = \frac{1}{2}\left[\left(\frac{y_{\text{obs}} - y_{\text{pred}}}{y_{\text{obs}}}\right)^2 + \left(\frac{x_{\text{obs}} - x_{\text{pred}}}{x_{\text{obs}}}\right)^2\right] \tag{5.3}$$

where

- y_{obs}, y_{pred} are the observed and predicted inter-arrival times, and
- x_{obs}, x_{pred} are the observed and predicted packet latencies.

To detect anomalies, the two models per relay perform their predictions and compare the actual observed features to calculate the combined score E. If E exceeds a pre-defined threshold th, an anomaly is flagged for that relay at time t. Threshold th is determined empirically during training. By also calculating the RMSE per model, this structure allows the anomaly detection process to pinpoint which specific feature experienced the anomalous behavior.

5.3.4 Machine Learning Algorithms

For anomaly detection in time-series data, we use three machine learning algorithms: LSTM networks, Simple Recurrent Neural Networks (RNN), and GRU and compare their performance to select the best-performing algorithm. These algorithms are well-suited for handling sequential data and capturing temporal dependencies, which is required when dealing with delay attacks. Each of these models, however, deals with time series data in a slightly different manner. LSTM networks address the issue of vanishing gradients and use memory cells and gates to remember information over long and short periods, making them effective in capturing dependencies and patterns in temporal data. Simple-RNNs are a basic form of RNN that update their hidden state based on the current input and the previous hidden state making them simple and fast. However, these RNNs struggle to capture long-term dependencies in temporal data. GRU are a variation of RNNs that use gates that regulate how information is passed through the network. This allows for more efficient computation and faster than LSTM, but better than RNNs at capturing temporal data dependency.

The choice of different machine learning models in this work was driven by the nature of the anomaly detection tasks and the characteristics of the data streams. Long Short-Term Memory (LSTM) networks were employed in scenarios where capturing long-term temporal dependencies

was essential, such as delay-induced anomalies that evolve gradually over time. Simple-RNN models served primarily as lightweight baselines, allowing a direct comparison of accuracy versus computational complexity. This comparative approach ensured that model complexity and performance requirements were appropriately balanced for real-time anomaly detection in IEC 61850 substations.

5.3.5 Evaluation Metrics

To evaluate the models' performance, we use the True Positives (TP), False Positives (FP), True Negatives (TN), and False Negatives (FN). We also use standard machine learning evaluation metrics, i.e., (i) Accuracy to measure the proportion of overall correct predictions, (ii) Precision to measure the reliability anomaly predictions, (iii) Recall to evaluate the percentage of actual anomalies that were correctly classified, and (iv) F1-score to provide a harmonic mean of precision and recall, offering a balanced measure when dealing with class imbalance.

5.3.6 Model Architectures and Hyperparameter Tuning

We implemented and compared the three neural networks, i.e., LSTM, RNN and GNN, using an identical set of hyperparameters selected via exhaustive grid search. Each model comprises two stacked recurrent layers, having a ReLU activation function. The first layer returns the full sequence to its successor, while the second layer outputs only its final hidden state. A single linear neuron is follows the final hidden layer and is used to predict the continuous target.

All models are trained with the RMSprop optimizer (learning rate 1×10^{-4}), minimizing the mean squared error (MSE) and monitoring mean absolute error (MAE) as the performance metric. We set the sequence length (`n_steps`) to 10, batch size to 32, and apply no dropout (rate = 0.0). This configuration is identified as the optimal set of hyperparameters through grid search.

5.4 Graph-based Verification

This section demonstrates how graph-based modeling and community analysis are used to verify the consistency of fault propagation in the substation network.

5.4.1 Graph Construction

The structure of the power substation network is captured using an undirected graph $G = (V, E)$, where V is the set of all substations, each node $v_i \in V$ represents a substation, and each edge $e_{ij} = \langle v_i, v_j \rangle$ where v_i and $v_j \in E$ represents a direct physical connection between substations v_i and v_j. Each edge is associated with a propagation delay t_{ij}, which denotes the time (in milliseconds) it takes for a fault to propagate from one substation to another. The set of propagation delays is derived from realistic simulations of fault scenarios on a power system modeled with dynamic load conditions using a 24-hour load profile. Faults were simulated at different times throughout the day to reflect varying grid states, and the propagation delay (from one substation to the next, i.e., fixed distance) across these scenarios was used to represent the expected latency under normal operating conditions. The result is a weighted graph where edge weights capture the temporal dynamics of fault propagation. These results are used to construct the graph in Fig. 5.5.

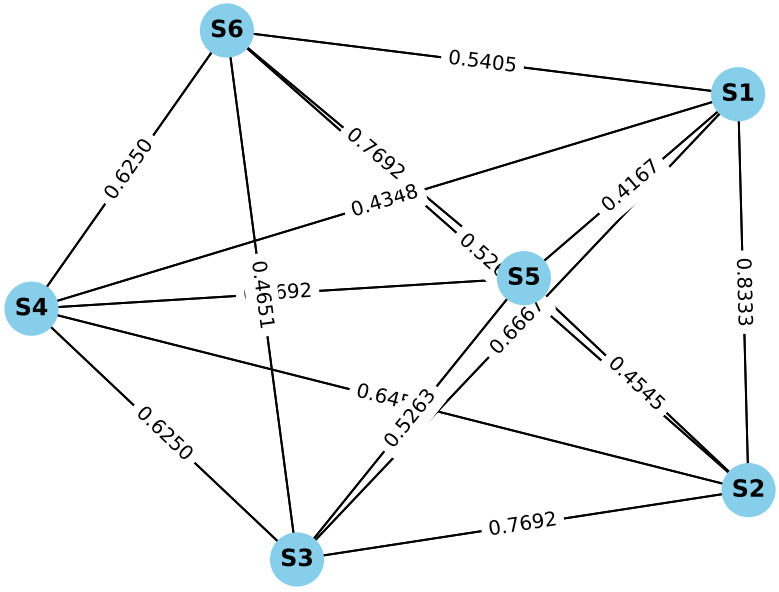


Figure 5.5: Weighted graph based on fault propagation.

5.4.2 Community Detection and Fault Clustering

To capture localized fault behavior, overlapping communities are identified using a modularity-based approach [116] tailored to the characteristics of the substation network. While the standard

Louvain method typically produces non-overlapping communities, our approach extends this by allowing substations to participate in multiple communities based on the strength of their connections. This flexibility is important in power systems, where a single substation may take part in different fault propagation paths or regions of influence.

This approach is performed offline before deployment and is scalable to larger grids. Since the size of the individual communities depends on the connection of each substation to its neighbors and is independent from the size of the entire grid, community sizes remain limited to a small number of nodes per community.

In this method, each edge in the graph is given a hybrid weight that reflects both physical and dynamic relationships. Specifically, it combines a physical link score ($phys_{ij}$), which is 1 if the two substations are directly connected and 0 otherwise, and a propagation closeness score, which represents a shorter fault propagation delay between the two substations. The final edge weight w_{ij} is computed as:

$$w_{ij} = \alpha \cdot \text{phys}_{ij} + (1 - \alpha) \cdot \left(\frac{1}{t_{ij} + 1} \right) \tag{5.4}$$

where t_{ij} is the propagation delay from node i to node j, and α is a tunable coefficient that controls the importance of each component. The parameter α emphasizes the physical layout of the network, while $(1 - \alpha)$ emphasizes how quickly a fault is likely to spread from one substation to another. Adjusting these values allows the graph to reflect both the static structure and the dynamic behavior of fault propagation. In this work, we assume $\alpha = 0.5$ to assign equal importance to both components.

To detect communities, a modularity-based edge scoring function is applied [116]. For each edge, $e_{ij} = (v_i, v_j)$, the modularity contribution is computed as:

$$Q_{ij} = w_{ij} - \frac{k_i \cdot k_j}{2m} \tag{5.5}$$

where k_i and k_j are the sum of the weights of all edges connected to nodes i and j, and m is the sum of all edge weights in the graph. A positive score means the connection between i and j is strong, indicating they belong to the same community.

Nodes are grouped with the neighbors with which they have a positive score, leading to overlapping communities. This overlapping structure helps the system identify shared risk areas, meaning it can identify groups of substations that are likely to be affected together by a fault, rather than isolating each substation and examining it independently. Each community $C \subseteq V$, where C is a group of substations and V is the set of all substations, goes through a two-stage fault verification process:

(1) Propagation consistency check: Let $\mathcal{C}$ be a community of substations. For each substation, node, $v_i \in \mathcal{C}$ that reports an anomaly, it is considered a candidate fault origin. Let Reported($\mathcal{C}$) $\subseteq \mathcal{C}$ be the set of substations in $\mathcal{C}$ that reported anomalies.

$$\text{Reported}(\mathcal{C}) = \{v_1, v_2, \ldots, v_m\} \quad \text{where } m = |\text{Reported}(\mathcal{C})| \tag{5.6}$$

Within each community, define the expected propagation order from v_i as:

$$\text{Ordered}_{v_i}(\mathcal{C}) = \langle v_1, v_2, \ldots, v_n \rangle \quad \text{such that } t_{i,j} \leq t_{i,j+1} \text{ where } j \leq n \tag{5.7}$$

such that the nodes are ordered by increasing propagation time t_{ij} from the origin node v_i to each of the other nodes v_j.

The propagation is considered consistent if Reported($\mathcal{C}$) matches the beginning of Ordered$_{v_i}(\mathcal{C})$. In simple terms, if the substations that reported anomalies appear in the same order as expected from the naturally occurring fault propagation sequence, the propagation is considered consistent with fault behavior.

(2) Majority threshold rule: Let n be the total number of substations in C, and $n^{\text{anomalous}}$ be the number of substations reporting an anomaly. The community is marked as "verified anomalous" if:

$$\frac{n_k^{\text{anomalous}}}{n_k} > \theta \tag{5.8}$$

where θ is a tunable threshold. In this work, we set $\theta = 0.5$ as a reasonable default to reflect a simple majority requirement. This value assumes that an anomaly is more likely to be valid if

observed by over half the substations in the community. While we did not perform extensive tuning of θ, this threshold provides a practical starting point and can be adjusted in future work based on operational requirements or validation data.

5.4.3 Global Anomaly Score and Decision

After verifying each community, the system computes a global anomaly score to quantify the overall confidence in system faults or attacks where:

- $N_{\text{verified\_anomalies}}$ be the number of communities that have been confirmed as anomalous (i.e., passed the fault verification checks),
- $N_{\text{reported\_anomalies}}$ be the number of communities that had at least one substation reporting an anomaly.

Then, the global anomaly score α is defined as:

$$\alpha = \frac{N_{\text{verified\_anomalies}}}{N_{\text{reported\_anomalies}}} \tag{5.9}$$

This scalar $\alpha \in [0, 1]$ represents the confidence level in identifying fault or attack behavior across the substation network. A lower value of α indicates more widespread inconsistencies, suggesting a higher likelihood of attacks.

5.5 Experimental Evaluation

This section presents the experimental setup and methodology used to validate our anomaly detection and graph-based verification framework. We describe the data generation procedures, including delay attacks and fault scenarios, evaluation metrics, and the comparative performance of the LSTM, GRU, and Simple-RNN models.

5.5.1 Simulation of Delay Attacks and Fault Scenarios

To thoroughly evaluate our detection framework under realistic operating conditions, we synthesized three classes of test data:

- Normal (no fault): GOOSE packet streams without any attacker-injected delays or system faults.
- Delay attacks: A simulated delay on the system traffic in the range 300–1000 microseconds (μs), reflecting real delay attacks.
- Normal faults: Physical fault events triggered at 13 distinct locations within the substation network.

Across all scenarios, we assembled a balanced dataset of approximately 36000 packet windows, split evenly between normal traffic and abnormal streams (delay attacks *plus* normal-fault traffic). For each of the 13 fault locations, we captured consecutive packets immediately following the event, ensuring coverage of diverse network loads and temporal patterns.

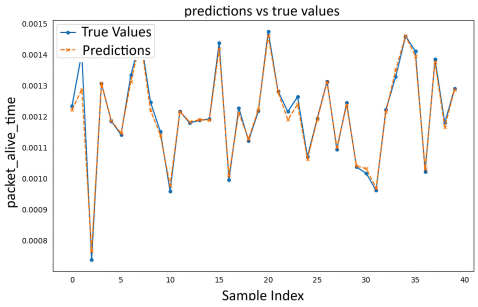
Each of these 13 fault locations represents a list of possible faults that could occur at any specific location on a given line.

5.5.2 Local Anomaly Detection

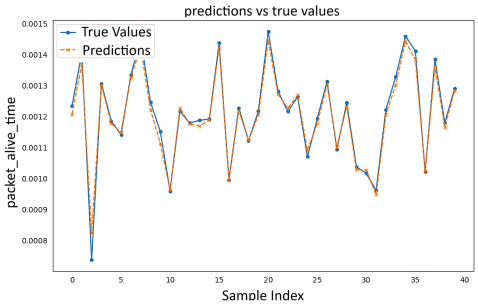
The trained models were able to detect delay attacks with delays as small as 0.3 milliseconds. This level of sensitivity is critical for real-time anomaly detection and quick response to potential threats.

Fig. 5.6a, 5.6b, and 5.6c illustrate the alignment between the predicted and the actual packet alive time under normal operating conditions. These results demonstrate each model's ability to accurately replicate system behavior, capturing both short-term fluctuations and long-term temporal patterns. Such predictive accuracy is essential for reliable anomaly detection, as deviations from these learned patterns indicate potential cyberattacks or abnormal events.

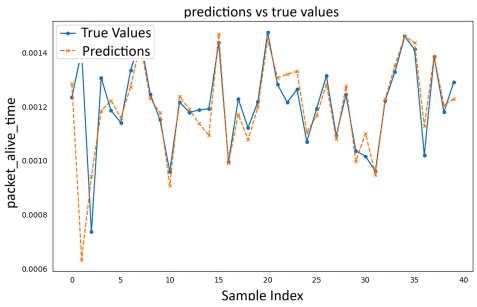
The detection results are then evaluated using the different performance metrics in section 5.3.5). This evaluation provides key insights into the strengths and limitations of each model.



(a) LSTM Model



(b) GRU Model



(c) Simple-RNN Model

Figure 5.6: Predictions vs. true values for LSTM, GRU, and Simple-RNN models.

Table 5.1: Average performance of the LSTM model

Relay Type	**Accuracy**				**Precision**				**Recall**				**F1-Score**			
	Avg.	σ	Min	Max	Avg.	σ	Min	Max	Avg.	σ	Min	Max	Avg.	σ	Min	Max
Distance Relays	0.984	0.014	0.956	0.999	0.977	0.025	0.924	0.998	0.991	0.012	0.966	1.000	0.984	0.014	0.957	0.990
Overcurrent Relay	0.982	0.011	0.966	0.998	0.976	0.016	0.945	0.999	0.988	0.020	0.945	0.999	0.982	0.011	0.965	0.998
Overvoltage Relay	0.987	0.002	0.984	0.990	0.980	0.009	0.969	0.991	0.993	0.009	0.980	1.000	0.987	0.002	0.984	0.990
Undervoltage Relay	0.984	0.007	0.975	0.989	0.986	0.002	0.984	0.990	0.982	0.016	0.959	0.994	0.984	0.007	0.974	0.989

The LSTM model effectively captured long-term dependencies using its memory cells and gating mechanisms, resulting in high accuracy and recall. The average model performance per relay type is presented in Table 5.1. On average, the models achieved a precision of 98%, a recall of 99%, and an F1 score of 98%. The results confirm both high sensitivity and specificity in distinguishing normal and anomalous traffic. The detailed tables presenting the performance metrics and the confusion matrix of the LSTM models per individual relay are presented in Table 5.5 Table 5.6 in Section 5.5.4.

The Simple-RNN model, while limited by the vanishing gradient problem and poor performance on longer delays, still detected minor delays reasonably well. The metrics used to evaluate the

Table 5.2: Average performance of the RNN model

Relay Type	Accuracy				Precision				Recall				F1-Score			
	Avg.	σ	Min	Max	Avg.	σ	Min	Max	Avg.	σ	Min	Max	Avg.	σ	Min	Max
Distance Relays	0.949	0.013	0.922	0.965	0.943	0.023	0.894	0.965	0.956	0.012	0.930	0.970	0.949	0.013	0.925	0.965
Overcurrent Relay	0.949	0.010	0.932	0.965	0.942	0.014	0.917	0.965	0.958	0.014	0.913	0.967	0.950	0.010	0.930	0.965
Overvoltage Relay	0.958	0.005	0.953	0.965	0.952	0.008	0.945	0.963	0.966	0.003	0.961	0.968	0.959	0.005	0.953	0.965
Undervoltage Relay	0.946	0.014	0.930	0.965	0.956	0.006	0.949	0.963	0.934	0.024	0.909	0.966	0.945	0.015	0.929	0.965

Table 5.3: Average performance of the GRU model

Relay Type	Accuracy				Precision				Recall				F1-Score			
	Avg.	σ	Min	Max	Avg.	σ	Min	Max	Avg.	σ	Min	Max	Avg.	σ	Min	Max
Distance Relays	0.971	0.014	0.943	0.986	0.964	0.025	0.912	0.987	0.978	0.012	0.953	0.988	0.971	0.013	0.946	0.986
Overcurrent Relay	0.971	0.009	0.954	0.987	0.963	0.015	0.939	0.986	0.981	0.015	0.932	0.989	0.972	0.009	0.953	0.987
Overvoltage Relay	0.980	0.006	0.974	0.987	0.974	0.008	0.967	0.985	0.986	0.003	0.981	0.989	0.980	0.006	0.974	0.987
Undervoltage Relay	0.967	0.013	0.954	0.986	0.978	0.005	0.973	0.985	0.955	0.022	0.933	0.986	0.967	0.014	0.953	0.986

average performance of the model by relay type are presented in Table 5.2. On average, the models achieved a precision of 94%, a recall of 95%, and an F1 score of 95%. Its simplicity and low computational cost make it suitable for resource-constrained environments. The detailed tables presenting the performance metrics and the confusion matrix of the RNN models per individual relay are presented in Table 5.7 Table 5.8 in Section 5.5.4.

The GRU model offers a strong balance between simplicity and performance, training faster than LSTM while maintaining good accuracy and recall, particularly for small to moderate delay attacks. The average model performance per relay type is presented in Table 5.3. On average, the models achieved a precision of 96%, a recall of 98%, and an F1 score of 97%. The detailed tables presenting the performance metrics and the confusion matrix of the RNN models per individual relay are presented in Table 5.9 Table 5.10 in Section 5.5.4.

These results demonstrate that all three models perform well in detecting large delay attacks close to the attack boundary of 1000 µs, achieving high precision and recall. However, only the LSTM and GRU were able to accurately detect small delays around 300 µs, while the RNN model fails to detect the majority of these small attacks. Overall, the LSTM and GRU demonstrated better generalization with lower false-positive and negative rates. However, the LSTM models proved to be the most effective, reliable, and accurate for real-time detection of delay attacks in GOOSE networks, making them suitable for practical deployment.

5.5.3 Graph Construction and Anomaly Verification

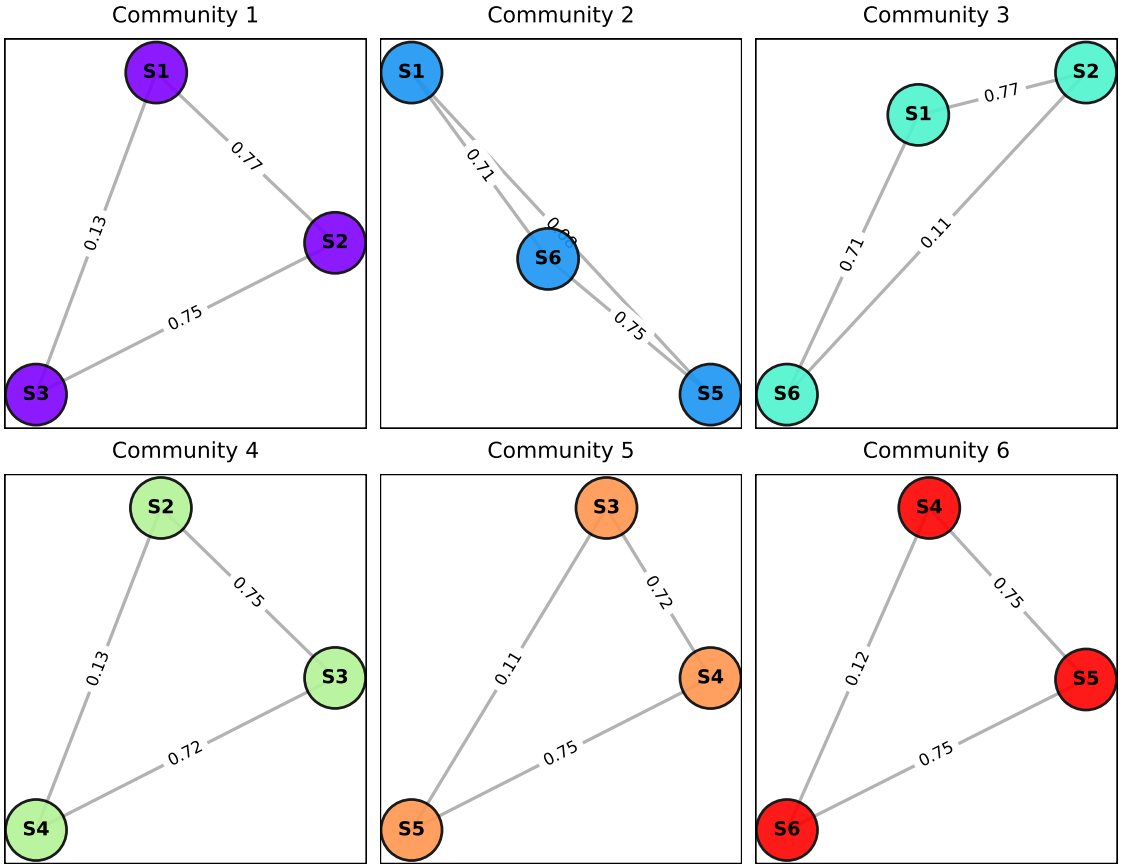


Figure 5.7: Overlapping communities.

The hybrid graph combining the physical connections and the simulated fault delays is constructed for the test grid, and the overlapping clusters (detected communities) are identified. These communities are presented in Fig. 5.7. Our graph-based verification approach achieved high accuracy across all thirteen simulated fault scenarios (F1–F13). For each possible fault, we count the number of communities that report the fault and then verify the expected propagation order. An anomaly is classified as a fault only after the majority of the involved communities verify it as a fault. Otherwise, it is considered an attack. Table 5.4 demonstrates that our graph-based community method can correctly distinguish between faults and attacks. This table also demonstrates the confidence with which each fault is classified. The results demonstrate that in the majority of cases, all involved communities accurately capture the fault behavior and report it correctly. Yet even for 4

of these cases, where the confidence drops to 0.67, this indicates that two-thirds of the communities were able to verify the corresponding faults. In case of attacks, only 0 or 1 communities were able to verify them as faults, failing to achieve a majority, thus classifying them as attacks. This method can thus successfully extend our anomaly detection by differentiating whether an anomaly is due to a fault or the result of a delay attack.

Table 5.4: Graph-based verification per fault location

Fault	Location	Reported	Verified	Confidence	Decision
F1	Bus 2	3	2	0.67	Normal
F2	Transmission line (1-2)	2	2	1.00	Normal
F3	Bus 8	3	2	0.67	Normal
F4	Transmission line (2-3)	2	2	1.00	Normal
F5	Bus 9	2	2	1.00	Normal
F6	Transmission line (3-4)	3	3	1.00	Normal
F7	Bus 6	3	3	1.00	Normal
F8	Transmission line (4-5)	2	2	1.00	Normal
F9	Bus 4	2	2	1.00	Normal
F10	Transmission line (5-6)	2	2	1.00	Normal
F11	Bus 5	3	2	0.67	Normal
F12	Transmission line (6-1)	2	2	1.00	Normal
F13	Bus 2	3	2	0.67	Normal

The end-to-end detection latency, from GOOSE packet capture to anomaly verification, was evaluated on our testbed. Feature extraction and preprocessing take under 0.3 ms, while the LSTM-based inference adds between 0.5ms and 1.0 ms. Including the time needed to transmit the anomaly detection results and perform the graph-based verification, the total latency of the overall approach remains within 2–4 ms. This meets the strict timing requirements of IEC 61850 protection schemes making our proposed approach suitable for deployment in such a time-constrained application.

5.5.4 Performance Metrics and Confusion Analysis per Relay

This section presents the detailed tables containing the confusion matrices and performance metrics of the LSTM, RNN, and GRU models per relay.

Table 5.5: Performance metrics for LSTM model per relay

Relay	Substation	Accuracy	Precision	Recall	F_1 Score
Distance relay 1	1	0.999	0.998	1.000	0.999
Distance relay 2	1	0.997	0.997	0.997	0.997
Overcurrent relay 1	1	0.998	0.998	0.998	0.998
Overcurrent relay 2	1	0.992	0.984	0.999	0.992
Distance relay 1	3	0.986	0.975	0.998	0.987
Distance relay 2	3	0.979	0.992	0.966	0.978
Overcurrent relay 1	3	0.977	0.959	0.997	0.978
Overcurrent relay 2	3	0.985	0.976	0.995	0.985
Distance relay 1	5	0.956	0.924	0.994	0.957
Distance relay 2	5	0.984	0.977	0.992	0.984
Overcurrent relay 1	5	0.973	0.951	0.997	0.973
Overcurrent relay 2	5	0.966	0.986	0.945	0.965
Distance relay 1	2	0.999	0.998	1.000	0.999
Distance relay 2	2	0.986	0.975	0.998	0.987
Overcurrent relay 1	2	0.998	0.998	0.998	0.998
Overcurrent relay 2	2	0.977	0.959	0.997	0.978
Overvoltage relay	2	0.990	0.980	1.000	0.990
Undervoltage relay	2	0.975	0.990	0.959	0.974
Distance relay 1	4	0.979	0.992	0.966	0.978
Distance relay 2	4	0.984	0.977	0.992	0.984
Overcurrent relay 1	4	0.985	0.976	0.995	0.985
Overcurrent relay 2	4	0.966	0.986	0.945	0.965
Overvoltage relay	4	0.984	0.969	1.000	0.984
Undervoltage relay	4	0.989	0.985	0.993	0.989
Distance relay 1	6	0.997	0.997	0.997	0.997
Distance relay 2	6	0.956	0.924	0.994	0.957
Overcurrent relay 1	6	0.992	0.984	0.999	0.992
Overcurrent relay 2	6	0.973	0.951	0.997	0.973
Overvoltage relay	6	0.986	0.991	0.980	0.986
Undervoltage relay	6	0.989	0.984	0.994	0.989

Table 5.6: Confusion matrix of the LSTM model

Relay	Substation	TP	FP	TN	FN
Distance relay 1	1	17,961	39	17,918	6
Overcurrent relay 1	1	17,939	43	17,914	28
Distance relay 2	1	17,917	54	17,903	50
Overcurrent relay 2	1	17,961	286	17,684	19
Distance relay 1	3	17,970	452	17,544	36
Overcurrent relay 1	3	17,947	763	17,233	59
Distance relay 2	3	17,396	149	17,853	616
Overcurrent relay 2	3	17,911	435	17,563	97
Distance relay 1	5	17,882	1,479	16,507	113
Overcurrent relay 1	5	17,958	934	17,066	52
Distance relay 2	5	17,876	422	17,586	141
Overcurrent relay 2	5	17,003	241	17,748	996
Overvoltage relay	2	17,967	370	17,588	0
Undervoltage relay	2	17,257	182	17,795	729
Distance relay 1	2	17,961	39	17,918	6
Overcurrent relay 1	2	17,939	43	17,914	28
Distance relay 2	2	17,970	452	17,544	36
Overcurrent relay 2	2	17,947	763	17,233	59
Overvoltage relay	4	17,967	571	17,386	0
Undervoltage relay	4	17,889	265	17,735	120
Distance relay 1	4	17,396	149	17,853	616
Overcurrent relay 1	4	17,911	435	17,563	97
Distance relay 2	4	17,876	422	17,586	141
Overcurrent relay 2	4	17,003	241	17,748	996
Overvoltage relay	6	17,664	155	17,853	354
Undervoltage relay	6	17,895	289	17,713	116
Distance relay 1	6	17,917	54	17,903	50
Overcurrent relay 1	6	17,961	286	17,684	19
Distance relay 2	6	17,882	1,479	16,507	113
Overcurrent relay 2	6	17,958	934	17,066	52

Table 5.7: Performance metrics for RNN model per relay

Relay	Substation	Accuracy	Precision	Recall	F_1 Score
Distance relay 1	1	0.963	0.962	0.964	0.963
Distance relay 2	1	0.965	0.965	0.965	0.965
Overcurrent relay 1	1	0.965	0.965	0.964	0.965
Overcurrent relay 2	1	0.959	0.953	0.966	0.959
Distance relay 1	3	0.955	0.946	0.965	0.955
Distance relay 2	3	0.947	0.960	0.932	0.946
Overcurrent relay 1	3	0.944	0.929	0.963	0.945
Overcurrent relay 2	3	0.951	0.944	0.958	0.951
Distance relay 1	5	0.922	0.895	0.957	0.925
Distance relay 2	5	0.949	0.941	0.959	0.950
Overcurrent relay 1	5	0.939	0.918	0.963	0.940
Overcurrent relay 2	5	0.932	0.948	0.913	0.930
Distance relay 1	2	0.953	0.939	0.970	0.954
Distance relay 2	2	0.954	0.958	0.950	0.954
Overcurrent relay 1	2	0.956	0.950	0.962	0.956
Overcurrent relay 2	2	0.955	0.950	0.961	0.956
Overvoltage relay	2	0.957	0.947	0.968	0.958
Undervoltage relay	2	0.942	0.957	0.926	0.941
Distance relay 1	4	0.950	0.940	0.962	0.951
Distance relay 2	4	0.943	0.955	0.930	0.942
Overcurrent relay 1	4	0.943	0.928	0.961	0.944
Overcurrent relay 2	4	0.953	0.946	0.962	0.954
Overvoltage relay	4	0.965	0.963	0.967	0.965
Undervoltage relay	4	0.965	0.963	0.966	0.965
Distance relay 1	6	0.961	0.960	0.961	0.961
Distance relay 2	6	0.922	0.894	0.957	0.925
Overcurrent relay 1	6	0.959	0.952	0.967	0.960
Overcurrent relay 2	6	0.937	0.917	0.962	0.939
Overvoltage relay	6	0.953	0.945	0.961	0.953
Undervoltage relay	6	0.930	0.949	0.909	0.929

Table 5.8: Confusion matrix of the RNN model

Relay	Substation	TP	FP	TN	FN
Distance relay 1	1	17,318	686	17,271	649
Overcurrent relay 1	1	17,325	629	17,328	642
Distance relay 2	1	17,342	629	17,328	625
Overcurrent relay 2	1	17,360	864	17,106	620
Distance relay 1	3	17,378	996	17,000	628
Overcurrent relay 1	3	17,332	1,332	16,664	674
Distance relay 2	3	16,786	693	17,309	1,226
Overcurrent relay 2	3	17,257	1,022	16,976	751
Distance relay 1	5	17,219	2,024	15,962	776
Overcurrent relay 1	5	17,345	1,548	16,452	665
Distance relay 2	5	17,270	1,085	16,923	747
Overcurrent relay 2	5	16,440	899	17,090	1,559
Overvoltage relay	2	17,397	967	16,991	570
Undervoltage relay	2	16,648	745	17,232	1,338
Distance relay 1	2	17,423	1,140	16,817	544
Overcurrent relay 1	2	17,329	908	17,092	680
Distance relay 2	2	17,115	757	17,251	903
Overcurrent relay 2	2	17,311	910	17,092	700
Overvoltage relay	4	17,382	668	17,289	585
Undervoltage relay	4	17,364	671	17,286	603
Distance relay 1	4	17,314	1,101	16,895	692
Overcurrent relay 1	4	17,297	1,339	16,657	709
Distance relay 2	4	16,753	795	17,207	1,259
Overcurrent relay 2	4	17,315	983	17,015	693
Overvoltage relay	6	17,320	1,010	16,998	697
Undervoltage relay	6	16,357	876	17,113	1,642
Distance relay 1	6	17,274	711	17,246	693
Overcurrent relay 1	6	17,395	878	17,092	585
Distance relay 2	6	17,223	2,034	15,952	772
Overcurrent relay 2	6	17,323	1,565	16,435	687

Table 5.9: Performance metrics for GRU model per relay

Relay	Substation	Accuracy	Precision	Recall	F_1 Score
Distance relay 1	1	0.986	0.985	0.987	0.986
Distance relay 2	1	0.985	0.984	0.985	0.985
Overcurrent relay 1	1	0.987	0.986	0.988	0.987
Overcurrent relay 2	1	0.981	0.974	0.989	0.981
Distance relay 1	3	0.974	0.963	0.987	0.975
Distance relay 2	3	0.967	0.980	0.954	0.967
Overcurrent relay 1	3	0.965	0.948	0.985	0.966
Overcurrent relay 2	3	0.975	0.966	0.984	0.975
Distance relay 1	5	0.943	0.912	0.981	0.946
Distance relay 2	5	0.973	0.967	0.980	0.974
Overcurrent relay 1	5	0.961	0.939	0.987	0.962
Overcurrent relay 2	5	0.954	0.975	0.932	0.953
Distance relay 1	2	0.972	0.959	0.987	0.973
Distance relay 2	2	0.975	0.981	0.969	0.975
Overcurrent relay 1	2	0.977	0.973	0.981	0.977
Overcurrent relay 2	2	0.977	0.973	0.982	0.977
Overvoltage relay	2	0.978	0.969	0.987	0.978
Undervoltage relay	2	0.962	0.977	0.947	0.961
Distance relay 1	4	0.975	0.963	0.988	0.975
Distance relay 2	4	0.967	0.980	0.953	0.967
Overcurrent relay 1	4	0.966	0.948	0.986	0.967
Overcurrent relay 2	4	0.974	0.965	0.984	0.974
Overvoltage relay	4	0.987	0.985	0.989	0.987
Undervoltage relay	4	0.986	0.985	0.986	0.986
Distance relay 1	6	0.986	0.987	0.985	0.986
Distance relay 2	6	0.944	0.912	0.982	0.946
Overcurrent relay 1	6	0.980	0.972	0.987	0.980
Overcurrent relay 2	6	0.961	0.939	0.985	0.962
Overvoltage relay	6	0.974	0.967	0.981	0.974
Undervoltage relay	6	0.954	0.973	0.933	0.953

Table 5.10: Confusion matrix of the GRU model

Relay	Substation	TP	FP	TN	FN
Distance relay 1	1	17,736	264	17,693	231
Overcurrent relay 1	1	17,748	258	17,699	219
Distance relay 2	1	17,705	281	17,676	262
Overcurrent relay 2	1	17,775	479	17,491	205
Distance relay 1	3	17,764	682	17,314	242
Overcurrent relay 1	3	17,741	982	17,014	265
Distance relay 2	3	17,192	355	17,647	820
Overcurrent relay 2	3	17,728	615	17,383	280
Distance relay 1	5	17,659	1,699	16,287	336
Overcurrent relay 1	5	17,771	1,163	16,837	239
Distance relay 2	5	17,665	606	17,402	352
Overcurrent relay 2	5	16,780	434	17,555	1,219
Overvoltage relay	2	17,737	558	17,400	230
Undervoltage relay	2	17,024	409	17,568	962
Distance relay 1	2	17,735	763	17,194	232
Overcurrent relay 1	2	17,673	491	17,509	336
Distance relay 2	2	17,466	337	17,671	552
Overcurrent relay 2	2	17,681	490	17,512	330
Overvoltage relay	4	17,774	267	17,690	193
Undervoltage relay	4	17,720	270	17,687	247
Distance relay 1	4	17,784	679	17,317	222
Overcurrent relay 1	4	17,750	974	17,022	256
Distance relay 2	4	17,167	343	17,659	845
Overcurrent relay 2	4	17,725	652	17,346	283
Overvoltage relay	6	17,678	604	17,404	339
Undervoltage relay	6	16,801	459	17,530	1,198
Distance relay 1	6	17,691	234	17,723	276
Overcurrent relay 1	6	17,754	506	17,464	226
Distance relay 2	6	17,673	1,710	16,276	322
Overcurrent relay 2	6	17,736	1,146	16,854	274

5.6 Conclusion

This chapter presented a DPI-based anomaly detection system for IEC 61850 substations. By extracting protocol data and applying a deep learning model, the framework effectively identified delay attacks and unusual traffic patterns. The experimental evaluation demonstrated the model's capability to capture long-term dependencies, offering an accurate and quick detection method. Our

proposed distributed architecture enabled continuous, real-time monitoring through local anomaly detection and global verification, demonstrating practical reliability for enhancing substation security.

Chapter Six

Conclusion and Future Directions

The evolution from a traditional power grid to a smart grid has introduced significant advantages through the integration of automation and intelligent systems. This, however, has also introduced a new cyber attack vector that malicious actors can use to destabilize power grid operations. To this end, this thesis presented a cybersecurity framework designed to strengthen the security and resilience of IEC 61850 substations, as one of the most critical elements of a smart grid, against cyber threats. This research emphasized assessing the cyber-physical impact of cyberattacks through realistic experimentation using a real-time co-simulation testbed. This research also highlighted the inadequacy of current security measures built into IEC 61850 and IEC 62351. This thesis also introduced a monitoring and security mechanisms based on the IEC 62351 security recommendations by leveraging Network and System Management (NSM) data and Deep Packet Inspection (DPI).

In Chapter 3, we presented a real-time HIL co-simulation testbed that integrates real-time power grid simulation with an OpenStack-based network emulator. The proposed framework enabled realistic experimentation with smart grid communication networks and facilitated the analysis of cyber-attack impacts on power grid behavior. Through demonstrative use cases, we demonstrated some of the vulnerabilities inherent to the smart grid, highlighting the necessity for the security measures introduced in subsequent chapters. The co-simulation testbed also served as the foundation for data collection and impact analysis in subsequent chapters and related research efforts [19, 20].

In Chapter 4 we designed and implemented a realistic IEC 61850 substation security monitoring

platform compliant with IEC 62351-7, utilizing NSM data objects for anomaly detection. We proposed a two-stage deep learning anomaly detection framework, where individual models (LSTM, GRU, and Simple-RNN) were integrated with autoencoders to enhance predictive performance. An ensemble learning approach further aggregated model outputs to maximize detection accuracy. Experimental results using our real-time HIL testbed demonstrated high detection accuracy and compliance with IEC 61850 timing constraints. We also conducted a critical security assessment of IEC 62351-7, highlighting its limitations and proposed recommendations to enhance its detection capabilities against advanced cyber threats.

In Chapter 5, we introduced our DPI agents to monitor IEC 61850 GOOSE traffic, in accordance with IEC 62351-90-2, to address the limitations identified in Chapter 4. These DPI agents extract key features such as control signals and timing statistics to train local AI-based anomaly detection models, leveraging LSTM-based detectors capable of identifying subtle anomalies and delay attacks previously undetectable through NSM-based methods. Furthermore, a centralized graph-based verification mechanism was implemented to distinguish between anomalies resulting from naturally occurring faults and cyberattacks by analyzing fault/anomaly propagation. Experimental evaluation on the IEEE 9-bus HIL testbed demonstrated approximately 98% detection accuracy, validating the precision and robustness of the proposed anomaly detection and verification framework. This approach significantly enhanced the resilience and detection capabilities in IEC 61850 substations based on the recommendations outlined in IEC 62351.

A key strength of this research lay in its adherence to standard-compliant approaches, specifically the IEC 62351, which ensures interoperability, facilitates industry adoption, and aligns with established cybersecurity guidelines for smart grids. The use of machine learning especially deep learning models such as LSTM and GRU enabled effective detection of time-sensitive and subtle anomalies that are often missed by traditional rule-based systems, thereby enhancing situational awareness and resilience. However, limitations persist. The IEC 62351-7 standard defines a restricted set of NSM MIB variables, limiting the scope of anomalies detectable through NSM-based monitoring alone. As a result, certain attack types, such as sophisticated delay attacks or manipulation attacks, may evade detection using NSM data. To mitigate this, DPI-based monitoring compliant with IEC 62351-90-2 was introduced, allowing inspection of GOOSE traffic and significantly

improving detection capabilities. Nevertheless, deploying DPI and AI-based models across large-scale or resource-constrained substations may introduce computational overhead, and integrating these advanced mechanisms into legacy systems remains a practical challenge that requires further investigation.

The research performed as part of this thesis has been published in multiple top-tier venues, emphasizing its novelty and practical significance in addressing emerging cybersecurity challenges within smart grid infrastructures. Collectively, the proposed solutions advanced the state of the art in cybersecurity monitoring for IEC 61850 substations, providing practical, scalable, and high-precision approaches to enhance substation detection capabilities and resilience.

This research provided valuable insights across multiple dimensions of smart grid cybersecurity. First, the development of a real-time co-simulation testbed facilitated a practical understanding of the technical complexities involved in synchronizing power system simulations with virtualized communication networks, highlighting the importance of timing accuracy, latency control, and system scalability. Second, working within the framework of IEC 62351 security recommendations demonstrated both the benefits and limitations of adhering to standard-compliant approaches. While these standards promote interoperability and provide a structured foundation for cybersecurity, they require extensions or complementary mechanisms to address sophisticated attack scenarios. Third, extensive experimentation with IEC 62351-7 Network and System Management (NSM) data objects confirmed their value for anomaly detection, while also revealing limitations in their predefined scope for identifying advanced cyber-physical threats. Fourth, the integration of Deep Packet Inspection (DPI) in accordance with IEC 62351-90-2 offered critical visibility into protocol-level traffic such as GOOSE messages, enabling the detection of delay and manipulation attacks, though this came with trade-offs in computational overhead and deployment complexity. Finally, the application of artificial intelligence, particularly deep learning models, demonstrated its effectiveness in detecting stealthily and its superiority compared to traditional methods. However, these models require careful training, periodic updating, and attention to resource constraints to ensure their practical deployment in real-world substations. Collectively, these findings contribute to the design of security solutions that balance technical innovation with operational feasibility.

Finally, the continuous evolution of the power grid towards a smart grid necessitates continuous

efforts to enhance its security. As a result, we discuss potential areas for future research, highlighting challenges and directions for further enhancement of the security and reliability of substations.

- Smart Grid Co-Simulation Framework: As future work, we will use the framework to devise novel cyber-attack scenarios against smart grid components and analyze the impact of those attacks on control center applications. This analysis is of extreme importance to propose strategies that harden smart grid security and allow the detection and prevention of cyberattacks against the smart grid.

- IEC 62351-7 NSM for Security Monitoring: Future directions for this research include (i) extending the list of NSM objects to improve the performance of the cyber defense system, and (ii) leveraging deep packet inspection techniques as a complementary tool to enhance the attack detection capability. As a continuation of this work, we intend to enhance our NSM-based anomaly detection approach by considering further NSM objects and complementing this approach with deep packet inspection of the exchanged traffic and other data sources. This is expected to improve our attack detection capabilities and harden the security of the substation.

- Deep Packet Inspection (DPI) for Security Monitoring: Future work could focus on expanding the detection capabilities to cover a wider array of cyber-physical threats, optimizing the system for even faster response times, and integrating advanced technologies and data, such as measurement data, to enhance security and scalability. Additionally, exploring the deployment of this system in various real-world substation environments would provide further insights and opportunities for refinement. By broadening the scope of threats the system can detect, we can ensure more comprehensive protection against evolving cyber-physical attacks. Enhancing the system's speed and responsiveness will be critical for minimizing the impact of detected threats. Integrating measurement data and other advanced technologies can improve the system's accuracy and reliability, enabling it to better differentiate between normal and anomalous behavior. Finally, deploying and testing the system in diverse substation environments will help identify practical challenges and areas for improvement, ensuring that the solution is robust and effective in real-world conditions.

- Integration of Explainable AI (XAI): Although the proposed deep learning–based detection frameworks achieved high accuracy in identifying cyber-physical anomalies, their decision-making process often lacks transparency. Future work should investigate the adoption of Explainable AI (XAI) techniques to provide interpretable and trustworthy insights into model predictions. Methods such as SHAP values, LIME, or attention mechanisms can help operators understand why a particular alert or anomaly is triggered [117, 118]. This will not only increase trust and usability for control-center personnel but also support compliance with emerging cybersecurity regulations that require accountability and interpretability in AI-driven decision-making.

- Hybrid Modeling of Natural Faults and Cyberattacks: Future work should focus on developing hybrid modeling approaches that incorporate both natural fault events and malicious cyberattack scenarios. This integration would enable the proposed detection framework to better differentiate between disturbances caused by normal system faults and those triggered by adversarial activities, reducing false alarms and improving situational awareness.

- Attack Mitigation Strategies: While this thesis focused on detecting and validating cyberattacks, future research should address real-time mitigation mechanisms. This includes designing automated response strategies that can isolate affected components, reconfigure communication paths, or trigger backup protection schemes within stringent millisecond-level timing constraints to maintain system stability during ongoing attacks.

Bibliography

[1] M. Gadelha da Silveira and P. H. Franco, "IEC 61850 network cybersecurity: Mitigating GOOSE message vulnerabilities," in *6th Annual PAC World Americas Conference*, 2019.

[2] W. Canada, "How canada–u.s. power connections affect your electricity bill," 2025, accessed: 2025-07-02. [Online]. Available: https://waterpowercanada.ca/learn/blog/all/how-canada-u-s-power-connections-affect-your-electricity-bill/

[3] E. Climate, "Global electricity review 2024," Ember, Tech. Rep., 2024, accessed: 2025-07-02. [Online]. Available: https://ember-climate.org/global-electricity-review-2024/global-electricity-trends/

[4] American Society of Civil Engineers, "2025 infrastructure report card: Energy," ASCE, Tech. Rep., 2025, accessed: 2025-07-02. [Online]. Available: https://infrastructurereportcard.org/cat-item/energy-infrastructure/

[5] E. Canada, "Electricity 101: Industry overview (may 2025 update)," 2024, accessed: 2025-07-02. [Online]. Available: https://www.electricity.ca/files/Electricity_101_2025_Updated_May_2025-1.pdf

[6] U.S. Energy Information Administration, "United states electricity profile, 2023," U.S. EIA, Tech. Rep., 2023, accessed: 2025-07-02. [Online]. Available: https://www.eia.gov/electricity/state/unitedstates/

[7] ——, "Electric power annual 2023: Table 2.1 – retail customer counts," U.S. EIA, Tech. Rep., 2023, accessed: 2025-07-02. [Online]. Available: https://www.eia.gov/electricity/annual/html/epa_02_01.html

[8] U.S. Census Bureau, "U.s. and world population clock," 2023, accessed: 2025-07-02. [Online]. Available: https://www.census.gov/popclock/

[9] S. Canada, "Population estimates, quarterly (table 17-10-0005-01)," 2024, accessed: 2025-07-02. [Online]. Available: https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=1710000501

[10] North American Electric Reliability Corporation, "2023 long-term reliability assessment," NERC, Tech. Rep., 2023, accessed: 2025-07-02. [Online]. Available: https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2023.pdf

[11] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87–98, 2013.

[12] E-ISAC and SANS Industrial Control Systems, "Analysis of the cyber attack on the ukrainian power grid," Electricity Information Sharing and Analysis Center (E-ISAC), Tech. Rep., March 2016, defense Use Case, Revision 1. [Online]. Available: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf

[13] L. Al Homoud, K. Davis, S. Hossain-McKenzie, and N. Jacobs, "Cyberdep: Towards the analysis of cyber-physical power system interdependencies using bayesian networks and temporal data," in *2024 IEEE Kansas Power and Energy Conference (KPEC)*. IEEE, 2024, pp. 1–6.

[14] CERT-UA, "Cybersecurity situation in ukraine: Annual report 2024," Ukrainian Government, Tech. Rep., 2024, available: https://cert.gov.ua.

[15] IEC/TS 62351-7, "Power systems management and associated information exchange – data and communications security – part 7: Network and system management (NSM) data object models," 2017.

[16] A. Albarakati, B. Moussa, M. Debbabi, A. Youssef, B. L. Agba, and M. Kassouf, "Openstack-based evaluation framework for smart grid cyber security," in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2018, pp. 1–6.

[17] A. Albarakati, C. Robillard, M. Karanfil, M. Kassouf, R. Hadjidj, M. Debbabi, and A. Youssef, "Security monitoring of IEC 61850 substations using IEC 62351-7 network and system management1," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2019, pp. 1–7.

[18] A. Albarakati, C. Robillard, M. Karanfil, M. Kassouf, M. Debbabi, A. Youssef, M. Ghafouri, and R. Hadjidj, "Security monitoring of IEC 61850 substations using IEC 62351-7 network and system management," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1641–1653, 2021.

[19] R. Kateb, P. Akaber, M. H. Tushar, A. Albarakati, M. Debbabi, and C. Assi, "Enhancing wams communication network against delay attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2738–2751, 2018.

[20] B. Moussa, A. Al-Barakati, M. Kassouf, M. Debbabi, and C. Assi, "Exploiting the vulnerability of relative data alignment in phasor data concentrators to time synchronization attacks," *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2541–2551, 2019.

[21] P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in *Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014. Proceedings 15*. Springer, 2014, pp. 63–72.

[22] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019.

[23] T. M. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[24] A.-Y. Lu and G.-H. Yang, "Stability analysis for cyber-physical systems under denial-of-service attacks," *IEEE Transactions on Cybernetics*, vol. 51, no. 11, pp. 5304–5313, 2020.

[25] A. Tesfahun and D. L. Bhaskari, "A scada testbed for investigating cyber security vulnerabilities in critical infrastructures," *Automatic Control and Computer Sciences*, vol. 50, pp. 54–62, 2016.

[26] R. Alguliyev, Y. Imamverdiyev, and L. Sukhostat, "Cyber-physical systems and their security issues," *Computers in Industry*, vol. 100, pp. 212–223, 2018.

[27] E. D. Emake, I. A. Adeyanju, and G. O. Uzedhe, "Industrial control systems (ics): Cyber attacks & security optimization," *International Journal of Computer Engineering and Information Technology*, vol. 12, no. 5, pp. 31–41, 2020.

[28] N. Falliere, L. O. Murchu, E. Chien *et al.*, "W32. stuxnet dossier," *White paper, symantec corp., security response*, vol. 5, no. 6, p. 29, 2011.

[29] R. A. Al-Mulhim, L. A. Al-Zamil, and F. M. Al-Dossary, "Cyber-attacks on saudi arabia environment," *International Journal of Computer Networks and Communications Security*, vol. 8, no. 3, pp. 26–31, 2020.

[30] C. Bronk and E. Tikk-Ringas, "The cyber attack on saudi aramco," *Survival*, vol. 55, no. 2, pp. 81–96, 2013.

[31] R. Khan, P. Maynard, K. McLaughlin, D. Laverty, and S. Sezer, "Threat analysis of black-energy malware for synchrophasor based real-time control and monitoring in smart grid," in *4th International Symposium for ICS & SCADA Cyber Security Research 2016*. BCS, 2016, pp. 53–63.

[32] M. Geiger, J. Bauer, M. Masuch, and J. Franke, "An analysis of black energy 3, crashoverride, and trisis, three malware approaches targeting operational technology systems," in *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 1. IEEE, 2020, pp. 1537–1543.

[33] R. Falcone, "Second wave of shamoon 2 attacks identified," *Palo Alto Networks Blog, January*, 2017.

[34] R. Štefko, K. Eliáš, K. Glajc, A. Hyseni, F. Margita, and J. Šimčák, "Cybersecurity challenges in the power sector: Analysing attacks on electrical grids and substations," in *2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI)*. IEEE, 2025, pp. 000 459–000 464.

[35] M. Santora, "Huge cyberattack knocks ukraine's largest mobile operator offline." *The New York Times (Digital Edition)*, pp. NA–NA, 2023.

[36] International Electrotechnical Commission, "IEC 61850 communication networks and systems for power utility automation," *International Electrotechnical Commission Std*, 2010.

[37] R. E. Mackiewicz, "Overview of IEC 61850 and benefits," in *2006 IEEE Power Engineering Society General Meeting*. IEEE, 2006, pp. 8–pp.

[38] M. Ghezelayagh, *Power Systems Protection, control and automation: Numerical Relays : Field Applications*. Maty Ghezelayagh, 2020.

[39] M. A. Aftab, S. S. Hussain, I. Ali, and T. S. Ustun, "IEC 61850 based substation automation system: A survey," *International Journal of Electrical Power & Energy Systems*, vol. 120, p. 106008, 2020.

[40] K. Saadi and R. Abbou, "On IEC 61850 communication networks in smart grids system: Methodology of implementation and performances analysis on an experimental platform," *International Journal of Energy Research*, vol. 46, no. 1, pp. 89–103, 2022.

[41] R. Mackiewicz, "Technical overview and benefits of the IEC 61850 standard for substation automation," in *Proceedings of the 2006 Power Systems Conference and Exposition*, 2006, pp. 623–630.

[42] International Electrotechnical Commission and others, "IEC 62351: Power systems management and associated information exchange - Data and Communication Security," 2021.

[43] *Communication networks and systems for power utility automation - Part 5: Communication requirements for functions and device models*, International Electrotechnical Commission Std. IEC 61 850-5:2013, 2013.

[44] *Communication networks and systems for power utility automation - Part 7-1: Basic communication structure - Principles and models*, International Electrotechnical Commission Std. IEC 61 850-7-1:2011, 2011.

[45] *Communication networks and systems for power utility automation - Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3*, International Electrotechnical Commission Std. IEC 61 850-8-1:2011, 2011.

[46] *Communication networks and systems for power utility automation - Part 6: Configuration description language for communication in electrical substations related to IEDs*, International Electrotechnical Commission Std. IEC 61 850-6:2009, 2009.

[47] *Communication networks and systems for power utility automation - Part 9-2: Specific Communication Service Mapping (SCSM) – Sampled values over ISO/IEC 8802-3*, International Electrotechnical Commission Std. IEC 61 850-9-2:2011, 2011.

[48] *Communication networks and systems for power utility automation - Part 7-2: Basic communication structure - Abstract Communication Service Interface (ACSI)*, International Electrotechnical Commission Std. IEC 61 850-7-2:2010, 2010.

[49] International Electrotechnical Commission, "Communication networks and systems for power utility automation - part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE c37.118," International Electrotechnical Commission, Technical Report IEC TR 61850-90-5:2012, 2012.

[50] R. Khan, K. Mclaughlin, D. Laverty, and S. Sezer, "Design and implementation of security gateway for synchrophasor based real-time control and monitoring in smart grid," *IEEE Access*, vol. 5, pp. 11 626–11 644, 2017.

[51] IEC/TS 62351-6, "IEC 62351-6: Power systems management and associated information exchange - data and communications security - part 6: Security for IEC 61850," 2007.

[52] IEC/TS 62351-7, "IEC 62351-7: Power systems management and associated information exchange - data and communications security - part 7: Network and system management (nsm) data object models," 2010.

[53] IEC/TS 62351-10, "IEC 62351-10: Power systems management and associated information exchange - data and communications security - part 10: Security architecture guidelines," 2012.

[54] M. T. A. Rashid, S. Yussof, Y. Yusoff, and R. Ismail, "A review of security attacks on IEC 61850 substation automation system network," in *Proceedings of the 6th International Conference on Information Technology and Multimedia*. IEEE, 2014, pp. 5–10.

[55] P. Blazek, A. Bohacik, R. Fujdiak, V. Jurak, and M. Ptacek, "Smart grids transmission network testbed: Design, deployment, and beyond," *IEEE Open Journal of the Communications Society*, vol. 6, pp. 51–76, 2025.

[56] H. Lin, Y. Deng, S. Shukla, J. Thorp, and L. Mili, "Cyber security impacts on all-PMU state estimator - a case study on co-simulation platform GECO," in *2012 IEEE SmartGridComm*, pp. 587–592.

[57] D. Bian, M. Kuzlu, M. Pipattanasomporn, S. Rahman, and Y. Wu, "Real-time co-simulation platform using opal-rt and opnet for analyzing smart grid performance," in *2015 IEEE Power Energy Society General Meeting*, July 2015, pp. 1–5.

[58] A. Herath, C.-C. Liu, J. Hong, and M. Girdhar, "An advanced cyber-physical system security testbed for substation automation," 2025. [Online]. Available: https://arxiv.org/abs/2505.24021

[59] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, B. Pranggono, P. Brogan, and H. Wang, "Intrusion detection system for network security in synchrophasor systems," in *IET International*

Conference on Information and Communications Technologies (IETICT). IET, 2013, pp. 246–252.

[60] H. Yoo and T. Shon, "Novel approach for detecting network anomalies for substation automation based on IEC 61850," *Multimedia Tools and Applications*, vol. 74, pp. 303–318, 2014.

[61] C. Feng, T. Li, Z. Zhu, and D. Chana, "A deep learning-based framework for conducting stealthy attacks in industrial control systems," 2017. [Online]. Available: https://arxiv.org/abs/1709.06397

[62] Y. Yang, K. McLaughlin, L. Gao, S. Sezer, Y. Yuan, and Y. Gong, "Intrusion detection system for IEC 61850 based smart substations," in *2016 IEEE Power and Energy Society General Meeting (PESGM)*. IEEE, 2016, pp. 1–5.

[63] A. Valdes, R. Macwan, and M. Backes, "Anomaly detection in electrical substation circuits via unsupervised machine learning," in *2016 IEEE 17th international conference on information reuse and integration (IRI)*. IEEE, 2016, pp. 500–505.

[64] Y. Kwon, H. K. Kim, Y. H. Lim, and J. I. Lim, "A behavior-based intrusion detection technique for smart grid infrastructure," in *2015 IEEE Eindhoven PowerTech*. IEEE, 2015, pp. 1–6.

[65] R. C. B. Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari, and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," in *2014 7th International symposium on resilient control systems (ISRCS)*. IEEE, 2014, pp. 1–8.

[66] J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1643–1653, 2014.

[67] J. Hong, C. Liu, and M. Govindarasu, "Detection of cyber intrusions using network-based multicast messages for substation automation," in *ISGT 2014*, 2014, pp. 1–5.

[68] H. Yoo and T. Shon, "Novel approach for detecting network anomalies for substation automation based on IEC 61850," *Multimedia Tools and Applications*, vol. 74, no. 1, pp. 303–318, 2015.

[69] C. Lee, M. Park, J. Lee, and I. Joe, "Design and implementation of packet analyzer for IEC 61850 communication networks in smart grid," in *International Conference on Future Generation Communication and Networking*. Springer, 2012, pp. 33–40.

[70] D. Formby, P. Srinivasan, A. M. Leonard, J. D. Rogers, and R. A. Beyah, "Who's in control of your control system? device fingerprinting for cyber-physical systems." in *NDSS*, 2016.

[71] F. Dawli, "Lightweight dpi anomaly detection framework for IEC 61850-based smart grids," Master's thesis, Mälardalen University, June 2025, master's Thesis, DiVA – Academic Archive. [Online]. Available: https://www.diva-portal.org/smash/get/diva2:1968474/FULLTEXT01.pdf

[72] J. Yu, H. Lee, M.-S. Kim, and D. Park, "Traffic flooding attack detection with SNMP MIB using SVM," *Computer Communications*, vol. 31, no. 17, pp. 4212–4219, 2008.

[73] J. Yu, H. Kang, D. Park, H.-C. Bang, and D. W. Kang, "An in-depth analysis on traffic flooding attacks detection and system using data mining techniques," *Journal of Systems Architecture*, vol. 59, no. 10, pp. 1005–1012, 2013.

[74] P. M. Priya, V. Akilandeswari, S. M. Shalinie, V. Lavanya, and M. S. Priya, "The protocol independent detection and classification (PIDC) system for DRDoS attack," in *2014 International Conference on Recent Trends in Information Technology*. IEEE, 2014, pp. 1–7.

[75] W. Cerroni, G. Moro, R. Pasolini, and M. Ramilli, "Decentralized detection of network attacks through p2p data clustering of SNMP data," *Computers & Security*, vol. 52, pp. 1–16, 2015.

[76] K. Choi, X. Chen, S. Li, M. Kim, K. Chae, and J. Na, "Intrusion detection of NSM based DoS attacks using data mining in smart grid," *Energies*, vol. 5, no. 10, pp. 4091–4109, 2012.

[77] B. Cui-Mei, "Intrusion detection based on one-class SVM and SNMP MIB data," in *2009 Fifth International Conference on Information Assurance and Security*, vol. 2. IEEE, 2009, pp. 346–349.

[78] M. H. Cintuglu, O. A. Mohammed, K. Akkaya, and A. S. Uluagac, "A survey on smart grid cyber-physical system testbeds," *IEEE ComST*, vol. 19, no. 1, pp. 446–464, Firstquarter 2017.

[79] R. Raghunarayan, "RFC 4022: Management information base for the Transmission Control Protocol (TCP)," Tech. Rep., 2005.

[80] A. Chattopadhyay, A. Ukil, D. Jap, and S. Bhasin, "Toward threat of implementation attacks on substation security: Case study on fault detection and isolation," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 6, pp. 2442–2451, 2018.

[81] S. M. S. Hussain, T. S. Ustun, and A. Kalam, "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5643–5654, 2020.

[82] D. Mashima, P. Gunathilaka, and B. Chen, "Artificial command delaying for secure substation remote control: Design and implementation," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 471–482, 2019.

[83] "OPAL-RT Technologies," 2021. [Online]. Available: https://www.opal-rt.com/

[84] "OpenStack Open source software for creating private and public clouds," 2021. [Online]. Available: https://www.openstack.org/

[85] "IEEE Standard for Synchrophasor Measurements for Power Systems," *IEEE Std C37.118.1-2011 (Revision of IEEE Std C37.118-2005)*, pp. 1–61, Dec 2011.

[86] "OPAL-RT Technologies." [Online]. Available: https://selinc.com/

[87] "Open and Extensible control & Analytics platform for synchrophasor data (openECA)." [Online]. Available: https://github.com/GridProtectionAlliance/openECA

[88] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," *IEEE Std 1588-2008 (Revision of IEEE Std 1588-2002)*, pp. 1–269, July 2008.

[89] *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, Std., 2019, iEEE Std 1588-2019 (revision of IEEE Std 1588-2008).

[90] W. Gao, H. Li, M. Zhong, and M. Lu, "An underestimated cybersecurity problem: quick-impact time synchronization attacks and a fast-triggered detection method," *IEEE Transactions on Smart Grid*, vol. 14, no. 6, pp. 4784–4798, 2023.

[91] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3, pp. 146–153, 2012.

[92] "Phase Angle Monitoring: Industry Experience Following the 2011 Pacific Southwest Outage Recommendation 27," The North American Electric Reliability Corporation (NERC), Tech. Rep., 06 2016.

[93] F. Cleveland, "Enhancing the reliability and security of the information infrastructure used to manage the power system," in *2007 IEEE Power Engineering Society General Meeting*, June 2007, pp. 1–8.

[94] D. M. E. Ingram, P. Schaub, R. R. Taylor, and D. A. Campbell, "Performance analysis of IEC 61850 sampled value process bus networks," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1445–1454, 2013.

[95] "IEEE standard electrical power system device function numbers, acronyms, and contact designations," *IEEE Std C37.2-2008 (Revision of IEEE Std C37.2-1996)*, pp. 1–48, 2008.

[96] "IEEE standard for inverse-time characteristics equations for overcurrent relays," *IEEE Std C37.112-2018 (Revision of IEEE Std C37.112-1996)*, pp. 1–25, 2019.

[97] W. Stallings, *SNMP, SNMPv2, SNMPv3, and RMON 1 and 2*. Addison-Wesley Longman Publishing Co., Inc., 1998.

[98] N. Kush, E. Ahmed, M. Branagan, and E. Foo, "Poisoned GOOSE: exploiting the GOOSE protocol," in *Proceedings of the Twelfth Australasian Information Security Conference*, vol. 149, 2014, pp. 17–22.

[99] M. Strobel, N. Wiedermann, and C. Eckert, "Novel weaknesses in IEC 62351 protected smart grid control systems," in *Smart Grid Communications (SmartGridComm), 2016 IEEE International Conference on*. IEEE, 2016, pp. 266–270.

[100] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *nature*, vol. 521, no. 7553, p. 436, 2015.

[101] N. K. Ahmed, A. F. Atiya, N. E. Gayar, and H. El-Shishiny, "An empirical comparison of machine learning models for time series forecasting," *Econometric Reviews*, vol. 29, no. 5-6, pp. 594–621, 2010.

[102] A. K. Palit and D. Popovic, *Computational intelligence in time series forecasting: theory and engineering applications*. Springer Science & Business Media, 2006.

[103] G. Bontempi, S. B. Taieb, and Y.-A. Le Borgne, "Machine learning strategies for time series forecasting," in *European business intelligence summer school*. Springer, 2012, pp. 62–77.

[104] A. Sfetsos and A. Coonick, "Univariate and multivariate forecasting of hourly solar radiation with artificial intelligence techniques," *Solar Energy*, vol. 68, no. 2, pp. 169–178, 2000.

[105] S. McNally, J. Roche, and S. Caton, "Predicting the price of bitcoin using machine learning," in *2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP)*. IEEE, 2018, pp. 339–343.

[106] R. Polikar, *Ensemble Learning*. Boston, MA: Springer US, 2012, pp. 1–34.

[107] A. Sayghe, Y. Hu, I. Zografopoulos, X. Liu, R. G. Dutta, Y. Jin, and C. Konstantinou, "Survey of machine learning methods for detecting false data injection attacks in power systems," *IET Smart Grid*, vol. 3, no. 5, pp. 581–595, 2020. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-stg.2020.0015

[108] A. Ameli, A. Ayad, E. El-Saadany, M. Salama, and A. Youssef, "A learning-based framework for detecting cyber-attacks against line current differential relays," *IEEE Transactions on Power Delivery*, pp. 1–1, 2020.

[109] IEC/TS 62351-6, "Power systems management and associated information exchange – data and communications security – part 6: Security for IEC 61850," 2007.

[110] IEC/TS 62351-4, "Power systems management and associated information exchange – data and communications security – part 4: Profiles including MMS," 2007.

[111] R. King, "Network system management: Implementations and applications of the IEC 62351-7 standard," EPRI, 2014.

[112] A. Albarakati, C. Robillard, M. Karanfil, M. Kassouf, M. Debbabi, A. Youssef, M. Ghafouri, and R. Hadjidj, "Security monitoring of IEC 61850 substations using IEC 62351-7 network and system management," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1641–1653, 2022.

[113] Z. Z. Darban, G. I. Webb, S. Pan, C. C. Aggarwal, and M. Salehi, "Deep learning for time series anomaly detection: A survey," *ACM Computing Surveys*, vol. 57, no. 1, p. Article 15, 2024.

[114] L. Wang, L. Peng, M. Su, B. Yang, and X. Zhou, "On the impact of packet inter arrival time for early stage traffic identification," in *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2016, pp. 510–515.

[115] E. Zivot and J. Wang, "Rolling analysis of time series," *Modeling Financial Time Series with S-Plus®*, pp. 299–346, 2003.

[116] M. E. Newman, "Modularity and community structure in networks," *Proceedings of the national academy of sciences*, vol. 103, 2006.

[117] S. M. Lundberg and S.-I. Lee, “A unified approach to interpreting model predictions,” *Advances in neural information processing systems*, vol. 30, 2017.

[118] M. T. Ribeiro, S. Singh, and C. Guestrin, “” why should i trust you?” explaining the predictions of any classifier,” in *Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining*, 2016, pp. 1135–1144.