Machine Learning Based Detection of False Data Injection Attacks in Wide Area Monitoring Systems

Christian Salem

A Thesis
in
The Concordia Institute
for
Information Systems Engineering (CIISE)

Presented in Partial Fulfillment of the Requirements
For the Degree of
Master of Applied Science (Information Systems Security) at
Concordia University
Montréal, Québec, Canada

March 2020

CONCORDIA UNIVERSITY
School of Graduate Studies

This is to certify that the thesis prepared

By: **Christian Salem**

Entitled: **Machine Learning Based Detection of False Data Injection Attacks in Wide Area Monitoring Systems**

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

Master of Applied Science (Information Systems Security)

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. Mohsen Ghafouri

______________________________ External
Dr. Otmane Ait Mohamed

______________________________ Examiner
Dr. Mohsen Ghafouri

______________________________ Thesis Supervisor
Dr. Mourad Debbabi

______________________________ Co-supervisor
Dr. Marthe Kassouf

Approved by ______________________________
Dr. Abdessamad Ben Hamza, Graduate Program Director

March 26, 2020 ______________________________
Dr. Amir Asif, Dean
Gina Cody School of Engineering and Computer Science

Abstract

Machine Learning Based Detection of False Data Injection Attacks in Wide Area Monitoring Systems

Christian Salem

The Smart Grid (SG) is an upgraded, intelligent, and a more reliable version of the traditional Power Grid due to the integration of information and communication technologies. The operation of the SG requires a dense communication network to link all its components. But such a network renders it prone to cyber attacks jeopardizing the integrity and security of the communicated data between the physical electric grid and the control centers. One of the most prominent components of the SG are Wide Area Monitoring Systems (WAMS). WAMS are a modern platform for grid-wide information, communication, and coordination that play a major role in maintaining the stability of the grid against major disturbances. In this thesis, an anomaly detection framework is proposed to identify False Data Injection (FDI) attacks in WAMS using different Machine Learning (ML) and Deep Learning (DL) techniques, i.e., Deep Autoencoders (DAE), Long-Short Term Memory (LSTM), and One-Class Support Vector Machine (OC-SVM). These algorithms leverage diverse, complex, and high-volume power measurements coming from communications between different components of the grid to detect intelligent FDI attacks. The injected false data is assumed to target several major WAMS monitoring applications, such as Voltage Stability Monitoring (VSM), and Phase Angle Monitoring (PAM). The attack vector is considered to be smartly crafted based on the power system data, so that it can pass the conventional bad data detection schemes and remain stealthy. Due to the lack of realistic attack data, machine learning-based anomaly detection techniques are used to detect FDI attacks. To demonstrate the impact of attacks on the realistic WAMS traffic and to show the effectiveness of the proposed detection framework, a Hardware-In-the-Loop (HIL) co-simulation testbed is developed. The performance of the implemented techniques is compared on the testbed data using different metrics: Accuracy, F_1 score, and False Positive Rate (FPR) and False Negative Rate (FNR). The IEEE 9-bus and IEEE 39-bus systems are used as benchmarks to investigate the framework scalability. The experimental results prove the effectiveness of the proposed models in detecting FDI attacks in WAMS.

Acknowledgments

I would like to express my gratitude to everyone who supported me throughout my Master's degree.

I am grateful for my supervisor, Prof. Mourad Debbabi, for his continuous guidance and support throughout this journey. His vast knowledge and experience in the field helped me develop a detailed understanding of the cybersecurity discipline. It was a privilege and a pleasure working under your supervision. I would also like to express my gratitude to Dr. Marthe Kassouf for believing in my abilities since the start of this journey, and for all the time she dedicated and feedback she provided to advance my work.

I extend my gratitude to Dr. Mohsen Ghafouri and Dr. Otmane Ait Mohamed for taking part in my examination committee.

Moreover, I am thankful for my lab colleagues and the many professors in the Security Research Center. I appreciate your advice, collaboration, and insightful discussions that were critical for the development of this research project over the last two years.

I am blessed with precious friends with whom I shared great experiences during this endeavor. Thank you to everyone at Willowdale for becoming my second family in Canada. And thank you to my friends back home, and those scattered around the world, for keeping me anchored from afar with your constant support and wonderful conversations. I truly appreciate your help and effort.

Furthermore, I would like to thank Prof. Danielle Azar for always having faith in me and constantly motivating me. I am immensely indebted to you.

Finally, I am deeply grateful to my parents and brothers. Thank you for your patience, support and endless encouragement. I couldn’t have done it without you, I hope I can ever pay you but little of all what you have given me. I love you.

Psalm 92:12

Contents

List of Figures **ix**

List of Tables **xii**

1 Introduction **1**

1.1 Motivations 1

1.2 Problem Statement 3

1.3 Objectives 3

1.4 Contributions 3

1.5 Thesis Structure 4

2 Background **5**

2.1 Supervisory Control and Data Acquisition Systems 5

2.2 Wide Area Monitoring Systems 7

2.2.1 Role in Smart Grid 7

2.2.2 Communication System 8

2.2.3 Communication Protocols 9

2.2.4 WAMS Applications 15

2.3 Cybersecurity Threats in WAMS 17

2.3.1 Attacks on Endpoints 18

2.3.2 Attacks on Communication Channels 20

2.4 Deep Packet Inspection 24

2.4.1 Definition 24

2.4.2 Deep Packet Inspection in the Smart Grid 25

2.5 Anomaly Detection 26

2.5.1 Rule-based Anomaly Detection 27

2.5.2 Data-driven Anomaly Detection 27

2.6 Classification 27

2.6.1 Rule-Based Classification 28

2.6.2 Data-Driven Classification 28

2.7 Conclusion 29

3 Literature Review 30

3.1 False Data Injection 31

3.2 Anomaly Detection 32

3.2.1 Rule-Based Deep Packet Inspection for Anomaly Detection 32

3.2.2 Data-Driven Deep Packet Inspection for Anomaly Detection 37

3.2.3 Deep Packet Inspection for Anomaly Detection 42

3.3 Classification 43

3.3.1 Rule-Based Deep Packet Inspection for Classification 43

3.3.2 Data-Driven Techniques 45

3.3.3 Deep Packet Inspection for Smart Grid Attack Classification 50

3.4 Wide Area Monitoring Systems Specific Works 51

3.5 Gap Analysis 53

3.5.1 Applications and Protocols 54

3.5.2 Threat Models 56

3.5.3 DPI Methodologies 57

4 Methodology **62**

4.1 Hardware-in-the-Loop Co-simulation Testbed Setup 62

4.1.1 Power Model 63

4.1.2 Communication Model 65

4.1.3 Simulated Scenarios 66

4.1.4 Optimal PMU Placement 67

4.2 Feature Extraction 70

4.3 Threat Model 71

4.4 Deep Autoencoders 73

4.5 Windowed Deep Autoencoders 76

4.6 Long Short-Term Memory 77

4.7 One-Class SVM 79

5 Experimental Results and Analysis **82**

5.1 Experimental Setup 82

5.1.1 Datasets 83

5.2 Parameter Tuning 89

5.2.1 Evaluation Metrics 95

5.3 Results 97

5.3.1 IEEE 9-bus System 97

5.3.2 IEEE 39-bus System 105

5.4 Result Analysis 114

6 Conclusion **116**

Bibliography **120**

List of Figures

1 SCADA Network Architecture 6

2 WAMS Network Architecture 9

3 IEEE C37.118 Protocol Stack. 10

4 IEC 61850 Protocol Stack 12

5 HMI Screenshot Sniffed by Threat Actors in the U.S. Energy Infrastructure 22

6 Taxonomy of DPI Techniques Based on Methodologies. 32

7 Taxonomy of DPI Techniques in WAMS Based on Protocols. 53

8 WAMS Co-simulation Testbed 63

9 IEEE 9-bus System 64

10 IEEE 39-bus System 65

11 Load Variation in IEEE 9-bus System 68

12 Load Variation in IEEE 39-bus System 69

13 FDI Attack Tree 74

14 Deep Autoencoder 75

15 Windowed Deep Autoencoder 77

16 Structure of LSTM Cell 79

17 Two Dimensional Representation of OC-SVM [1] 81

18 Raw Voltage Measurements 84

19 Raw Current Measurements 84

20 Raw Frequency Measurements 85

21 Raw ROCOF Measurements 85

22 Scaled Voltage Measurements 86

23 Scaled Current Measurements 86

24 Scaled Frequency Measurements 87

25 Scaled ROCOF Measurements 87

26 Correlation Matrix of PMU 9 Measurements 88

27 Correlation Matrix of PMU 9 and PMU 10 Measurements 89

28 Reconstruction Error of Different Functions with 1 Hidden Layer 90

29 Log (Reconstruction Error) of Different Functions with 1 Hidden Layer . . 91

30 Log (Reconstruction Error) of Different Functions with 5 Hidden Layers . . 91

31 Log (Reconstruction Error) of Different Functions with 11 Hidden Layers . 92

32 Log (Reconstruction Error) of Different Functions with 15 Hidden Layers . 92

33 Run Time for Different Network Architectures 93

34 Reconstruction Error with Different Number of Hidden Layers 93

35 Run Time for Different Network Architectures 94

36 PAM Experiment on Line 2 of IEEE 9-bus System 98

37 F_1 for Different Number of Compromised PMUs 99

38 FVSI Experiment on Line 4 of IEEE 9-bus System 100

39 F_1 for Different Number of Compromised PMUs 100

40 ISI Experiment on Bus 6 of IEEE 9-bus System 101

41 F_1 for Different Number of Compromised PMUs 101

42 F_1 for Different Number of Compromised PMUs 102

43 F_1 for Different Number of Compromised PMUs 103

44 F_1 for Different Number of Compromised PMUs 104

45 PAM Experiment on Line 32 of IEEE 39-bus System 105

46 F_1 for Different Number of Compromised PMUs 106

47 FVSI Experiment on Line 27 of IEEE 39-bus System 107

48 F_1 for Different Number of Compromised PMUs 107

49 ISI Experiment on Bus 20 of IEEE 39-bus System 108

50 F_1 for Different Number of Compromised PMUs 108

51 F_1 for Different Number of Compromised PMUs 109

52 F_1 for Different Number of Compromised PMUs 110

53 F_1 for Different Number of Compromised PMUs 111

List of Tables

1 Feature Comparison Between IEEE C37.118 and IEC 61850-90-5 15

2 Overview of WAMS research 60

3 Acronyms of Simulated Scenarios 61

4 IEEE 9-bus System Load Variation Over Time 68

5 Optimal Locations of PMUs for the IEEE 9-bus and IEEE 39-bus Systems . 69

6 Hyperparameters of DAE, w-DAE, and LSTM models 94

7 Hyperparameters of OC-SVM models 94

8 Generic Confusion Matrix 95

9 Detection Results for FDI Against Applications in the IEEE 9-bus System. . 104

10 Detection Results for Masking FDI Attacks in the IEEE 9-bus System. . . . 104

11 Detection Results for FDI Against Applications in the IEEE 39-bus System. 112

12 Detection Results for Masking FDI Attacks in the IEEE 39-bus System. . . 113

Chapter 1

Introduction

1.1 Motivations

Energy infrastructures, in particular power systems, are one of the major critical infrastructures in a modern society [2]. The power system ensures the generation and distribution of electric energy among the consumers. Such a large-scale energy delivery system is comprised of 3 main subsystems, namely, generation, transmission, and distribution. The coordinated operation of these systems ensures the uninterrupted and stable production, delivery, and consumption of electricity. However, the generation and transmission systems can experience various types of instabilities and operational issues due to natural causes and electrical malfunctions [3]. Consequently, analyzing the stability and operation of transmission and generation systems is of paramount importance since these systems cover large geographic areas that can span thousands of kilometers. As a result, any issue in the operation of these systems may affect a huge number of consumers or even cause blackouts. Therefore, the use of a monitoring and data acquisition system is necessary to improve the operation of the system. In power system, the Supervisory Control and Data Acquisition (SCADA) system is traditionally used for monitoring purposes. However, it suffers from various limitations, such as very limited communication infrastructure, and low data sampling rates. Recently, in order to improve efficiency and reliability of the power system, the smart grid concept is introduced. The majority of the advantages of deploying the smart grid concept are the result of the integration of distributed renewable energy generation systems and Information and Communication Technologies (ICTs) into the conventional electric grid. As a result, power systems start to increasingly employ significant amount of communication technologies and cyber devices [4]. WAMS benefit from this cyber and communication layer to tackle the drawbacks of conventional SCADA system [5]. This system is one of the major smart grid domains that monitors the grid operation and provides real-time, highly-sampled, and time-synchronized data for the control and protection layers of the power grid [6]. WAMS is composed of physical and cyber layers. The former comprises generators, buses and transmission lines of the grid, while the latter encompasses the Phasor Measurement Units (PMU), the Phasor Data Concentrators (PDC) and the communication links that connect them to the system operator. The design of WAMS requires an extremely dense communication network and extensive deployment of Intelligent Electronic Devices (IEDs), which renders it prone to cyberattacks [7]. These attacks can have catastrophic consequences such as cascading failures and blackouts over large areas. Recent events demonstrate the susceptibility of the cyber layer of smart grid systems to cyber attacks, such as the Ukraine cyberattack [8]. It is worth mentioning that various types of malware have been used to launch such attacks, e.g., BlackEnergy [9], Industroyer [10], Duqu [11], Stuxnet [12]. One dangerous class of attacks is stealthy False Data Inspection (FDI) attacks. FDI attacks manipulate the collected physical measurements in order to mislead the decision-making process of the WAMS operator. Such attacks can have grave consequences such as line overloads that can lead to large-scale blackouts [13]. Deep Packet Inspection (DPI) is a suitable approach to examine the communicated measurements over the network since it allows the real-time extraction and analysis of these measurements.

1.2 Problem Statement

The purpose of this research is to design, implement, and evaluate a new platform for WAMS security monitoring that utilizes DPI and ML-based anomaly detection methods in order to identify stealthy FDI attacks.

1.3 Objectives

The objectives of this research are as follows:

- To assess the benefits of employing ML as a solution for WAMS security monitoring with a focus on leveraging DPI-extracted features by anomaly detection models to enhance the threat detection in WAMS.
- Develop a realistic WAMS cyber-physical testbed that integrates hardware, different scenarios and WAMS-specific monitoring indices for evaluation of proposed ML-based approach.
- Design and implement a real-time WAMS monitoring platform based on DPI and ML anomaly detection to monitor and protect WAMS operations.
- Elaborate and compare multiple anomaly detection methods and evaluate their scalability and effectiveness in attack identification.

1.4 Contributions

The contributions of this research are:

1. An investigation on the validity and effectiveness of DPI and ML for WAMS security monitoring with a focus 2 WAMS-specific protocols IEEE C37.118 and IEC 61850-90-5.

2. A real-time, realistic, HIL WAMS co-simulation model is elaborated. The model incorporates commercial hardware and takes into account different operational scenarios, applications, and system sizes.

3. A set of FDI attack scenarios is developed and implemented. The attacks are tailored for WAMS-specific application in order to prompt erroneous behavior from the control center.

4. An anomaly detection approach to the FDI attack problem is developed in order to align the solution with the real-world operation of the smart grid where normal data is abundant but attack data is scarce.

5. The performance and scalability of different anomaly detection techniques in identifying FDI attacks in WAMS are evaluated and compared.

1.5 Thesis Structure

The remainder of this thesis if organized as follows. Chapter 2 of this thesis presents background information and concepts on WAMS, its communication infrastructure, threat models, and DPI. Chapter 3 provides a literature review on WAMS, FDI attacks targeting them, and solutions against these threats. Chapter 4 describes the design of the proposed DPI platform and details the different anomaly detection models developed. It also presents the methodology that can be used to craft and launch the studied cyberattacks. Chapter 5 details the WAMS testbed architecture and its communications. Moreover, it details the attack scenarios implemented and launched against the WAMS applications. Furthermore, it presents the experimental results on the effectiveness of the proposed DPI platform at detecting the attacks. Chapter 6 draws the conclusions and discusses the implications and the insights gained, along with potential future research directions in the studied area.

Chapter 2

Background

This chapter provides an overview of the concepts discussed in this research. First, legacy SCADA systems are introduced. Second, the concepts related to WAMS are discussed covering WAMS communication networks, protocols, and applications. Third, cyberattack threats that can impact WAMS are presented. Fourth, the potential of DPI is explained with respect to the proposed cybersecurity approach. Finally, anomaly detection is detailed.

2.1 Supervisory Control and Data Acquisition Systems

SCADA systems are widely-used automation control systems in many industries, including power, water, oil and gas, among others [14]. Although IEDs are replacing legacy sensors and actuators in SCADA systems, the incumbent SCADA systems will still provide a majority of monitoring and control capabilities to the smart grid in the near future, before being eventually upgraded to or replaced by the WAMS [15].

An overview of the SCADA architecture is shown in Fig. 1 (adapted from [16]). In general, SCADA encompasses two principal activities, the monitoring of processes and equipment as well as the corresponding supervisory control, carried out by four components: the Remote Terminal Units (RTUs), the communication systems, the Master Terminal Units

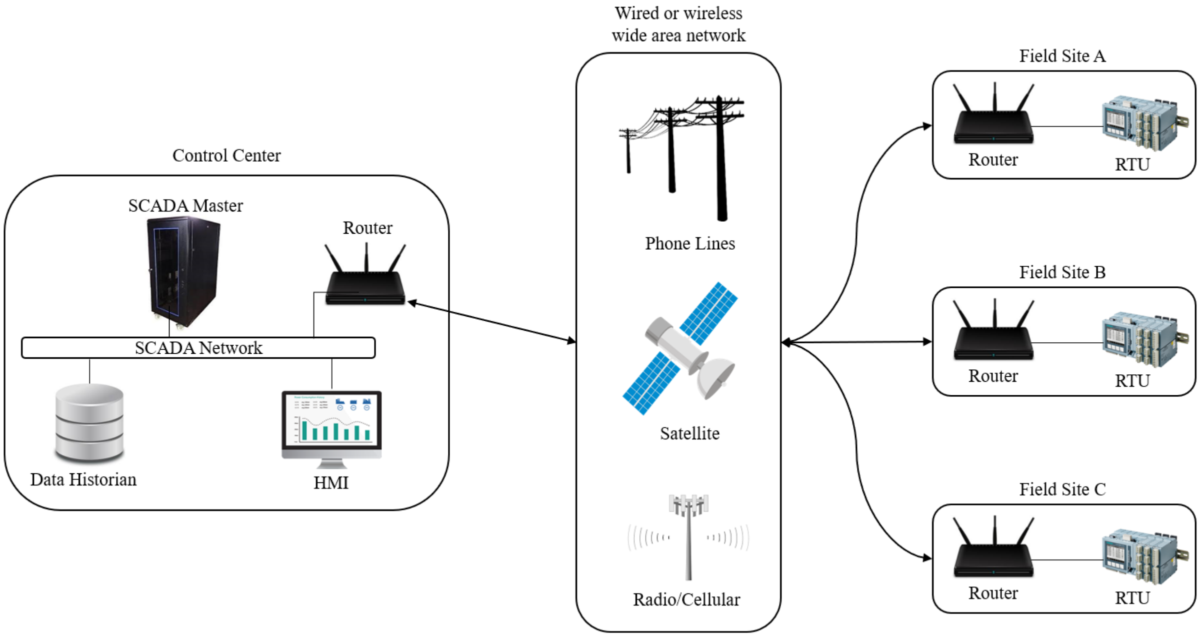


Figure 1: SCADA Network Architecture

(MTUs), and the Human-Machine Interface (HMI). The RTU acquires analogue measurements from field sensors and converts them into digital signals to be sent to the MTU; it also converts control commands received from the MTU to control actions executable by the actuators. The measurements and commands are exchanged as packet payloads through the proprietary communication protocols between RTUs in the field and MTUs at the control centers. A MTU collects and monitors the state of the grid with measurements received from the RTUs and determines proper commands to be sent back through the feedback control loop. An HMI allows SCADA operators to interact with the MTU and manage the entire system [15]. Historians may also be deployed along with the MTU and HMI to archive the measurements and event logs for further auditing and analysis.

In the smart grid, SCADA systems provide non-synchronous information of the system at lower data sampling rates, normally less than one sample per second. Subsequently, the control center is required to re-align the various measurements arriving at different times within a certain time window - which can vary from 2 to 15 seconds depending on system configuration - and further down-sample the data. The lower sampling rate and realignment thereby provides a low resolution view of the system compared to WAMS, with benefit in terms of bandwidth requirement and energy consumption. Also, many legacy SCADA systems were initially designed before the 2000s. As such, these systems do not provide native or adequate support for security features like encryption. Recently, with the increased adoption of PMUs, some studies have explored their integration into SCADA systems in order to enhance the monitoring performance [17]. SCADA systems don't usually rely on PMUs, however, with the introduction of PMUs to SCADA, we notice a step towards the transition from legacy SCADA systems which are still more widely used today, to novel real-time WAMS systems. It is important to note that SCADA and WAMS are complimentary since they both serve the same purpose of monitoring the transmission system and protecting it against faults and disturbances.

2.2 Wide Area Monitoring Systems

This section discusses concepts related to WAMS. It is broken down into four parts. The first part explains the role that WAMS play in the SG. The second discusses the WAMS digital communication system. The third part describes the WAMS protocols used in the communication. The final part describes WAMS applications with a focus on three main applications, namely PAM, Fast Voltage Stability Index (FVSI) and Impedance Stability Index (ISI).

2.2.1 Role in Smart Grid

As an upgrade of the legacy SCADA system, WAMS is used to gather, process, and transmit physical data to different applications for monitoring, control, and protection purposes of transmission systems. WAMS allow grid-wide, information, communication, and coordination against major disturbances and blackouts [5]. WAMS rely on a dense hierarchical communication network to transfer the data from the sensors in the field to the control center. The transmitted data is used in different applications to reflect the state of the grid to the operator. Accordingly, the operator will determine the appropriate course of action that will maintain the stability and security of the grid [5]. The cyber components deployed in WAMS structure provide real-time, accurate monitoring of the state of the grid allowing for faster remedial actions in case of faults, disturbances, or performance degradation.

2.2.2 Communication System

In order to track the fast-dynamics of fault and failures in the smart grid, which may occur for less than a second, WAMS relies heavily on advanced cyber infrastructure and dedicated protocols to transmit data between control centers and field devices over hundreds to thousands of kilometers. As the key innovative sensing technology, PMUs installed at selected locations of the grid collect current, voltage, phase, and frequency measurements and transmit them to PDCs that time-align and combine measurements coming from multiple PMUs, and forward them to higher level PDCs, and ultimately the control center. The measurements are time-stamped and synchronized using Global Positioning System (GPS) receivers with up to one microsecond accuracy [5]. The time-aligned measurements provide high-resolution snapshots of interconnected smart grid system over spatial and temporal domains. WAMS offers unprecedented granularity of steady states and transients and enables advanced early warning against widespread disturbances. An overview of the WAMS architecture is shown in Fig. 2. The volume and speed of data exchange in WAMS also impose stringent latency constraints. While early WAMS standards requires as few as 10 samples per second, the latest standards are setting forth real-time sampling rates up to 12,800 Hz [18]. In order to accommodate the temporal resolution, dedicated protocols have been developed for WAMS systems to transmit data between PMUs and PDCs, which include IEEE 1344, IEEE C37.118, and IEC 61850 [6].

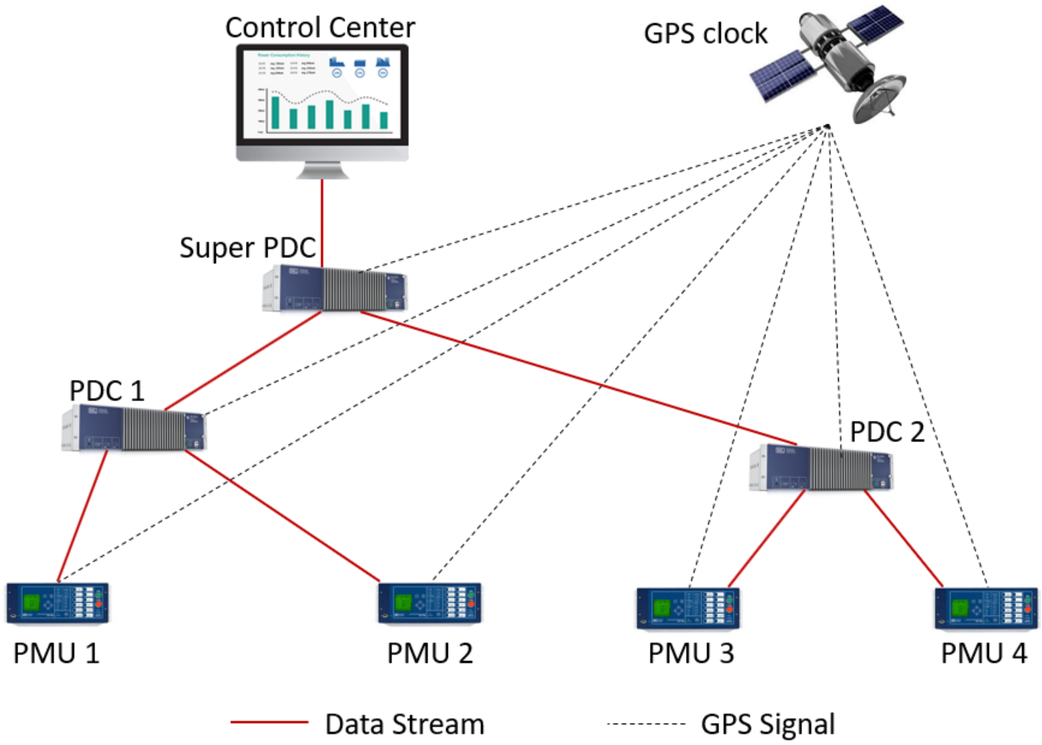


Figure 2: WAMS Network Architecture

2.2.3 Communication Protocols

The communication of synchrophasor measurements from PMUs in the field to the control center is done by using WAMS-specific communication protocols. With different regulations pertaining to different regions, 2 main protocols have been developed for synchrophasor communication: The widely used IEEE C37.118 [19] and the newer IEC 61850-90-5 [20]. Both establish data transmission formats for real-time synchrophasor data transfer.

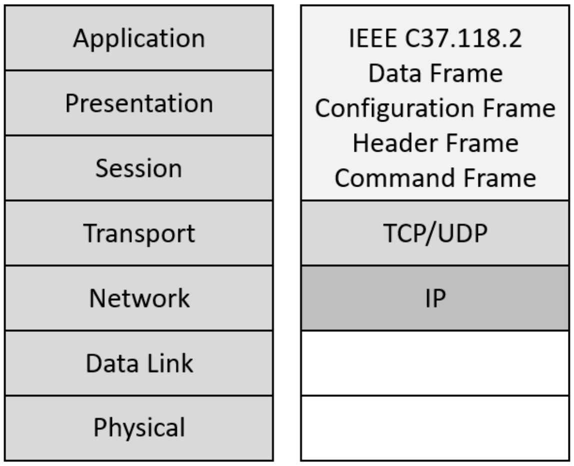


Figure 3: IEEE C37.118 Protocol Stack.

IEEE C37.118

IEEE C37.118 addresses the measurement and communication needs for synchrophasors, which represent requirements for accuracy verification, data transmission formats and real-time communication. IEEE C37.118 was first introduced in 2005 as the successor of the IEEE 1344 protocol; in 2011, it was split into IEEE C37.118.1 for measurement-related requirements and IEEE C37.118.2 for data transfer requirements [18].

The IEEE C37.118 protocol stack is illustrated in Fig. 3. IEEE C37.118.1 defines measurements including synchrophasor, frequency, and Rate of Change of Frequency (ROCOF); it also specifies the steady-state and dynamic performance requirements as well as time synchronization and data rates [21]. However, it does not tackle the different frame formats, their structures and functions, which are the main points of interest for DPI, because these attributes have to be leveraged by any DPI application to identify IEEE C37.118 packets, their type, and extract the information they carry. Such attributes are detailed in IEEE C37.118.2, which specifies message types, use, contents, and data formats for real-time communication between PMUs, PDCs, and other devices [18].

The IEEE C37.118 standard defines four types of messages related to the configuration and data transfer for PMU/PDC communication: data, configuration, header, and command frames. The first three frame types (data, configuration, and header) are sent from a PMU or a PDC, carrying synchrophasor measurements and configurations such as channel numbers and readable descriptive information. The last frame type (command) can be sent to both PMU and PDC for configuration and control purposes. All frame types share a common structure that includes frame identification and synchronization, frame size, data stream ID, timestamp, time quality, and Cyclic Redundancy Check (CRC) error check.

The data frames hold the measurement data, frequency and ROCOF collected and calculated by the PMU or PDC, as well as other analog sample and digital values. The configuration frames carry information and processing parameters of the data that the sender IED is capable of and is currently broadcasting. The header frames carry human-readable information about the PMU, the data sources, scaling and other related information. The command frames are sent by data receiving devices to the sending devices, with requests to start or stop transmission. These frames may also carry commands to send configuration information or to change configuration.

IEC 61850

IEC 61850 is a comprehensive standard for substation-based smart grid communications first published in 2004 [22]. As an Ethernet-based communication protocol intended for IEDs in electrical substations, IEC 61850 identifies general and specific communication functional requirements, which include high-speed IED-to-IED communication, high-availability, time requirements, multi-vendor interoperability, support for voltage and current measurements data, support for file transfer, and support for security features, among others [23]. The IEC 61850 defines abstract objects for the communication services using the Abstract Communication Service Interface (ACSI), through which the abstract objects are mapped to existing protocols.

This protocol-independent setup of data objects and services allows a mapping to any

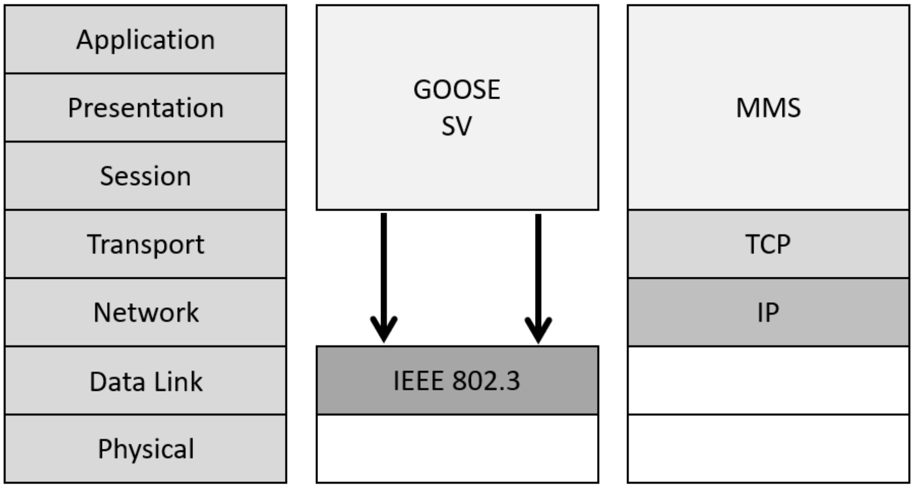


Figure 4: IEC 61850 Protocol Stack

new protocol that meets the defined data and service requirements [24]. This ensures the compatibility of protocols between a variety of power system components.

An overview of the IEC 61850 protocol stack is shown in Fig. 4. Currently, the standard maps the abstract objects to three main protocols [25]: Generic Object Oriented Substation Events (GOOSE), Sampled Values (SV), and Manufacturing Message Specification (MMS). GOOSE and SV are time-critical protocols involved in the protection and control of the substation; both GOOSE and SV operate on layer 2 of the OSI model to decrease the communication overhead. MMS operates on layer 3 of the OSI model and deals with substation devices management.

GOOSE. GOOSE is used to send control signals and warnings in substations when time-critical events take place [26]: as an example, protection commands are sent over GOOSE to substation IEDs within a four-millisecond time window. Consequently, applying encryption or authentication algorithms on GOOSE messages can be challenging because of the strict time constraints. In order to assure the integrity of the transmitted information, GOOSE will re-transmit the same message multiple times, which ensures receipt of the message and allows the receiver to compare the different messages and detect potential tampering or anomalies. GOOSE can also broadcast a wide range of data in a dataset across the substation Local Area Networks (LAN). A GOOSE frame consists of fixed, preset fields and variable fields in terms of length and content depending on the communicated information. Each frame can be divided into four parts: header MAC, priority tag information, Ethernet Protocol Data Unit (PDU) and GOOSE Application Protocol Data Unit (APDU) [26]. The header MAC, priority tag information and Ethernet PDU contain standard protocol and routing information such as destination and source IDs, protocol and virtual LAN identifiers, application identifier, and length [24]. The GOOSE APDU holds the state and sequence numbers that ensure message synchronization between the GOOSE sender and receiver.

SV. SV is used to transmit numerically sampled real-time values of power system measurements, such as line currents and voltages. It uses a publisher-subscriber model, where registered PMUs publish their measurements in the substation network such that subscribing PDCs can collect them [24]. In addition, SV has a very high sampling rate that can reach 4,800 messages per second. Consequently, encryption of the measurements may impose a large overhead on the network and violate the preset time constraints. SV utilizes different packet fields such as sequence number, sample count field and the time synchronization field to ensure the alignment of the received packets by the subscriber IED and the synchronization with the time source [27]. SV frames have a similar structure to that of GOOSE, which are divided into header MAC, priority tag information, Ethernet PDU and SV APDU. The measurements are encapsulated within the SV APDU, along with a sequence number field, a sample count field and the time synchronization field.

MMS. MMS is a client-server protocol used to transmit status information and commands for control, monitoring, and communication between user-interface systems and IEDs. MMS maps ACSI models of IEC 61850 to lower levels to ensure correct interpretation of information among IEDs [28]; the mapping includes a multitude of IEC 61850 objects, e.g., the data class, data-set and log classes. An MMS frame consists of a fixed sized header that contains information pertaining to version and packet length, and a PDU that holds a four-bit type specification field that indicates the type of the PDU, followed by the payload [29].

IEC 61850-90-5. IEC 61850-90-5 [20] was introduced in 2012 as an extension to the original IEC 61850 standard to address WAMS synchrophasor communications. It defines Routable GOOSE (R-GOOSE) and Routable SV (R-SV) packets which are layer 3 versions of the original GOOSE and SV protocols. These packets are used to establish connections, and transfer synchrophasor data between PMUs and PDCs. Furthermore, IEC 61850-90-5 emphasises communication security by introducing HMAC signature schemes and AES symmetric encryption to protect the integrity and confidentiality of the messages. It also offers a higher sampling rate than IEEE C37.118 that can reach 12000 samples/second. Table 1 presents a comparison of the features of the protocols.

Table 1: Feature Comparison Between IEEE C37.118 and IEC 61850-90-5

Features	**IEEE C37.118**	**IEC 61850-90-5**
Year	2005	2012
Protocol Stack	Network Layer	Network Layer
Sampling Rate	120 samples/second	12000 samples/second
Integrity	CRC	HMAC
Confidentiality	None	AES
Availability	None	None
Average Data Packet Size	112 bytes	305 bytes

2.2.4 WAMS Applications

WAMS applications improve on traditional SCADA systems with a faster, more dynamic and proactive grid stability management approach. These applications help the grid operators improve the performance of the transmission and distribution networks by portraying information about stability, system security and efficiency.

WAMS applications include phase angle monitoring, voltage stability monitoring, and power oscillation monitoring among others. In this thesis we focus on 3 applications: PAM, FVSI and ISI. Next we will define each application, and explain its role in the control center.

Phase Angle Monitoring

PAM examines the active power going through a power line. It calculates the difference in voltage phase angles between the two ends of the line. The index is calculated following Equation 1.

$$Pr = \frac{V_s \times V_r}{X} \times sin\Delta \tag{1}$$

where *Pr* is the real power going through the line, V_s is the sending-end voltage, V_r is the receiving-end voltage, *X* is the line impedance between the two buses, and Δ is the difference between the voltage angles α_s and α_r.

Based on the angle difference, the operator may initiate different actions to improve the stability of the grid such as rescheduling generation or compensation of reactive power, reconfiguration of system topology, and load shedding [30].

Fast Voltage Stability Index

FVSI is a line voltage stability index that can determine the maximum possible line load, critical lines in inter-connected systems, and the point of voltage collapse [31]. It is calculated following Equation 2.

$$FVSI_{ij} = \frac{4 \times Z^2 \times Q_j}{V_i^2 \times X} \tag{2}$$

where *Z* is the line impedance, *X* the line reactance, Q_i the reactive power at the receiving end, and V_i the voltage at the sending end. FVSI can range from 0 to 1. An FVSI value greater than 0.7 implies that the line is exhibiting instabilities. In such situations, the operator may disconnect the line or modify the generator's supply to avoid further damages and a possible system collapse.

Impedance Stability Index

ISI is a bus voltage stability index that leverages the load impedance and Thevenin impedance at a load bus to determine the point of voltage collapse [32]. It is calculated following Equation 3.

$$ISI = 1 - \frac{\Delta V_j \times I_{ji}}{V_j \times \Delta I_{ij}} \tag{3}$$

where ΔV_j and ΔI_{ij} are the differences between two consecutive voltage and current measurements reported by PMUs, respectively. V_j and I_{ji} correspond to the voltage and current values at load bus *j*. ISI can range from 0 to 1. An ISI value close to 0 indicates critical voltage instability at the bus, which can lead the operator to inject reactive power, adjust the generation or initiate load shedding.

2.3 Cybersecurity Threats in WAMS

The critical role of WAMS in the SG renders it an appealing target for cyber attackers. In addition, the deployment of densely connected information systems increases the attack surface that can be used to compromise WAMS. Attackers can take advantage of the cyber-physical nature of WAMS and launch cyberattacks against the information system and attacks against the physical assets in the grid. The closely connected physical and digital aspects of WAMS allow cyberattacks to have an impact on the physical operation of the grid. Harmful impacts from such attacks include increase in cost, power loss, transmission line tripping, unnecessary load shedding, and blackouts. Understanding an attacker's perspective is often a key to the successful defense. As such, extensive efforts have been made to investigate prominent cyber-physical attacks and develop DPI-based Intrusion Detection Systems (IDS) taking into account the cyber-physical context [33]. In order to better discuss the discovered threat models in the context of DPI, this section will categorize the threats based on where the anomalous or malicious information is injected to affect the packet payloads. Specifically, the threats addressed will be categorized based on whether the intrusion is predominantly launched on the IEDs or in the communication channels. It is notable that a large number of schemes can be launched on both targets.

2.3.1 Attacks on Endpoints

Attacks on IEDs aim to gain access to the endpoint devices and directly tamper with the generation of the packets. To this end, attackers may exploit back-doors, firmware vulnerabilities, specialized malwares, phishing emails, or may attempt to physically access the IED in remote sites. The targeted IEDs may range from Programmable Logic Controllers (PLC) as in the Stuxnet attack [12] to control center workstations as in the Ukrainian power grid attack [8], and all the RTUs, PMUs, intelligent relays, and PDCs in-between. It is notable that many critical endpoint IEDs are protected behind industrial firewalls or demilitarized zones. Also, the attackers may not be able to manipulate all packet payloads on a compromised device because of restricted access to overwrite in many fixed-function IEDs. Nevertheless, from the attacker's perspective, the IEDs may provide convenient capacity and privilege for them to send legitimate messages at the full speed to inflict great impacts on the grid with false commands and/or misleading information. The attacks in this class include packet modification, false data injection, command injection, and fuzzing which we will detail next.

Packet modification

Packet modification attacks assume that the attackers have gained access to the sensing devices and can directly manipulate different packet fields to trigger improper behavior in the system. As one of the most intuitive threat models, packet modification has been investigated extensively in generic ICT networks, while a small number of studies have been dedicated to the smart grid context.

False Data Injection

The term FDI can be used to describe an attack that injects any type of data in the system such as measurements, commands, configuration information, etc. However, in this thesis, we use the term FDI to refer to attacks that target solely the measurements as described in [34] and we consider command injection attacks as a separate class of attacks.

FDI is a widely investigated threat that targets exclusively the measurements reported for grid control decision-making. It can be viewed as a special case of packet modification with significant impacts on the smart grid. As the term FDI may refer to any attack that injects false data into the system, we specify two classes of FDI: the generic FDI and the stealthy FDI. In the generic FDI, an attacker sends false measurements to the control center without particularly leveraging the specific residual-based model vulnerability and grid topology [34]. The stealthy FDI is a special data integrity attack first proposed by Liu *et al.* [34] to exploit a mathematical model vulnerability in the power system state estimation. While the threat has yet to be implemented as part of a practical scheme, numerous studies have shown that the stealthy FDI scheme can exploit the knowledge of system topology to manipulate the measurements, without being detected by the existing residual-based Bad Data Detector (BDD) installed in control centers.

State estimation can be formulated by the linear function:

$$z = Hx + n \tag{4}$$

where z is the measurement vector, H is the topological Jacobian matrix, x is the state vector to be estimated, and n is the noise vector. The estimated state $\hat{x}$ can be given by:

$$\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} z \tag{5}$$

where R is the covariance matrix of an assumptive zero-mean white Gaussian noise of the sensors. The conventional BDD calculates the residual between observed and estimated measurements:

$$z - H\hat{x} \tag{6}$$

to identify and eliminate a noisy data. With the knowledge of H and the ability to manipulate z, however, it has been shown [34] that an attacker can effectively bypass the BDD and manipulate the measurements. While no incidences have been reported, extensive studies have shown that the stealthy FDI can cause transmission congestion, mask line outages, and obtain illegal gains in the electricity market, among others [35].

Command Injection

Command injection is one of the most impactful threats, where an attacker directly issues a false command to the IEDs and actuators. For the smart grid, command injection can cause immediate impact on critical systems and processes under control, especially when limited response time is allowed for authentication or verification between the arrival and execution of a command in many protection and control applications.

Fuzzing

Fuzzing is a common threat on packet generation. In this scenario, the attacker tries to randomly modify the packet content to create invalid or unexpected packet fields. The device receiving the modified packet is then observed to detect exceptions such as crashes and memory leaks as a result of the received random information [36].

2.3.2 Attacks on Communication Channels

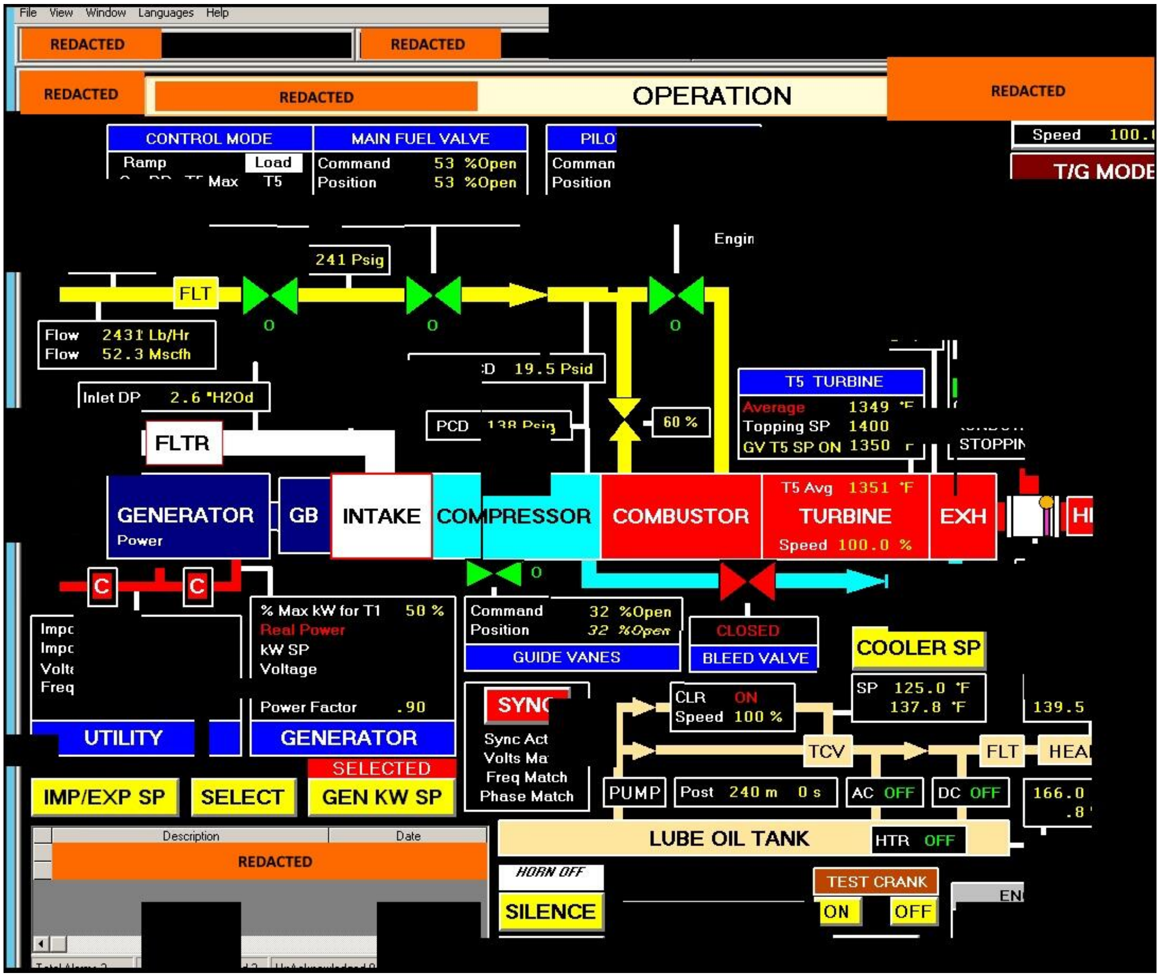
Compared to the endpoint IEDs, communication networks and channels constitute a large attack surface over dispersed geographical areas, making them attractive targets to intercept the packets and manipulate their payloads. The low-speed, security-deficient SCADA networks and protocols have long been a target of cyber-attacks [37]; even in the high-speed Industrial Control System (ICS) networks that allow limited time to tamper with the packet payloads, skillful intrusions [38] and advanced persistent threats [39] can still effectively compromise the network to inflict major disturbances into the interconnected power grids. The threats in this category include scanning, sniffing, spoofing, Denial-of-Service (DoS) and Distributed DoS (DDoS), Man-in-the-Middle (MITM), and replay attacks, whose details will be reviewed next.

Scanning Attack

Scanning is a common precursor for most cyberattacks. This information gathering technique has been increasingly employed by ICS and smart grid attackers [40] to gain high-level intelligence of network topology, communication protocols, and traffic patterns to conceive a sophisticated attack scheme, especially for power systems with proprietary networks, protocols, and ports.

Sniffing Attack

Sniffing is another early stage attack, where an attacker passively eavesdrops or examines the content of packets. Records of packets of interest may be retained without manipulating the traffic, providing detailed information on physical system environment, configuration and behaviors to construct well-informed attacks [33]. In the smart grid, sniffing has been shown to provide crucial in-depth intelligence of the interconnected systems and devices, as shown in Fig. 5. The figure depicts an HMI screenshot of a power plant ICS intelligence acquired by threat actors, reported in ICS-CERT Technical Alert 18-074A [38]. The screenshot shows redacted information of a generator-turbine control panel with system specifications and dynamic status [38].



Speed 100.

CONTROL MODE
Ramp Load
Max T5

MAIN FUEL VALVE
Command 53 %Open
Position 53 %Open

PILO
Comman
Position

241 Psig

Engin

Flow 2431 Lb/Hr
Flow 52.3 Mscfh

Inlet DP 2.6 "H2Od

D 19.5 Psid

PCD 138 Psig

60 %

T5 TURBINE
Average 1349 °F
Topping SP 1400
GV T5 SP ON 1350

STOPPIN

T5 Avg 1351 °F
Speed 100.0 %

Generator Power

Impc
Impc
Volt
Freq

% Max kW for T1 50 %
Real Power
kW SP
Voltage
Power Factor .90

Command 32 %Open
Position 32 %Open
GUIDE VANES

CLOSED
BLEED VALVE

Sync Act
Volts Ma
Freq Match
Phase Match

CLR ON
Speed 100 %

SP 125.0 °F
137.8 °F

139.5

Post 240 m 0 s
AC OFF
DC OFF
HTR OFF

166.0
.8

Figure 5: HMI Screenshot Sniffed by Threat Actors in the U.S. Energy Infrastructure

Spoofing Attack

Spoofing is a critical threat in the smart grid [41], where an attacker infiltrates the network by disguising as a legitimate user in order to initiate a trusted connection. A successful spoofing can allow the attacker to inject malwares, bypass access controls, mislead honest devices, and obtain confidential data. Spoofing attacks may also involve the connection of an unidentified rogue device into the network to conduct scanning, sniffing, and other schemes.

Denial-of-Service and Distributed DoS

DoS and DDoS are prominent cyber-threats [42, 43] that can also significantly compromise availability in the smart grid [44]. On the Internet, DoS/DDoS attacks like Mirai botnet [45] prevented massive numbers of users from accessing network resources or hardware devices. In the context of smart grid, DoS/DDoS can result in degraded, delayed, or completely disconnected communication, impairing situational awareness and control capacity over critical systems and processes in the smart grid.

Replay Attack

Replay attack is a widely-seen threat that records past packets and re-sends them at a future time. The re-sent packets usually follow the same legitimate format except for outdated sequence numbers or timestamps; as a result, checking and ensuring the freshness of the received packets can mitigate such attacks. In the context of smart grid communication, replay attack is mainly focused on synchrophasors, where the attacker would replay measurements of recorded faults or disturbance to mislead the controller into adopting improper responses against non-existent events.

Man-in-the-Middle Attack

MITM attack is another common generic threat model in the smart grid. It refers to the family of schemes where attackers are able to insert themselves in the network between the sender and the receiver of a communication [46]. This can be leveraged to launch attacks such as sniffing, spoofing, and replay attacks among others.

2.4 Deep Packet Inspection

2.4.1 Definition

DPI is a widely-used context-aware security monitoring technique for cybersecurity [47]. It analyzes the payloads of packets passing network inspection points, e.g., firewalls, routers or switches, in order to find matching patterns corresponding to a known misuse, intrusion, or other incidences. Compared to common packet filtering techniques, the term “deep" in DPI refers to the direct inspection of payloads, or the actual contents to be communicated, for anomalous or malicious activities. Compared to packet headers and network flow statistics, the payloads may carry more information on the context of communication and may reveal additional traces of the activities of interest. Such advantage often makes DPI a popular choice to examine network application signatures, detect potential intrusions, identify sensitive information leakage, manage network bandwidth, enforce copyright protection, and censor digital contents, among others [48]. A typical DPI procedure consists of two main functionalities, i.e., *recognition* and *action* [47]. During recognition, relevant information such as application protocols and data units are extracted and compared to a set of pre-defined anomalous or malicious patterns. If a match is found, actions may be triggered to raise an alarm, drop the packet, log the event, and/or inform the administrator.

2.4.2 Deep Packet Inspection in the Smart Grid

Most of the existing works on DPI applications in the smart grid focus on the recognition functionality due to the complexity of the action functionality: in the Internet and other communication networks, actions by DPI can be determined within the context of cyberspace; in the smart grid and other cyber-physical systems, however, most actions are dependent on the physical system applications and requirements, which can involve sophisticated physical system processes and responses. As opposed to traditional Information Technology (IT) systems, the main focus in Operational Technology (OT) and cyber-physical systems is on data availability and timeliness subsequently, DPI cyberattack detection measures should be accurate and fast in order avoid any delays in the communications. Furthermore alerting should be real-time to allow for fast reaction in order to avoid damage to physical assets. In addition, cyber-physical systems such as the SG have unique communication protocols with real-time performance demands that carry domain specific data like voltage and current measurements [49]. In this thesis, we discuss detection and classification as two critical tasks of DPI in smart grid security and we focus on anomaly detection for a specific attack threat. In both tasks, the inspection of the payloads may foster the discovery of otherwise stealthy attacks without knowing the context. To illustrate the importance of DPI, consider an insider who launches a data integrity attack by modifying the measurements, which may result in major consequences by evoking unnecessary control responses without affecting the header fields. In practice, such attack can be launched by a grudging employee who may access field devices and manipulate the readings. Simple access control policies may not flag the access as anomalous; network and system management tools may not detect abnormal behavior when traffic statistics, e.g. packet size, packet delivery rate, and inter-arrival time, are not affected. The “shallow" packet inspection that analyzes header fields like MAC addresses, IP addresses, and/or port numbers may also be bypassed as these fields would remain normal to the system. With DPI that monitors the content of the network, however, anomalies against system models, predictable trends, or safety margins could be flagged and reported for further investigation, thus restricting and mitigating the potential impact of the attack [50].

2.5 Anomaly Detection

The abundance of cyber-physical data and the complexity of cyber-physical threats have attracted significant interest and progress on the context-aware DPI methods for smart grid security monitoring. In general, these methods can be categorized into two categories, i.e., anomaly detection and attack classification, which focus on the identification of anomalous and malicious events, respectively. Based on the physical context utilized in the DPI techniques, both categories can be further divided into rule-based and data-driven techniques: the former leverages physical models and system specifications to derive rule sets and attack signatures, while the latter employs data mining and machine learning methods to derive new models that characterize anomalous or malicious patterns. The DPI-based anomaly detection focuses on the segregation of anomalous data and events from normal operations. The anomalies refer to the nonconforming patterns, which can be characterized based on pre-defined physical models in rule-based techniques or measurement-based statistical models in data-driven techniques [51]. In this thesis we focus on anomaly detection because anomaly detection methods only require normal data to train and develop which aligns with the real-world operation of the smart grid where normal data is abundant but attack data is scarce.While classification requires data corresponding to normal and attack instances which is very hard to generate in a real setting because of the potential damage such attacks can have.

2.5.1 Rule-based Anomaly Detection

Rule-based anomaly detection depends on expert knowledge, standards and system specifications to set conditions that model the normal behavioral patterns. Subsequently, the rules developed tend to be simple to understand and can be easily interpreted by the operator. Anomalies are instances that break any one of the set rules. However, developing rules that cover all possible normal scenarios in a complex system, such as the smart grid, can become strenuous and almost unattainable.

2.5.2 Data-driven Anomaly Detection

Data-driven techniques employ data mining and machine learning methods such as statistical inferences, unsupervised learning, and semi-supervised learning [52]. These methods take complex data, such as PMU measurements, as input, and create models of normal operations from the measurements. Data-driven techniques require sizeable training datasets to produce robust, well-grounded models capable of capturing compound non-linear patterns, in order to differentiate between normal system measurements and anomalies.

2.6 Classification

For classification of different attack scenarios, most works in the DPI literature also utilize either the rules based on attack signatures and system specifications, or the data-driven methods based on supervised machine learning. Similar to the rule-based anomaly detection, the rule-based attack classification rely on expert knowledge to develop the rules that can classify a packet into the category of attacks, faults, and normal operations, or their potential sub-types. The supervised machine learning also aims to achieve the same objective by using measurement data labeled as normal, fault, and attack. When a sufficient amount of labeled data is available, an accurate mapping can be generated such that unlabeled data can be assigned corresponding labels with high confidence [53]. As suggested by the term supervised, labels must be pre-acquired to obtain the mapping through an adaptive training process, however, obtaining labeled data for large-scale, realistic datasets may be very costly

2.6.1 Rule-Based Classification

Rule-based attack classification depends on expert knowledge to assign the classes through rules, attack signatures and system specifications that must be obtained for different conditions. Other than the simplicity and efficiency, one main advantage of rule-based DPI in attack classification is the interpretability of labels, which allows the controller to precisely investigate the misbehavior and take necessary action quickly. An instance is considered an attack if it follows all the rules of specific attack signature. Consequently, rule-based techniques usually produce a smaller number of false alarms because the rules are specifically tailored to each attack. However, developing such rules and signatures can be tedious and hard, and might not scale up to large complex systems.

2.6.2 Data-Driven Classification

To address the growing complexity of attack classification in the smart grid, significant interest has been drawn to the data-driven methods, particularly supervised machine learning and deep learning, for the development of DPI techniques. These models take large, complex datasets that contain data from normal and attack scenarios in order to learn to differentiate between them. Data-driven techniques require large datasets for training, and usually perform better the larger the training dataset.

2.7 Conclusion

This chapter provided an overview of the concepts and technologies related to the studied research topic. These include legacy SCADA systems and modern WAMS. This chapter discussed the difference between SCADA and WAMS, and the role of WAMS in the SG. It also discussed the architecture of the communication system in WAMS, the WAMS-specific communication protocols, and the different WAMS applications. Furthermore, this chapter outlined the cybersecurity threats, their locations and types in WAMS. In addition, this chapter outlined specific concepts related to DPI, classification, and anomaly detection, which are used in the proposed solution of this research work tackling the problem of WAMS security. The provided background information lays out a good foundation to better understand the related work on WAMS and its cybersecurity.

Chapter 3

Literature Review

This chapter presents a literature review on the topics of FDI attacks, anomaly detection, and classification for the security of different areas of the SG. The background knowledge on these topics represents an important element of this research work. The related work on FDI attacks describes two types of FDI attacks: generic and stealthy. In addition, it discusses recent surveys tackling FDI schemes and countermeasures, and it highlights different approaches utilized to detect FDI attacks. The related work on anomaly detection describes the different anomaly detection models applied to detect cyberattacks in the SG. It groups the approaches into two main categories: rule-based and data-driven, and each category is further split into several subcategories. Similarly, classification models used to characterize cyberattacks in the different SG domains are presented in the classification section. They are also divided into rule-based and data-driven categories with each category split into several subcategories. Fig. 6 shows the taxonomy of the studied DPI techniques based on methodologies. Furthermore, we summarize all the works related to WAMS, in the WAMS-specific section, where we highlight the benefits and limitations of each work, and we present the different research gaps that can be addressed, which include the topic tackled in this thesis.

3.1 False Data Injection

FDI attacks can be categorized in two main classes as previously outlined in Section 2.3.1: generic FDI and stealthy FDI. Generic FDI has been studied from the control side and from the customer side of the SG. On the control side, the generic FDI has been the subject of various DPI investigations with smart grid specific protocols, including Modbus [54, 55], IEC 60870-5-104 [56], IEEE C37.118 [57], and IEC 61850 SV [58], among others. On the customer side, the generic FDI attacks are often leveraged in energy theft, which manipulate the smart meter readings to report a lower consumption and obtain a financial gain. Attacks on Advanced Metering Infrastructures (AMIs) can target ANSI C12.19, C12.22, IEEE 802.15.4, and other AMI-related protocols at various geographic locations [59, 60].

On the other hand, stealthy FDI was first introduced in [34] to exploit a vulnerability in the mathematical model of the power system state estimation. It is directed exclusively against the measurements used in the decision-making process of the system operator. In recent years, interest has increased in stealthy FDI attacks and their detection, and this can be seen by the large number of articles tackling this problem. As a result, recent surveys have provided a comprehensive audit of the state-of-the-art FDI attacks and defense strategies [61–64]. As stealthy FDI attacks manipulate the physical measurements directly, most IDS employed against these FDI schemes will rely on DPI techniques to identify the threats, although a small number of statistical methods have also been proposed, as can be seen in these surveys. To date, different studies have investigated DPI solutions against stealthy FDI threats for WAMS [65–67], substations [68], microgrids [69] along with other studies that tackle this problem without specifying a particular domain of the SG [70–74]. Details and results of these studies are presented in Section 3.2.

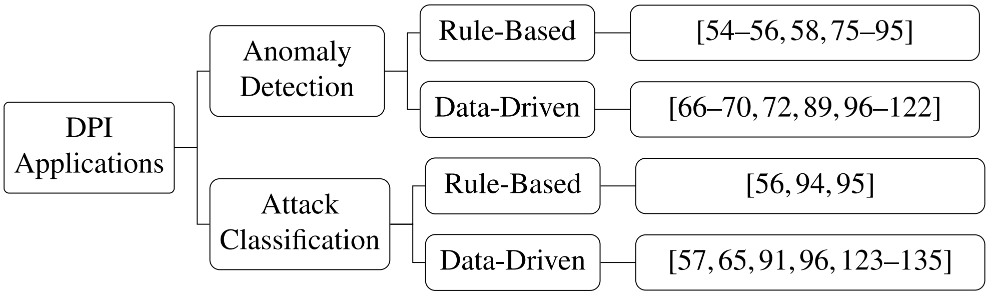


Figure 6: Taxonomy of DPI Techniques Based on Methodologies.

3.2 Anomaly Detection

Based on the existing studies in the literature we split the anomaly detection techniques into two large categories: Rule-based and data-driven. Both categories are unsupervised learning approaches since the models learn the normal behavior of a system from regular, none-attack data points only. We further split rule-based approaches based on the communication protocol they model. However, data-driven models are divided into five subcategories: statistical inferences, clustering methods, decision trees, neural networks, and kernel methods.

3.2.1 Rule-Based Deep Packet Inspection for Anomaly Detection

Rule-based anomaly detection has been mostly investigated based on protocols used in different applications of the smart grid. The rules are system-specific: for example, rule sets for PMUs made by different vendors or installed for different monitoring purposes [136]. Subsequently, developing scalable or reusable rules for all possible normal scenarios can become tedious for the interconnected and inter-operating devices in the smart grid. Nevertheless, for fixed-function IEDs and small-scale systems, rule-based DPI-based anomaly detection has been widely investigated. The works in this area will be reviewed below.

Modbus Protocol

Rule-based anomaly detection has been shown to be highly effective on Modbus due to the simplicity of the protocol. Morris *et al.* [54] described the conversion of Modbus RTU to Modbus/TCP and develop 11 rules to detect intrusions in Modbus/TCP. The rules were tested in two settings: in the passive setting, network traffic is logged and intrusion detection is performed offline; in the inline setting, the IDS takes the role of as an intrusion prevention system (IPS) and drops anomalous packets. The simulations showed that the inline IPS introduces time delays that can be acceptable depending on the system requirements. The work was further extended to 50 IDS rules [79] using a comprehensive specification of Modbus/TCP and Modbus over Serial Line protocol packet fields. Collectively, these DPI rules examine the majority of packet fields, including transaction identifier, protocol identifier, unit identifier and function code. Faisal *et al.* [75] used the Modbus specification and expert knowledge to develop detection rules over Modbus/TCP function code field and packet response time. The rules are customized for the communication requirements, which were tested on real-life datasets from a water storage facility and a university campus power grid. The results demonstrated that the rule-based DPI is both more accurate and efficient compared to conventional Deterministic Finite Automata (DFA) and Discrete Time Markov Chains (DTMCs). A hybrid IDS automata was proposed in [55], which combines the communication network rules with the physical system limits to detect the anomalies. The method examines control commands, current measurements, circuit breaker status, packet sequence, elapsed time between consecutive packets and physical systems constraints to monitor the entire traffic and context of Modbus communication. The results demonstrated that the hybrid automata can effectively detect malicious packet injection, malicious transformer isolation, or imitation of the master controller's behavior.

DNP3 Protocol

Similarly to Modbus, DNP3 has the protocol simplicity that benefits rule-based detection techniques. Wei *et al.* [76] proposed a role-based access control and deep packet inspection system for DNP3 in distribution substations. The IDS inspects the DNP3 function code, source and destination station numbers, object group, as well as their variation and index. The experiments showed that while effective at detecting and preventing illegitimate access to IEDs, the approach added a round trip delay of five to twenty milliseconds between master and slave. Lin *et al.* [86] also proposed a rule-based intra-packet and inter-packet validation for DNP3. The intra-packet validation examines the fields in a single packet (e.g., if the value of the length field is consistent with the real payload length) while inter-packet rules investigate the sequence of packets. For example, a packet holding the command “OPERATE" is almost always issued right after a “SELECT" command packet to control the remote field devices chosen by the previous “SELECT" packet. This technique was used to analyze real-life data coming from an Ohio electrical power grid utility. The results showed that the DNP3 parser processed 30% more packets/second that the DNP3 analyzer. This is due to the costly analysis performed on almost all DNP3 fields.

IEC 61850 Protocols

IEC 61850 has been the most investigated standard for rule-based anomaly detection due to its popularity, importance, and comprehensive specifications for monitoring, protection, and control. Hong *et al.* [58] investigated rules over GOOSE and SV packets for host-based and network-based IDS solutions. The host-based IDS examines device settings and logs, while the network-based aspect evaluates GOOSE and SV packet fields such as sequence and state numbers in GOOSE and message counts in SV. Under different attacks, both IDS perform similarly well with false positive and false negative rates lower than 0.1%. The work also introduced an attack similarity index that leverages data from multiple substations to detect coordinated, multi-substation attacks. Kwon *et al.* [78] proposed statistical rules for GOOSE and MMS packets using a multitude of flow features. These include the rates of packets, bytes and connections, the recency, frequency and monetary aspect of GOOSE packets, and the MMS messages such as confirmed response and unconfirmed report. Each feature is weighted and they are all added to get an anomaly score. This method was tested under multiple attack scenarios and reported an FP rate of 0% and an FN rate of 1.1%. Yang *et al.* [77] developed an IEC 61850 substation-specific IDS. The design is composed of four components: the access-based detection where Media Access Control (MAC) address, IP address and port number are inspected; a protocol filter for specific protocols such as GOOSE and MMS; an anomaly behavior detection that tracks the format of different fields in the filtered protocol; and a remote signaling checker that inspects if measurements are within a certain range and if MMS and GOOSE packet contents are consistent. The work was further expanded in [87], where substation configuration language (SCD) files and IEC 61850 traffic were included for inspections of sequence number increments in GOOSE, priority field in GOOSE and SV, and SV measurements ranges. The two studies combine packet headers and payload data with access control, network configuration, signal comparison, and substation settings, providing a holistic view of the substation behavior in order to improve the detection performance. The results show that the proposed technique effectively identified the different attack scenarios.

IEEE C37.118 Protocol

Despite its importance, IEEE C37.118 has been less investigated for anomaly detection due to its complexity. The protocol employs different frames, each carrying different functions and different data types, that are transmitted at different rates, making it difficult to formulate effective rules. Yang *et al.* [80] investigated behavior-based rules that inspect packet protocol pattern, time synchronization of messages, range of physical measurements, and length of packet fields. The results have shown that the rules were able to properly identify scanning, sniffing, MITM, and DoS/DDoS attacks. Sprabery *et al.* [85] also proposed a rule-based IDS for the IEEE C37.118 synchrophasors. The authors developed 36 single and multi-packet rules to detect anomalous behavior in each of the four protocol frames. The rules were tested against a protocol fuzzer in both online and offline settings without generating any false positives.

Advanced Metering Infrastructure Protocols

DPI techniques have been extensively investigated for IDS in the AMI and smart meters, especially for energy theft attacks. Berthier *et al.* [84] propose a rule-based IDS for ANSI C12.19 and C12.22. The rules focus on identifying compromised meters and network activity in Neighborhood Area Networks (NANs) by enforcing network-based, device-based, and application-based constraints. The technique was able to detect all malicious meter reading and connection requests in real-time. However, the sensors used do not handle encryption, which is not the case in realistic setups. Jokar *et al.* [91] propose a rule-based energy theft detection that compares the total electricity delivery to a neighborhood based on transformer meter reading with the total consumption reported by the smart meters of that neighborhood. A discrepancy between the two values will trigger an alarm signaling possible theft. The checker is complemented by an support vector machine-based classifier to confirm and localize the attack. The approach downsamples the data to preserve the privacy of the customer without compromising the detection performance. Chakraborty *et al.* [92] propose an IDS for a dedicated Distributed and Intelligent Energy Theft (DIET) attack. The proposed IDS monitors a cluster of smart meters and compares the electricity usage reported by a meter and its neighbors to the total usage calculated by the controller. The cross-checking allows the IDS to identify inconsistencies and report the anomalies.

Multiple Protocols

Some of the DPI techniques can be generalized to multiple protocols simultaneously. Yang *et al.* [81] extended the work in [80] by including more protocols such as Modbus, DNP3, IEC 61850, IEC 60870-5 and IEC 60870-6. The extension includes more rules for compliance checks for the additional protocols. Notably, these additional checks can efficiently monitor multiple protocols without incurring significant latency to the network traffic. Morris *et al.* in [83] explore cybersecurity requirements for synchrophasors in multiple protocols. Requirements such as access control, audit requirement, continuity of operation, and use of cryptography in Modbus and IEEE C37.118 protocols, were derived from the National Institute of Standards and Technology (NIST) Inter-agency Report 7628 guidelines for smart grid security, along with the Department of Homeland Security Cyber-Security Procurement Language for Control Systems, and the utility internal requirements. The rules were tested on commercial PMUs and PDCs from different manufacturers, under DoS and fuzzing attacks. Limited testing results were provided due to confidentiality agreements and ethical reporting requirements.

Bao *et al.* [88] present encryption for attack prevention and a state machine model for detection. Elliptic curve digital signature algorithm [137] was implemented and was able to prevent sniffing and MITM attack. The state machine method successfully detected inside attackers that tampered with the measurements. However, the authors do not specify the protocol they considered, they only state that they examined PMU measurements.

3.2.2 Data-Driven Deep Packet Inspection for Anomaly Detection

Data-driven DPI techniques have been effectively introduced in numerous IDS designs [138], which utilize statistical inferences, unsupervised learning, semi-supervised learning, and other machine learning techniques to create models of normal operations from the measurements. The data-driven techniques usually require a large number of data to create reliable and robust models, which can capture complex nonlinear relations and patterns that can pinpoint anomalies from system measurements. A variety of data-driven anomaly detection algorithms have been proposed for DPI-based security monitoring in the smart grid, which can be categorized into five main classes: statistical inferences, clustering methods, decision trees, neural networks, and kernel methods. The details are presented next.

Statistical Inference

Statistical methods are classical anomaly detection techniques that use probability distribution and statistical tools to identify outliers. In general, data points distant from the distribution of normal events are flagged as anomalous. Some of the classical statistical inferences used for anomaly detection include Bloom filter [139], probability density functions and Chi-square test [140], which are relatively lightweight, efficient, and less data-demanding compared to other data-driven techniques. Among notable statistical inference-based DPI techniques for smart grid communication, Kundur *et al.* [98] proposed a probabilistic IDS for Modbus/TCP traffic using Bloom filter and n-gram analysis. The IDS inspects the function codes and PDU collected from normal, remedial, and emergency states to identify the anomalies. The approach achieved a FNR between 2% and 6% and a FPR of 0%. The statistical methods have also been shown to be effective against FDI attacks. Pal *et al.* [100] proposed a Chi-square test against stealthy FDI attacks. The Gauss-Newton algorithm [141] was used to estimate line parameters, e.g., resistance, inductance, capacitance, and conductance, from PMU data. A Chi-square test is performed based on known and estimated line parameters to detect the anomalies. Chakhchoukh *et al.* [101] also proposed a statistical inference approach for anomaly detection. Assuming that the samples observed by the attacker are drawn from a changing distribution that is different than the one of normal measurements, the work applies Density Ratio Estimation (DRE) [142] to identify anomalous instances. The method calculates the density ratio between the Probability Density Function (PDF) of normal operations and the PDF of a given observation, on which a preset threshold determines if the latter represents a class of anomalies. Using stealthy FDI attacks as the anomalous event, the approach outperforms Support Vector Machines (SVM) and Gaussian methods under different tested scenarios. Esmalifalak *et al.* [102] compared the Gaussian PDF and SVM for detection of stealthy FDI attacks. The Gaussian PDF calculates the probability that a data point is similar to normal data and flags it as anomalous if the probability is lower than a learned threshold. SVM is applied in a supervised learning setup. Gaussian PDF outperformed SVM on smaller training sets but performed worse when the training set size was increased. In a similar work, Gu *et al.* [103] propose the use of Kullback-Leibler (KL) divergence to compare dissimilarity between the probability distributions of normal and attack incidences. Considering both FDI and replay attacks as the unknown anomalies, the KL divergence achieved more accurate detection performance than absolute distance. However, it was noted that FDI-induced anomalies on certain buses were more difficult to detect when there are fewer lines connecting these buses to the rest of the grid. In addition, the work of Liu *et al.* [70] introduces two statistical based techniques, nuclear norm minimization and low rank matrix factorization for FDI detection. These techniques were tested on multiple datasets and under different assumptions such as missing measurements data and showed effectiveness in detecting FDI attacks with a True Positive Rate (TPR) of varying between is 93% and 95%. In [72], the authors propose using a Kalman filter along with a Chi-square detector and a Euclidean distance metric detector to identify FDIs. The Chi-square detector failed to identify stealthy attacks while the Euclidean distance metric technique succeeded in doing so. The authors in [73] also use a Kalman filter along with a Chi-square detector which yields the same outcome as [72]. In addition, [73] proposes a cosine similarity matching approach that was able to detect FDI.

Clustering Methods

Clustering is a widely-used unsupervised method that groups data points into clusters without knowing any ground truth (actual labels). In anomaly detection, clustering can be applied to form a group of closely-arranged normal data, outside which a more distant data point will be considered as anomalous. Kundur *et al.* [66] propose a clustering-based DPI against false PMU data injection. Expectation-Maximization (EM) clustering was utilized to optimize intractable likelihood functions and find missing data points. On the IEEE 14-bus system, the method was shown to be capable of detecting all false PMU data injected at different locations of the grid.

Decision Trees

Decision trees are well-established machine learning algorithms. Originally developed for classification, some of their variants are capable of performing unsupervised anomaly detection. El Chamie *et al.* [99] propose a physics-based unsupervised and supervised learning framework to detect anomalies in distribution systems using the measurements. Tested on an IEEE 34-bus test feeder system, the unsupervised isolation forests learn normal patterns from unlabeled data and represent them with a pseudo-label; a random forest is then created to map input features to the pseudo-label. A threshold is applied for anomaly detection, which achieves an F_1 score of 0.903 against single line to ground fault and breaker tripping attacks in the distribution system.

Neural Networks

Neural Networks (NN) have seen much success in anomaly detection [138]. As complex higher-order nonlinear models, NN-based DPI has shown the ability to accurately learn the patterns of normal behavior out of data and differentiate them from abnormal actions.

Valdes *et al.* [68] propose a SOM-based IDS to learn normal behavior patterns of SV measurements in an IEC 61850 substation. In this work, a new class is learned if the feature vector does not match any known pattern in the SOM. The model was tested using three setups and achieved 0.01% FPR and 100% attack detection rate in some cases. Hariri *et al.* [69] propose a time-series NN with one hidden layer for anomaly detection in microgrid SV packets. This lightweight technique achieved a FP rate of 0.5% over anomalies caused by FDI attacks within the strict time requirements of the protocol. Wang *et al.* [67] propose a DAE based anomaly detection against PMU data manipulation in the smart grid. By inspecting the WAMS measurements, the DAE-based method outperformed other techniques, including XGBoost and SVM, with an F_1 score of 0.938. DAE allows to compress the input into a smaller representation, then tries to reconstruct the initial input vector, by decoding the information in the compressed representation. In addition, a delayed triggering algorithm is applied to account for noise and reduce FPR. For stealthy FDI detection, Niu *et al.* [64] employ Convolutional Neural Network (CNN), a popular feed-forward ANN, and LSTM neural networks, to account for time-related knowledge. This method examines measurements and flow features and achieves an accuracy between 80% and 100% depending on the capabilities of the attacker. In [74], Recurrent Neural Networks (RNNs) are applied to detect stealthy FDI attacks in the IEEE 14-bus systems. The applied techniques are shown to be successful in detecting FDI attacks with high accuracy, achieving an F_1 score of 0.95.

Kernel Methods

Kernel methods like SVM aim to map the data with kernel functions a into higher dimensions, where it would be easier to distinguish the difference among different distributions or classes of data. The SVM is one the most widely used kernel algorithms, which constructs an optimized decision boundary to separate instances of different classes. The unsupervised learning variant of SVM for anomaly detection, known as one-class SVM, has been shown to be able to handle large, complex datasets in an efficient manner. Yoo *et al.* [97] propose a one-class SVM for anomaly detection over the MMS and GOOSE traffic from a real-life IEC 61850 substation in South Korea. The method processes both single packets and combined packet sequences to extracted features including MMS message, GOOSE sequence and state numbers and packet headers. The EM clustering and local outlier factor (LOF) were applied during data preprocessing to remove outliers, before one-class SVM was used to develop the normal-behavior model, which achieved a FPR between 0.01 and 0.06.

3.2.3 Deep Packet Inspection for Anomaly Detection

The surveyed research works include an abundance of rule-based anomaly detection techniques in the smart grid. This may be attributed to the simplicity and popularity of some protocols such as Modbus and DNP3. In addition, it is easier to model the normal behavior of a system than modeling the malicious behavior of attacks, particularly when attack data is difficult to obtain.

It was also observed that statistical inference approaches perform well on simple protocols like Modbus but the number of attack scenarios addressed was relatively small. The majority of the surveyed statistical methods only focused on anomalies in a single protocol or those caused by only the FDI attack. In contrast, other data driven methods like ANNs and SVM have demonstrated convincing performance on larger systems and with more protocols and attack scenarios. As the smart grid demonstrates increasing non-linearity, uncertainty, and time-variance, there is a growing interest in moving from rule-based and statistical DPI toward more advanced data-driven methods.

All the reviewed techniques demonstrated a high accuracy on a variety of datasets or testbeds. Some of the articles used real-world smart grid communication traffic from a university grid [75] or a field substation [87, 97]. A number of recent works leveraged HIL testbeds for SCADA systems [55, 98], WAMS [96], Substation Automation Systems (SAS) [58, 68, 77, 78], and microgrids [69]. Software-based simulations were conducted in the MATLAB/Simulink environment, using standardized test systems like IEEE 14-bus [66, 67], 34-bus [99], and 118-bus [101, 102] systems to generate the measurements. The diversity of research works offers an extensive coverage of different operation and attack scenarios while leaving a significant gap with respect to benchmarking the performance among different works.

3.3 Classification

Similarly to anomaly detection, we split the existing classification studies in the literature into two categories: Rule-based and data-driven. Both categories fall under the supervised learning class since the models learn from both normal and attack behavior of a system. We further split rule-based approaches based on the communication protocol they model. However, data-driven models are divided into four subcategories: statistical methods, nearest neighbors, decision trees, neural networks, and kernel methods. In addition, some works present a number of less common ML algorithms along with other works providing comparative studies on classification methods on smart grid datasets.

3.3.1 Rule-Based Deep Packet Inspection for Classification

Rule-based DPI techniques for attack classification have also been developed for different smart grid protocols. Similarly to rule-based anomaly detection, rule-based attack classification techniques still face major difficulties to scale up in larger systems or to be reused in more complicated scenarios. This, coupled with the lack of known attack signatures in the

SG context, results in a notably reduced number of research works aimed in this direction.

IEC 60870-5-104 Protocol

Compared to other modern protocols for smart grid communication, IEC 60870-5-104 is one of the least complicated, which allows for easier development of rules based on the system behavior and attack signatures. Yang *et al.* [56] developed signature-based and model-based attack classification, respectively, for IEC 60870-5-104. The signature-based checker matches observations against an attack signatures database; it also contains rules that look for unauthorized interrogation commands sent to a server. The model-based checker inspects the transmission cause, length field and TCP port number of the agent initiating connections. This allows to create rules based on system specifications and to classify misuses against these rules.

IEEE C37.118 Protocol

IEEE C37.118 packets carry heterogeneous yet critical information for control, measurements, and configuration settings, which has attracted significant research efforts and was accompanied by notable results. Khan *et al.* [94] propose a rule-base classifier for the IEEE C37.118 synchrophasors based on the NIST-recommended security architecture. The system is expected to be deployed in different IEDs, local networks, and wide area networks in the smart grid. Behavioral patterns of known malicious signatures from all systems will be collected to classify the data and ongoing events. The design also creates validity rules that check the range of the physical measurements and rules that track the packet sequences over time. The rules are shown to be able to accurately identify several attacks on the IEEE C37.118, including GPS spoofing, MITM, packet injection, and packet drop. The work was further extended in [95] to include signatures of more sophisticated attacks and new rules to detect stealthy data manipulation attacks, which gradually modify physical measurements over an extended time. The results of this work were validated on a HIL microgrid testbed and demonstrate that simple rules remain effective against the extended list of attacks.

3.3.2 Data-Driven Techniques

Data-driven classification techniques utilize supervised machine learning techniques to create robust models, from labeled datasets, able to distinguish between normal and attack instances. Similar to anomaly detection, data-driven DPI in attack classification also include statistical methods, nearest neighbors, decision trees and neural networks. As in the case if anomaly detection, some works present a number of less common ML algorithms while other works provide comparative studies on classification methods on smart grid datasets. Subsequently, we detail the work done in each of these classes.

Statistical Methods

Statistical methods, most notably probabilistic graphical models [143], have been introduced for DPI-based attack classification due to their advantage in representing complex probabilistic relationships using graphical representations. The graphs aim to create a concise encoding of a high-dimensional feature space that expresses the conditional dependencies between features. The main advantage is the use of domain knowledge to create an intuitive representation of the features and their dependencies, which reduces the computational overhead for inference and scales up to large, high-dimensional datasets. In this direction, Pan *et al.* [57] proposed a Bayesian network for the classification of attacks and faults in WAMS. The Bayesian network examines current measurements and event logs under a combination of two fault and four attack scenarios. With a clear depiction of the dependencies and interdependencies between features, the Bayesian network model is able to correctly classify all test cases defined in the study.

Nearest Neighbors

Nearest neighbors are simple, efficient classification techniques that assign a label to an incoming data sample based on the labels of the nearest data points. The approach does not need to retain or update a complex model, making it ideal for attack classification at end-point devices. Adhikari *et al.* [126] proposed an IDS that creates Non-Nested Generalized Exemplars (NNGE) from a State Tracking and Extraction Method (STEM). The STEM pre-processes raw PMU measurements and event logs to generate a continuous stream of states with low storage overhead. The NNGE, a nearest-neighbor-like algorithm, is trained on the state stream to extract generalized exemplars. The exemplars are then used as signatures to classify the incoming data into corresponding classes. This hybrid approach achieved a 98% accuracy in binary classification between benign and malignant events and a 94% accuracy for multi-class classification among different types of faults, attacks, and normal operations.

Decision Trees

As mentioned earlier, decision trees are widely used in classification tasks, using a tree structure that resembles human reasoning and decision-making process to assign the class labels. They generally rely on entropy measures when segmenting the dataset and building the tree. The interpretable nature of decision trees is favorable for security applications, as it provides explainable decision support. For smart grid security monitoring, classic decision trees are often combined with other pre-processing techniques to improve their performance over the complex cyber-physical data.

Adhikari *et al.* [123] propose a DPI-based attack classifier with Hoeffding Adaptive Trees (HAT), augmented with the Drift Detection Method (DDM) and Adaptive Windowing (ADWIN). Using HAT as the base classifier, the approach addresses the fast-dynamics and slow-drifts in smart grids by introducing the DDM as a change detector and the ADWIN as a model re-trainer. Once significant changes have been identified, ADWIN will prompt the re-training or fine-tuning of a well-trained HAT to retain its classification performance among normal, fault, and attack classes.

Wang *et al.* [127] propose an attack classifier against FDI attacks with consideration of imbalanced data. Assuming that attack incidences are much more scarce than normal and fault data, the method leverages the Synthetic Minority Over-Sampling Technique (SMOTE) and Edited Nearest Neighbors (ENN) to create a balanced dataset that is aimed to boost the classification performance. SMOTE is first applied to randomly select minority data points and interpolate new data between a selected minority point and its neighbors [144]. The ENN is then applied to clean the oversampled data by removing noisy outliers in the minority class. With the re-balanced data, XGBoost [145], a more recent technique that leverages an ensemble of decision trees to improve classification performance, is used to classify the FDI attacks. Overall the approach achieves a 0.891 F_1 score.

Neural Networks

Instead of trying to learn a representation of normal patterns for anomaly detection, NNs can also be directly trained to assign class labels to a data sample based on the predicted likelihood that it belongs to different classes. The prediction is provided through a multi-layered non-linear mapping between the features and the label of the data sample. The NN's ability to extract complex context and relations from measurements to determine the situation translates well to DPI-based monitoring for the smart grid. He *et al.* [128] proposed a deep learning-based IDS against stealthy FDI attacks under different conditions like meter fault, and measurement noise among others. A Conditional Deep Belief Network (CDBN) is developed by stacking multiple Restricted Boltzmann Machine (RBM) layers over a Conditional Gaussian-Bernoulli RBM (CGBRBM) layer that integrates temporal information into the model. The attack data in the dataset are up-sampled using Fourier transform and Principal Component Analysis (PCA) [146] to obtain an adequate number of compromised instances for training. The CDBN is shown to outperform simple SVM and NN classifiers, with an accuracy over 90% under simulated attack scenarios. Hamedani *et al.* [130] propose Delayed Feedback Networks (DFN) for stealthy FDI detection. The DFN is used as a Reservoir Computing (RC) system to process the data as a temporal sequence [147]. By taking into account the time-domain information, DFN also outperformed the SVM and NN classifiers against both generic and stealthy FDI attacks under different attack scenarios.

Other Data-Driven Deep Packet Inspection for Attack Classification

Other than the well known machine learning techniques, a Common Path Mining (CPM) technique was also proposed by Pan *et al.* in two DPI-based attack classifier designs [96, 125]. The CPM creates a generic stateful signature of known scenarios in the smart grid. In [125], CPM uses system measurements and relay status as features. Against simulated one-line-ground fault and command injection attacks, CPM achieved a 95% accuracy. In contrast, when the one-line-ground faults were diversified with different fault locations and system loads, CPM's accuracy dropped to 87.6%. Moreover, when four additional short-circuit faults and three cyberattacks were introduced, CPM accomplished a 93.2% accuracy. The work was extended in [96] where CPM was evaluated against 25 fault and attack scenarios. When all scenarios were present in the training set, CPM achieved a 90.4% accuracy with a 0.8% FP rate. Meanwhile, it is notable that CPM performance could drop to 73.47% when some of the scenarios were randomly removed from the training set, showing a limited capacity to generalize against some zero-day threats.

Comparative Studies

Given the popularity and variety of data-driven techniques, some researchers have conducted comparative studies to establish performance benchmarks of well-known data-driven classifiers. Hink *et al.* [124] compared the performance of seven different classification algorithms with different faults and attacks in the smart grid. The models were tested in three different settings, including a binary case with normal and abnormal (fault and attack) classes, a ternary case with normal, fault, and attack classes, and a multi-class case with 37 attack and fault scenarios. Among these three settings, a combination of AdaBoost [148] and JRip [149] had achieved the highest accuracy of over 90%, followed by decent performance of JRip and Random Forest that varied between 70% and 80%, and less-desirable performance of Naive Bayes, SVM, Nearest Neighbor and OneR that was less than 30% [124]. Comparative studies have also been conducted against FDI attacks. Yan *et al.* [65] tackled FDI by implementing SVM, k-Nearest Neighbor (kNN) and extended-Nearest Neighbor (eNN) for classification of stealthy and generic FDI on balanced and unbalanced datasets. SVM consistently outperformed the other techniques in all scenarios, while kNN and eNN had comparable results in all scenarios. Ozay *et al.* [129] provide a comparative study of 11 machine learning-based classifiers against false data injection. The techniques include supervised, semisupervised, decision-level and feature-level fusion, as well as online learning methods. The supervised techniques tested include perceptron, kNN, SVM, and Sparse Logistic Regression (SLR); S3VM was implemented as the semisupervised approach; AdaBoost and Multiple Kernel Learning (MKL) have been utilized for decision-level and feature-level fusion, respectively. Online learning techniques include Online Perceptron (OP) and OP with weighted models, online SVM, and online SLR were also tested. The methods have been evaluated on variants of FDI that differ in the attack strength, and the results have shown that kNN was the best-performer in small-sized systems but conceded to SVM in large-scale systems. The study has also found that semi-supervised methods are more robust than supervised methods when dealing with sparse data. Also, fusion methods were more robust against variations in data sparsity and system size. Furthermore, online learning and offline batch algorithms achieved similar results.

3.3.3 Deep Packet Inspection for Smart Grid Attack Classification

Attack classification requires the IDS to not only inform on events that are anomalous but also to identify those that are malicious, which is generally more challenging than the anomaly detection. As attack incidences are scarce and effective rules can become highly sophisticated, we observed a reduced number of rule-based DPI in attack classification. A lack of attack signature databases in the smart grid may also have limited the research efforts and progress. Meanwhile, the scarcity of attack data also poses challenges to data-driven techniques, despite the growing interests with the recent development of deep learning and other advanced artificial intelligence technology. Pre-processing techniques have been one of the major innovations in this direction: it has been shown that the efficacy of predictive models, especially decision trees, is heavily affected by the balance of labeled training data [150]. The proposed classifications techniques in the literature are validated on different datasets. Some of the works used WAMS HIL testbeds such as [96, 123, 125], while others utilized substation HIL testbeds [77, 80, 81]. Additionally, in two other studies [56,87], data from real-life electric utilities was leveraged to test the classification methods. Other works have also resorted to datasets of simulated power systems such as the IEEE 9-bus system [127, 129] and IEEE 118-bus system [128, 129], among others. Similar to the case of anomaly detection, the diversity of approaches offers the coverage of more scenarios while also making it difficult to compare their respective performance.

3.4 Wide Area Monitoring Systems Specific Works

In the literature, we found 10 research works that tackle attack detection and classification in WAMS using DPI extracted features. Figure 7 presents a taxonomy of the works based on the protocol studied. To the best of our knowledge, no research work investigated the IEC 61850-90-2 protocol. Table 2 details the surveyed works based on the testbed, simulated scenarios, extracted features, proposed technique, and detection performance. Table 3 provides a list of the scenario acronyms used in Table 2. Next, we compare the works based on each of these aspects.

First, with regards to the testbeds used, we notice that most works [57, 83, 85, 96, 123, 125, 126, 131] rely solely on small HIL testbeds (3-bus and 9-bus systems) and only 2 research initiatives [67, 151] test their approach on larger systems although their setup does not include HIL. Including hardware devices in the simulation is critical because this renders it more realistic and aligned with the operation of real utilities. Moreover, testing the proposed approach on both small and large systems such as the IEEE 30-bus system asses the scalability of the detection technique and further validates it if the results are consistent. Therefore, having a HIL setup in addition to evaluating the approach on small and large systems is essential in order to align the work with real-life grid operation.

Second, the WAMS articles consider different attack and fault scenarios. 5 works [57, 96, 123, 125, 126] simulate a wide array of attack and fault scenarios that include command injection, relay tripping, over current fault, and line to line fault. Simulating multiple attack and operational scenarios allows for the collection of large labeled datasets containing a variety of classes, knowing that such datasets are very rare and not usually shared by utilities. Subsequently, these works take advantage of a large number of available scenarios by developing classification models that differentiate between the distinct classes. On the other hand, the work in [67,83,85,131,151] focuses on 1 or 2 scenarios only. Some of these works [67, 131, 151] tackle attacks that target the physical measurements directly such as

FDI and fault replay attacks while others [83, 85] concentrate on fuzzing and DoS.

Third, in most articles except [151], the protocol used is IEEE C37.118 and the extracted measurement features involve voltage, current, frequency, and ROCOF. Some approaches [57, 96, 123, 125, 126, 131] combine the physical measurements with network and device logs in order to get a holistic view of the communications in the network. On the other hand, the articles studying fuzzing [83, 85] extract all the fields in the IEEE C37.118 and Modbus packets such as IP source and destination, port numbers, trigger reason, command, etc. and compare their values to preset rules. Wei et al. [151] specify the WAMS domain and the features without mentioning which protocol is used. Although all these articles focus on WAMS, we can see that the features that can be collected in this domain are numerous and heterogeneous, conveying information on different aspects of WAMS. Thus combining both data-driven and rule-based techniques to monitor the physical features, device logs, and network communications can be very advantageous.

Fourth, with regards to detection techniques, most articles [57, 96, 123, 125, 126, 131, 151] focus on classification of attack and fault scenarios using different data-driven techniques that include statistical inference, tree algorithms, CPM, nearest neighbor, and neural networks. The performance of these techniques is similar, ranging between 87% and 99% accuracy, however, it is difficult to directly compare their results and decide which approach is better because of the differences in the experimental setup, the simulated scenarios and the evaluation metrics used. Also, one work [96] combined classification and anomaly detection to differentiate zero-day events from known attacks, however, the technique was not very accurate. On the other hand, only 3 works [67, 83, 85] tackle anomaly detection, 2 of which [83, 85] are rule-based that focus on fuzzing and the other [67] uses DAE to detect FDI attacks. The research initiative in [83] modeled normal behavior while the one in [95] developed attack signatures to monitor all fields in all four IEEE C37.118 frames but did not provide the rules or detailed results. However, the authors test these rules against simple attacks in the context of a microgrid, without providing a detailed validation of the results. In addition, some of these attacks can be stopped by the security measures implemented in the IEC 61850-90-5 protocol.

Moreover, we notice a lack of works utilizing machine learning anomaly detection models against FDI attacks in WAMS. Notably, the initiative in [67] proposes a DAE approach to detect data manipulation attacks in WAMS, however, their approach requires the collection of PMU measurements from both sides of each line, which can be very costly because it requires the deployment of a large number of PMUs. Moreover, the aforementioned work focused on data manipulation attacks that randomly change the reported values, with limited focus and analysis of stealthy FDI attacks. Finally, to the best of our knowledge, there are no works that focus on anomaly detection of stealthy FDI in realistic environments while linking the attacks to WAMS applications in order to examine their perceived impact.

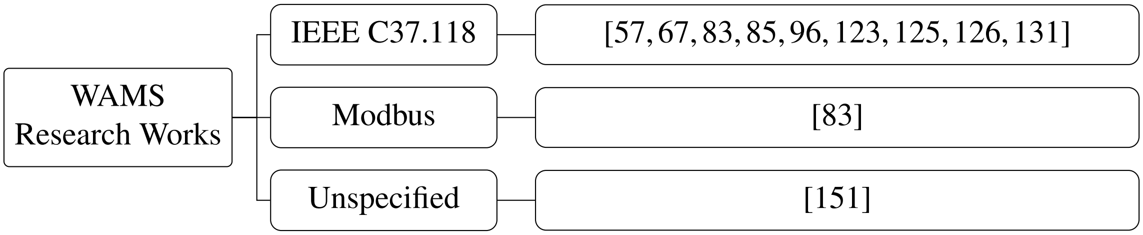


Figure 7: Taxonomy of DPI Techniques in WAMS Based on Protocols.

3.5 Gap Analysis

Extensive effort has been made to advance the state of DPI-based security monitoring in the smart grid. In this section, we provide a gap analysis of the smart grid applications and communication protocols, threat models, and DPI techniques. Based on the identified gaps, we reflect on the challenges and future research opportunities.

3.5.1 Applications and Protocols

Applications coverage

The majority of existing works have investigated SCADA and AMI applications, while SAS, WAMS, and microgrids are less investigated. Other emerging applications in the smart grid, such as renewable energy plants, distributed energy resources, demand response, distribution automation, among others, have not been investigated. DPI for microgrids also requires additional attention and exclusive investigations due to their lower system inertia, higher distributed energy resource installation, and different contexts between grid-connected and islanded modes. While the technological maturity, especially the availability of high-resolution physical measurements, may have a strong impact on the efforts and progress, many of these important applications still require significant enhancements to the security monitoring capacity under the increasing cyber-physical integration.

Protocol Coverage

Smart grid applications are supported by multiple protocols, while the existing coverage in the DPI literature is still relatively limited. Studies on SAS mostly focused on individual IEC 61850 protocols, while the incorporation of GOOSE, SV, and MMS messages simultaneously may provide additional context for the IDS. Within the IEEE C37.118 protocol, other frames (configuration, header, command) may also provide the communication system context in addition to the data frame. This would provide a holistic view of the WAMS communication between sensors and controllers and help identify more complex attacks and faults by integrating communication control information and configuration information into the detection models. Moreover, existing DPI works on AMI covered a diverse set of protocols, mostly due to the availability of public AMI datasets, but few have been evaluated and validated on a HIL testbed like other applications.

Protocol Overlap and Discrepancy

With the difference in standard requirements and regional regulations, the same functionality in a smart grid application may be covered by different standards and protocols. As an example, both IEEE C37.118 and IEC 61850-90-5 specify the requirement and protocol for synchrophasor communication in WAMS/WAMPACS [18]. To date, most DPI studies for WAMS focused on IEEE C37.118, which was released earlier than IEC 61850-90-5. Although IEEE C37.118 is currently the most widely used protocol for synchrophasor communication, it lacks security features to ensure confidentiality and strong integrity. IEEE C37.118 employs CRC checks to ensure integrity of the messages. An attacker knowledgeable of the CRC algorithm can modify the packet content and re-calculate the CRC field, allowing it to bypass future CRC verifications. IEC 61850-90-5 was introduced to address these security shortcomings. To guarantee confidentiality and integrity, IEC 61850-90-5 proposes the use of secret keys – shared and periodically refreshed by a key distribution center – for symmetric encryption and signature schemes. The proposed security features can help prevent attacks previously discussed such as sniffing, packet modification, packet injection, and replay attacks. IEC 61850-90-5 also offers a higher sampling rate through its R-SV protocol. R-SV has a sampling rate up to 4800 messages/second, compared to up to 120 messages/second for IEEE C37.118. This would provide the controller with a more detailed image of the system for real-time monitoring and diagnosis. However, due to the high sampling rate, encryption and signature schemes, and the bigger size of packets, IEC 61850-90-5 would also require more resources to implement, which calls for more efforts to investigate given its importance in future WAMS and WAMPACS applications.

3.5.2 Threat Models

Threat Details

The threat models addressed in the DPI literature contained certain levels of details, but most did not specify to the level of attack trees similar to the ones shown in Fig. 13, which illustrates the ways an attacker can compromise a circuit breaker at a SAS. Such level of granularity and visualization provides illustrative information and penetration paths of the threat to design and deploy security monitoring capacities at the most proper locations. From the attacker's perspective, many threat models assumed only the worst-case scenario, while in practice an attacker may not have full access the power grid's dynamic topology, operating points, or even the physical models, which will affect the actual impact. A detailed model on the knowledge and resource used to launch a successful intrusion, along with the projection of potential impacts, will provide a clear picture of cyber-physical vulnerabilities and threat intelligence to develop the needed security monitoring capacity for the smart grid.

Threat Timing and Persistence

The frequent sampling in smart grid communications not only affects the time window to launch an attack but also the success of a launched threat. Consider the example of FDI: a high sampling rate would require the attacker to tamper with a large number of packets over a relatively long period of time to effectively mislead the control actions, as a few modified SV packets may be simply discarded as outliers without triggering the emergency response. Therefore, a successful FDI on the SV packets will have to be an advanced persistent attack, which might not always be possible due to constraints on the attacker's resources and the countermeasures in the system. Even if the attacker targets protocols with low sampling rates like GOOSE, if the allowable packets exchange rate was not obeyed, the attempt may still be easily detected. As an example, an attacker may inject multiple

GOOSE commands into the network to trip a targeted relay, which will increase the number of GOOSE messages received by the subscribed IEDs. This deviation may be exposed by other context-aware security monitors, such as the Network and System Management (NSM) devices, who may report to the system manager for further inspection [152].

3.5.3 DPI Methodologies

Online Monitoring

Most data-driven methods have assumed an offline training/building process before online deployment. However, only a minority of them actually evaluate the performance in the actual online setting. The works in [54, 69, 85, 123] implemented the DPI in a HIL testbed to run the evaluations with limited fault and attack conditions. Only one study explored real-time classification over a wide array of scenarios [123]. In practice, online performance is critical to the success of security monitoring, especially for the smart grid where a long time-to-detection may result in a failed remedial effort on the physical side. The ability to adapt when changes occur in the system will also be critical in the online environment, as both the system dynamics and threat models may change over time and result in a degraded performance. Considering the affordability and availability of field test sites, HIL co-simulation testbeds [153] and digital twins [154] may provide the most cost-effective online platform for research and development of DPI-based security monitoring.

Advanced Data-driven Techniques

Another aspect that has attracted growing attention but was not fully addressed is the machine learning and deep learning algorithms for DPI approaches. Deep learning is a relatively new field that has been proven to be effective in many challenging tasks; the high dimensionality and complexity of smart grid data make deep learning a promising, customizable solution for advanced DPI solutions. However, the explainability and trustworthiness of deep learning in security decision-making and safety-critical applications remain to be fully demonstrated.

Hybrid DPI Techniques

While rule-based and data-driven techniques have been widely investigated, few have been combined to offer a multifaceted attack detector/classifier with rules defined by human experts and learned from machine intelligence. The rule-based techniques are suitable to simpler protocols like Modbus and DNP3, where normal and attack behaviors can be accurately modeled using rules; the machine learning techniques are highly effective for measurements over SV or IEEE C37.118 protocols because of the complexity and uncertainty of the physical system reflected in the measurements. A hybrid DPI may retain the accuracy from existing knowledge and the adaptability for incoming variants, combing the best from both sides for better context-aware security monitoring. As an example, to monitor the full behavior of the IEEE C37.118 protocol, all of the four frame types may be examined. The configuration, command, and header frames will demonstrate relatively simple behaviors over a small number of packets; subsequently, a set of rules may be able to characterize the normal behavior of packets and specify potential attack signatures. On the other hand, the data frame of the IEEE C37.118 protocol carries physical measurements of the power system; these data points may be impossible to model with simple rules due to the non-linearity, uncertainty, and time-variance. The challenges will call for more advanced data-driven techniques.

Combined Detection-Classification DPI

Finally, we identify the lack of combined classification-detection techniques that can accurately classify previously seen instances and flag zero-day behavior. Among the reviewed works, only two studies performed anomaly detection and classification simultaneously [91, 96], while the rest are investigating classification and anomaly detection separately. A hierarchical design or a collaborative pipeline may combine both detection and classification to offer enhanced robustness against real-world threats in the smart grid.

Table 2: Overview of WAMS research

Article	Testbed	HIL	Attacks	Faults	Approach	Technique	Features	Performance	Online/Offline
[57]	3-bus 2-generator	Yes	CI, PT, DI, BF	OCF, LMF	Classification	Bayesian Networks	Current, Snort log, relay log, control log (C37.118)	"All scenarios were correctly classified"	Offline
[67]	IEEE 9-bus system, IEEE 30-bus system	No	FDI	SCF	Anomaly Detection	DAE	Voltage, current, impedance (C37.118)	Acc: 94.1% F1: 93.8%	N/A
[83]	Connect physical PMU and PDC to RTDS	Yes	DoS, Fuzzing	None	Anomaly detection	Rule-based	All frame fields (C37.118, Modbus)	N/A	N/A
[85]	Connect physical PMU and PDC to RTDS	Yes	Fuzzing	None	Anomaly Detection	Rule-based (stand-alone and multi-packet)	All frame fields (C37.118)	N/A	Online + offline
[96]	3-bus 2-generator	Yes	CI, FR, RD, LMA, 1LF,AA	LGF, LL, LMF	Classification + Anomaly Detection	Common Path Mining	Voltage, current, impedance, frequency, phase angles, Snort logs (C37.118)	Multi-class acc: 90.4% Anomaly detection acc: 73.43%	Offline
[123]	3-bus 2-generator	Yes	CI, FR, RD, LMA, 1LF,AA	LGF, LL, LMF	Classification	Hoeffding Adaptive Trees	Voltage, current, impedance, frequency, phase angles, Snort logs (C37.118)	Binary acc: 98% Multi-class acc: 92%	Online
[125]	3-bus 2-generator	Yes	CI, FR, AA	LGF, LL	Classification	Common Path Mining	3-phase current, magnitude, relay logs (C37.118)	87.6∼95% binary and multiclass acc	Offline
[126]	3-bus 2-generator, IEEE 9-bus	Yes	CI, FR, RD, AA	LGF, LL, LMF	Classification	Non-nested generalized exemplar (NNGE)	Voltage, current, impedance, frequency, phase angles, Snort logs (C37.118)	Binary acc: 98% FPR: 0.05 Multi-class acc: 94∼95.5% Multi-class FPR: 0.05	Online
[131]	3-bus 2-generator	Yes	CI, FR	None	Classification	Stacked Autoencoder (SAE)	Voltage, current, impedance, frequency, Snort logs (C37.118)	Acc: 94∼99%	Online
[151]	39-bus New England test system	No	FDI	None	Classification	Conditional Deep Belief Network	Rotor angles, frequency (Unspecified)	N/A	N/A

Table 3: Acronyms of Simulated Scenarios

Scenario	**Acronym**
Single/Double Relay Trip Command Injection	CI
Fault Replay	FR
Single Relay Disabled Fault Attack	RD
Single/Double Relay Disabled Line Maintenance Attack	LMA
Double Relay Disabled with 1LG Fault Attack	1LF
Aurora Attack	AA
Denial of Service	DoS
Physical Trip of Relay at Faceplate	PT
Data Injection	DI
Breaker Failure	BF
1/2/3 Line Ground Fault (LGF)	LGF
Line to Line Fault	LL
Line Maintenance	LMF
Over current fault	OCF
Short Circuit Fault	SCF

Chapter 4

Methodology

In this chapter we detail the experimental framework that covers the developed benchmark power models used in the HIL co-simulation testbed, along with the communication protocols and tools used in the real-time simulation of the power system. Furthermore, we present the extracted features used, the threat model, and the implemented anomaly detection algorithms.

4.1 Hardware-in-the-Loop Co-simulation Testbed Setup

The WAMS co-simulation testbed is made of two parts: the real-time power model simulator and the communication network that connects the power model simulator with physical and virtual IEDs found in the network. The simulated model includes simulated equipment such as PMUs and PDCs that can send and receive messages over the network to communicate with Virtual Machines (VMs) and other IEDs. As a result, the information generated by the power model simulator can be shared with other devices deployed on the communication network for further analysis. Fig. 8 shows a high-level view of the WAMS co-simulation testbed.

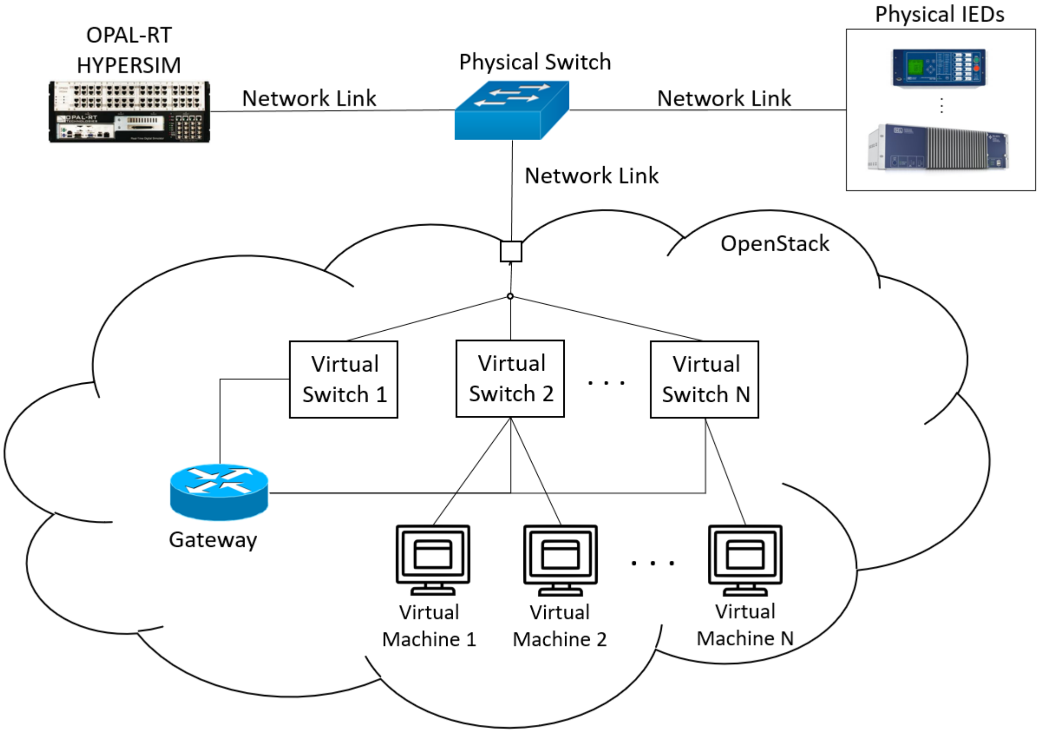


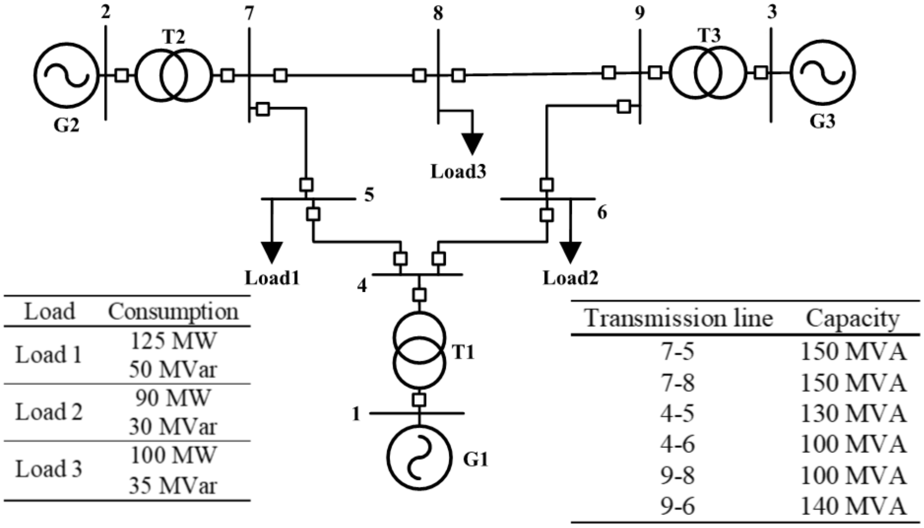
Figure 8: WAMS Co-simulation Testbed

4.1.1 Power Model

In this thesis, we develop the electric power models using Hypersim DRTS [155] developed by OPAL-RT Technologies. Hypersim DRTS can integrate HIL and different SG-specific communication protocols into the real-time simulation of the power grid, allowing real IEDs to act as part the power model simulation. Hypersim constructs electrical power system models using modular components that include simulated power generation sources, line equipment, control functions, control signals, and input and output nodes for communication with real IEDs connected to the simulation. These features of Hypersim provide the ability to monitor the operation of the power system under different conditions i.e. instabilities, faults, etc. Furthermore, Hypersim provides simulated real-time power system measurements like voltage, current and frequency. To achieve a co-simulation framework, power systems simulated in Hypersim can send and receive messages using SG-specific communication protocols over communication networks connected to the simulator. This allows the integration of real IEDs into the simulation that can exchange information and possibly impact the behavior of the simulated system. In this chapter, we construct two real-time transmission power models using Hypersim: IEEE 9-bus system and IEEE 39-bus system. The capabilities provided by Hypersim render it appropriate to evaluate the performance of DPI-based detection schemes against cyber-physical attacks in WAMS. Details on the constructed testbed are provided in the subsequent sections.

IEEE 9-bus System

The IEEE 9-bus system, also known as the P.M. Anderson 9 bus system, represents an approximation of the Western System Coordinating Council (WSCC) system. It comprises 9 buses, 3 generators, 3 power transformers, 6 lines and 3 loads. The base voltage levels are 13.8 kV, 16.5 kV, 18 kV, and 230 kV and the line capacities are between 100 and 150 MVA [156]. The active power of the loads ranges from 90 MW to 125 MW, and the reactive power ranges from 30 to 50 MVar. A single line diagram of the system is shown in Fig. 9



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 9: IEEE 9-bus System

IEEE 39-bus System

The IEEE 39-bus system, also known as the 10-machine New-England Power System, contains 39 buses, 32 transmission lines, 24 transformers, 10 generators and 19 loads. The complete system parameters are presented in [157]. A single line diagram of the system is shown in Fig. 10

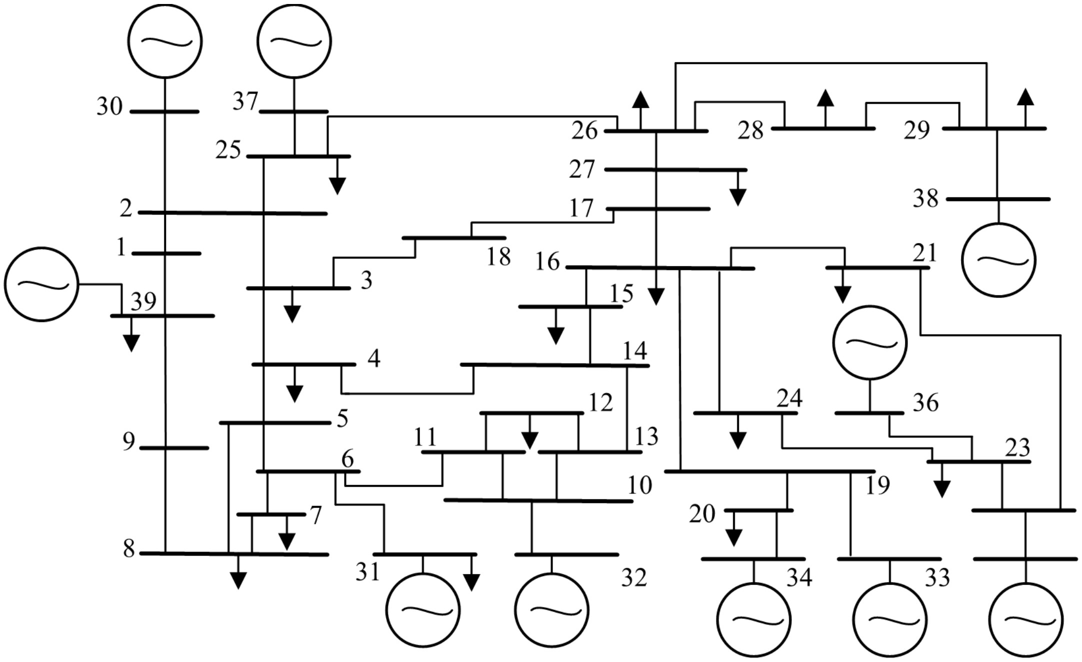


Figure 10: IEEE 39-bus System

4.1.2 Communication Model

We implement a communication network in the testbed in order to facilitate the transmission of digital messages carrying commands and physical measurements within the WAMS simulation. The communication network is a local IP network with configurable routing. Since we simulate different cyberattacks compromising the communication channels in this research work, having such an insulated and controllable network allows us to safely run cyberattack experiments without the risk of damaging publicly accessible devices and communication channels. We employ a server with an IP communication network to connect the Hypersim simulator with VMs, and real IEDs. VMs are deployed within the network and are used to collect and analyze packets in real-time. On the other hand, the Hypersim simulator uses built-in network interfaces to connect to the communication network. A physical switch connects the IP network and the Hypersim simulator through which they communicate. The communication network used in the testbed is built using OpenStack [158]. OpenStack is a software networking tool that provides the means to create and manage IP communication networks. It can create VMs and virtual network switches within the network, and configure communication channels between different machines, routers, and switches. The virtual switches allow subnetting of the VMs into different subnets with access to each subnet regulated by routing and firewall rules. In this work, we choose to use OpenStack to setup the communication network because it can easily integrate Hypersim into the IP network, create VMs that contain custom code for data collection and analysis, and configure access to different subnets. It is mandatory to integrate Hypersim into the IP network in order transport the physical measurements generated by the transmission power model to the WAMS applications and attack detection models in real-time. To perform traffic monitoring and launch cyberattacks, network bridges between different subnets are set up. These bridges contain custom code that captures and modifies packets coming from PMUs to PDCs on the fly and forwards them to other VMs that analyze the packet contents. This monitoring setup allows us to launch online cyberattacks, analyze their impact, and detect them in real-time.

4.1.3 Simulated Scenarios

In our experiments, we consider multiple scenarios as normal in our training set, and we use data from all of them to train our anomaly detection models. We use a load flow to simulate the normal behavior of the system over 24 hours as shown in Table 4 for the 9-bus system. This step is a very important aspect of our research because simulating the power model with varying loads over time renders our experiments more realistic. As such, they would resemble the behavior of real power models where loads are always changing. Furthermore, physical measurements under constant loads will show very little variation, rendering any change in their values very obvious thus not requiring advanced detection methods to spot attacks. Fig. 11 shows the voltage variation as the load varies over 24 hours, as measured by the PMU placed on bus 6 of the IEEE 9-bus system, under different conditions that include an increase of 50% of the load for a certain period of time, an increase in a generator's voltage and a decrease in a generator's voltage at different times of the day. Similarly, Fig. 12 shows the voltage variation as the load varies over 24 hours in the IEEE 39-bus system under normal conditions, an increase of 50% of the load, increase in a generator's voltage and a decrease in a generator's voltage at different times of the day. We collect the data of these scenarios and feed it to the anomaly detection algorithms for training. We include multiple variations of scenarios in our training set in order to depict the dynamic nature of the smart grid where we can see different, fast-changing behaviors that correspond to a safe state but are nevertheless very distinct.

4.1.4 Optimal PMU Placement

PMUs are becoming more and more an integral tool for monitoring and control in the SG. They provide instantaneous, time-aligned voltage, current and frequency measurements at the buses and lines connected to them. However, PMUs are expensive and require a dense communication infrastructure to deploy, which can increase the attack surface. Therefore, it is inadvisable and sometimes impossible to place PMUs at all buses of the grid for monitoring purposes. Subsequently, it is necessary to find the minimum number of PMUs that can provide full system observability to the control center. The Optimal PMU Placement

Table 4: IEEE 9-bus System Load Variation Over Time

Hour	Load 1 MW	Load 2 MW	Load 3 MW	Load 1 MVAR	Load 2 MVAR	Load 3 MVAR
0	67.2	84.1	60.5	23.5	33.6	20.2
1	62.6	78.3	56.4	21.9	31.3	18.8
2	59.8	74.8	53.9	20.9	29.9	18
3	58.1	72.6	52.3	20.3	29	17.4
4	57.7	72.1	51.9	20.2	28.9	17.3
5	59.1	73.8	53.1	20.7	29.5	17.7
6	63	78.8	56.7	22.1	31.5	18.9
7	71.2	89.1	64.1	24.9	35.6	21.4
8	78.5	98.2	70.7	27.5	39.3	23.6
9	84.6	105.7	76.1	29.6	42.3	25.4
10	90	112.5	81	31.5	45	27
11	93.6	117	84.3	32.8	46.8	28.1
12	96.2	120.3	86.6	33.7	48.1	28.9
13	98.5	123.1	88.7	34.5	49.3	29.6
14	99.3	124.1	89.4	34.8	49.7	29.8
15	100	125	90	35	50	30
16	99.7	124.7	89.8	34.9	49.9	29.9
17	99.9	124.9	89.9	35	50	30
18	99.4	124.2	89.4	34.8	49.7	29.8
19	97.2	121.5	87.5	34	48.6	29.2
20	93.5	116.8	84.1	32.7	46.7	28
21	91.8	114.7	82.6	32.1	45.9	27.5
22	85.9	107.4	77.3	30.1	43	25.8
23	77.7	97.1	69.9	27.2	38.8	23.3

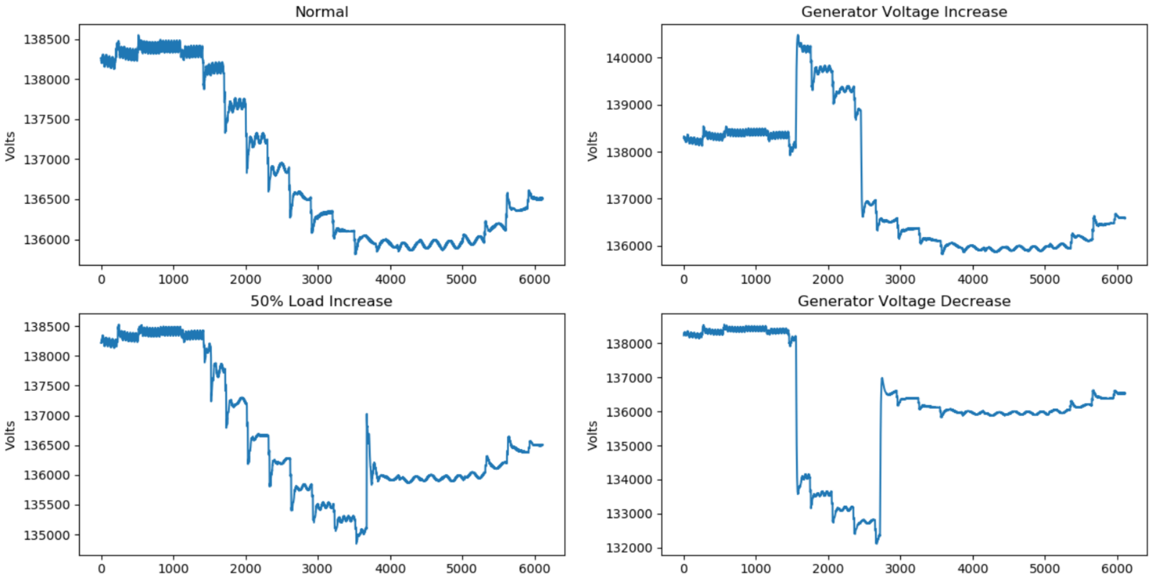


Figure 11: Load Variation in IEEE 9-bus System

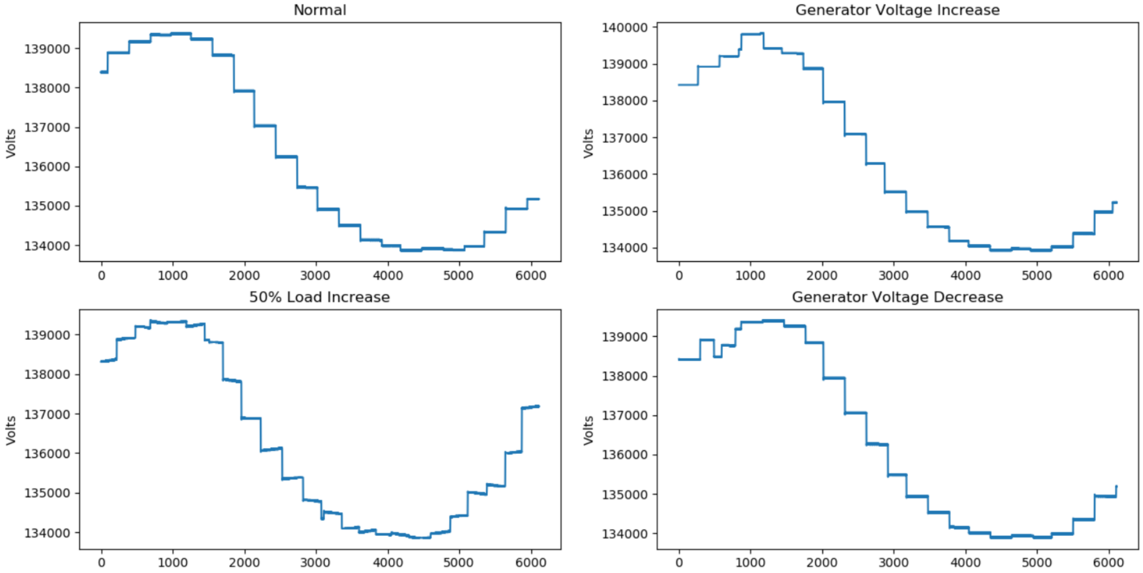


Figure 12: Load Variation in IEEE 39-bus System

Table 5: Optimal Locations of PMUs for the IEEE 9-bus and IEEE 39-bus Systems

Test System	Minimum Number of PMUs	PMU Locations (Bus)
IEEE 9-Bus	3	5,6,8
IEEE 39-Bus	13	2, 6, 9, 10, 11, 14, 17, 19, 20, 22, 23, 25, 29

(OPP) problem tackles this issue and aims to find the minimal suitable set of locations where PMUs can be installed in order to ensure system observability. In this research work, we choose not to collect the physical measurements from all possible buses, rather we opt to install a restricted number of PMUs on select buses only, in order to ensure a realistic setup. This approach aligns with real deployments of the smart grid previously outlined. The buses that hold PMUs are selected by solving the optimal PMU placement problem [159] that ensures system observability. The PMU locations for the 9-bus and 39-bus systems are taken from [160] and [161] respectively and are shown in Table 5.

4.2 Feature Extraction

Before training the anomaly detection models, feature extraction is necessary. This is a vital task in this research work because it can have an immense impact on the final result of the approach. In this chapter, we focus on applying anomaly detection algorithms on DPI-based features. Subsequently the features we use as input to these algorithms are extracted from the payloads of the IEEE C37.118 packets sent over the communication network. More specifically, the features we extract are the physical measurements collected by PMUs in the field and forwarded to the control center. These features include voltage phasors at the bus where PMUs are installed, current phasors for each line connected to the bus, frequency and ROCOF. After extracting the features, we perform 2 preprocessing steps: data cleaning and feature scaling. In data cleaning, we remove the instances that only have zeros for all the features. These correspond to dropped packets which happens occasionally over the network. Furthermore, we simulate each scenario for a specific time period beyond which the loads become constant at a generic value thus we extract all the instances that correspond to the simulated scenario by disregarding from the dataset all data collected before starting the simulation of the scenario and after the end of the simulation. All collected features are continuous variables that vary in different ranges. For example, voltage magnitude features vary between 120,000 and 150,000 while voltage phase angles oscillate between -180 and +180. Other features such as frequency show less variability, keeping a value close to 60 with small variations over time. In order to ensure optimal performance of the proposed models, we choose to scale our input data features to the range of [0, 1]. We do so because having features with different scales can mislead the learning algorithms, since features with larger scales can have a bigger influence on the outcome than those with smaller ranges, and this can lead to unsatisfactory detection results. To perform the scaling for each feature, we use the following formula:

$$X_{scaled} = \frac{X_{original} - X_{min}}{X_{max} - X_{min}} \tag{7}$$

where $X_{original}$ is the raw measurement collected from the packet, X_{min} is the smallest value for a particular feature, and X_{max} is the largest value for a particular feature. Applying this transformation for each feature in the dataset individually will result in changing the range of all the features to [0, 1].

Finally, the resulting feature vector coming from the 3 PMUs deployed in the 9-bus system is composed of 78 features collected and the feature vector of the 39-bus has 356 features collected from 13 PMUs.

4.3 Threat Model

WAMS and their applications play a vital role in securing and ensuring the stability of the electrical grid as shown by the reliance on these indices by grid operators when taking control decisions. Subsequently, attackers looking to cause significant harm to the grid find that targeting the measurements reported to these applications is very appealing. By altering the measurements, along with a sufficient knowledge of the grid, the attacker can portray a different scenario to the operator that might trigger unnecessary, harmful control actions, or hide real instabilities in the grid. For example, attacks on PAM by tampering the reported phase angles can lead to an increase in cost, power loss, and transmission line tripping. Also attacks on FVSI by modifying the reported voltage phasors can lead to load shedding, and blackouts. Furthermore, hiding an increase in the value of these indices can lead to equipment damage, blackouts, etc. because the operator would not notice any instability and subsequently would fail to issue commands to bring the grid back to its normal operation.

In addition, the WAMS-specific protocols do not offer the necessary security features to stop such attacks. IEEE C37.118 is the most widely used protocol currently, and it lacks confidentiality and robust integrity features since it only offers CRC error checking. A knowledgeable attacker can modify the measurements in the packet and recalculate the CRC field, bypassing future integrity verifications. IEC 61850-90-5 was introduced with added security features to address these shortcomings. It proposes the establishment of a key distribution center to share and periodically refresh secret keys among different IEDs for symmetric encryption and signature schemes. The proposed features enhance the security of the communications but attackers with sufficient capabilities can still bypass them and execute their attack successfully.

Fig. 13 shows the attack tree for successfully tampering with the reported measurements. The attacker has 2 paths to achieve his goal: attacking the communication network or attacking the PMUs directly. By gaining access to the communication network and establishing a MITM, the attacker can modify the measurements and the corresponding CRC while they are being transported over the network. However, the security measures introduced by IEC 61850-90-5 can stop such an attack because the attacker needs the secret encryption key to decrypt and sign the content of the packet. The second branch of the attack tree depicts a direct attack on the PMUs in the field. This is possible via installing a malware on the PMU, or by physically connecting to it and gaining access, which is a reasonable assumption given that these devices are often deployed in remote, unattended locations or in the case of an insider attack. In this scenario, both protocols are unable to deter the attacker because the integrity and confidentiality features implemented are compromised since the attacker controls the device and the keys stored on it. Thus, the currently used protocols are still vulnerable to stealthy FDI attacks that can lead to severe consequences for the smart grid.

In this research, we study 6 different stealthy FDI attacks. First we investigate attacks targeting the PAM, FVSI, and ISI applications where the attacker manipulates the reported measurements in order to portray an instability through the attacked application. Second, we investigate masking attacks whereby the attacker manipulates the reported measurements in a manner that portrays a normal operation of the grid while one of the applications is indicating an instability. Thus the term masking suggests that the attacker tries to hide/mask the instabilities from the controller.

4.4 Deep Autoencoders

Autoencoders are a subdivision of neural networks that are trained to predict the input they are given. In order to do so, an autoencoder has 3 main components: encoder, decoder and a bottleneck layer that separates the encoder and the decoder. The architecture of an autoencoder is symmetrical with respect to the bottleneck layer, that is there are the same number of hidden layers in the encoder and the decoder and the same number of neurons in each layer. And since the network is trained to predict the input, both the input and output layers have the same number of neurons. The encoder takes the input *x* and compresses it, using a smaller number of neurons, to get a representation of the initial feature vector *y* such that

$$y = \phi(x) = \sigma(Wx + b) \tag{8}$$

where $\sigma()$ is the activation function used, *W* is the weight matrix and *b* is the bias vector of the encoder.

The compressed representation of the input layer *y* is known as the bottleneck layer.

The decoder is trained to take the information in the bottleneck layer and reproduce the input layer using the information condensed in the bottleneck [162].

$$\hat{x} = \psi(y) = \hat{\sigma}(\hat{W}y + c) \tag{9}$$

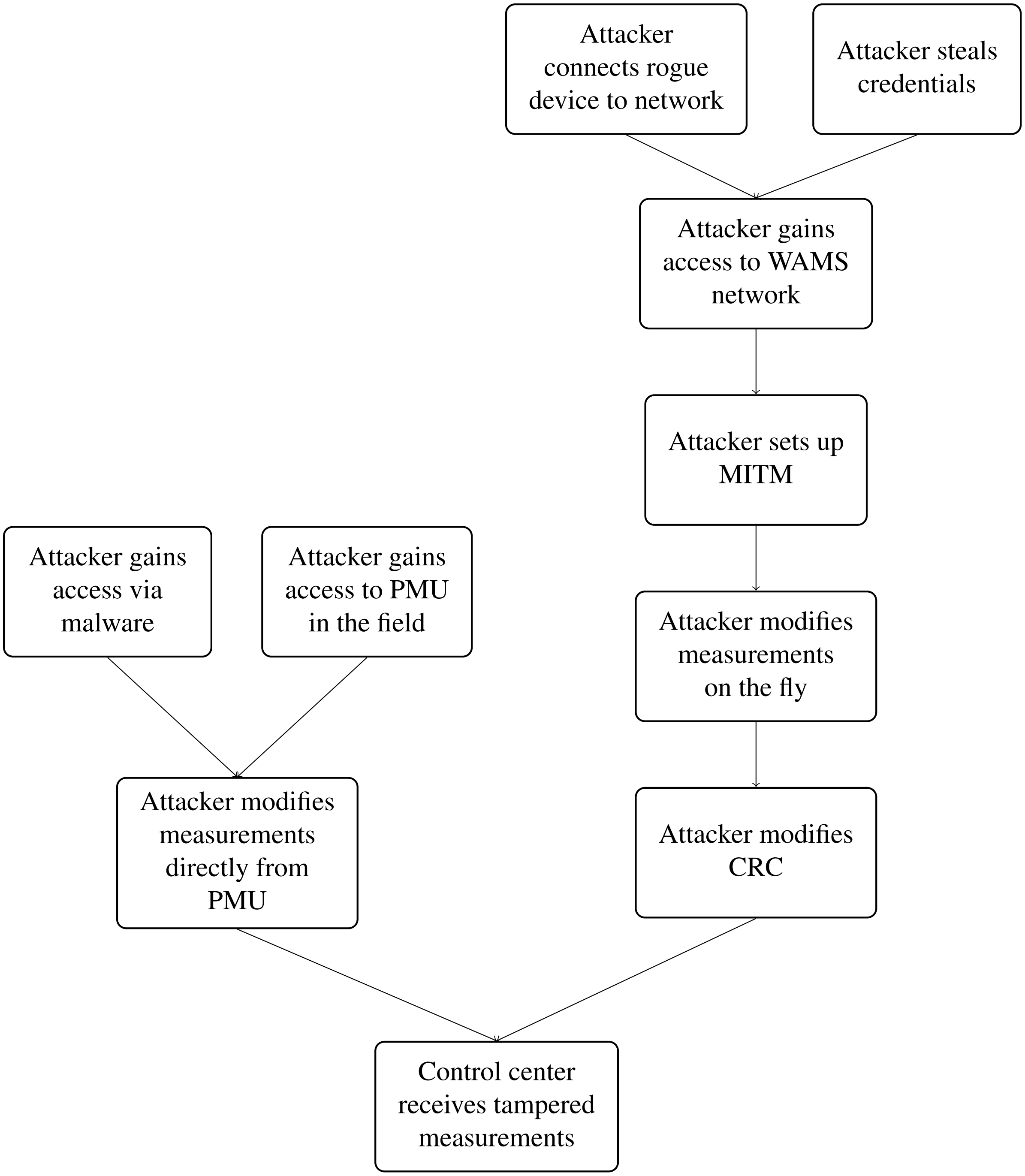

Attacker connects rogue device to network
Attacker steals credentials
Attacker gains access to WAMS network
Attacker sets up MITM
Attacker gains access via malware
Attacker gains access to PMU in the field
Attacker modifies measurements on the fly
Attacker modifies measurements directly from PMU
Attacker modifies CRC
Control center receives tampered measurements

Figure 13: FDI Attack Tree

where $\hat{\sigma}()$ is the activation function used, $\hat{W}$ is the weight matrix and c is the bias vector of the decoder. Parameters W, b, $\hat{W}$ and c are regulated during training in order to find a set that minimizes the reconstruction error such that

$$\phi, \psi = arg \min_{\phi,\psi} \mathcal{L}(x, \hat{x}) \tag{10}$$

where $\mathcal{L}(x, \hat{x})$ is the reconstruction error. The smaller the reconstruction error, the better the performance of the autoencoder network. To test if an instance is anomalous, we check if its reconstruction error is greater than a set threshold. If so, the instance is flagged as anomalous. Fig. 14 shows an overview of the architecture of an autoencoder.

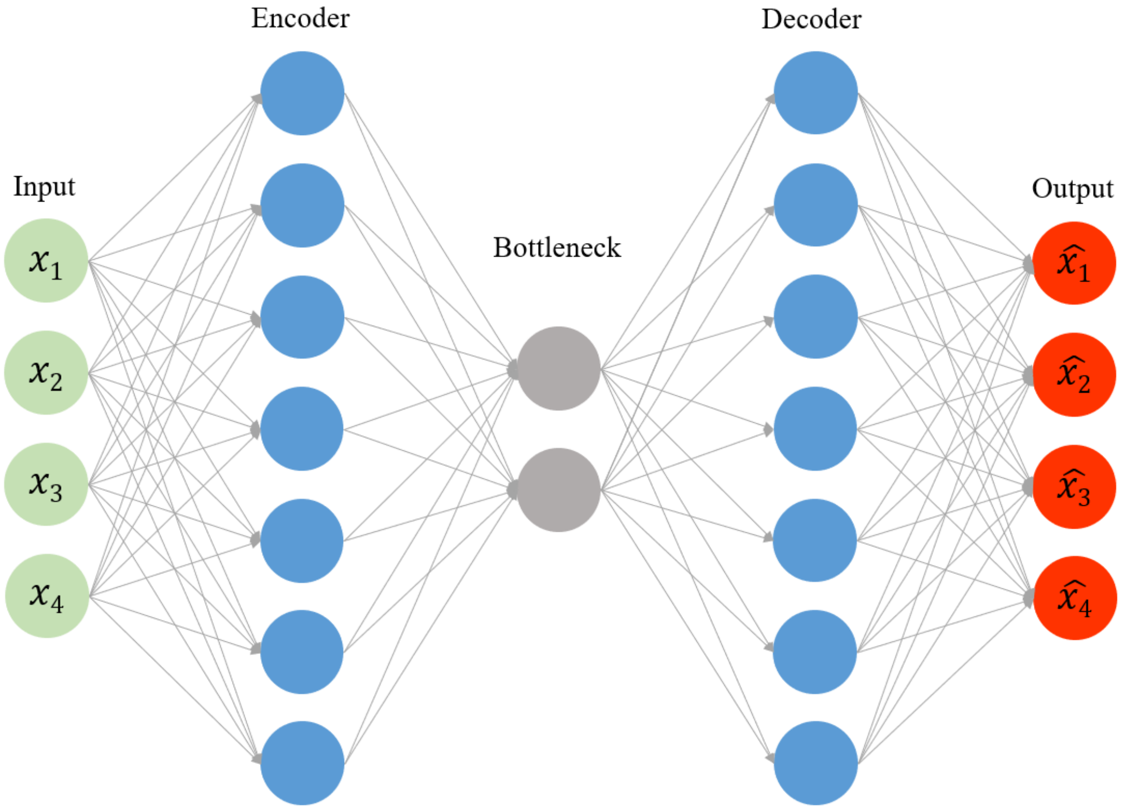


Figure 14: Deep Autoencoder

4.5 Windowed Deep Autoencoders

Windowed-Deep Autoencoders (w-DAE) are a variation of DAE neural networks that incorporate temporal information inherent in time-series data. w-DAE have a similar structure to DAE whereby they are comprised of 3 components: encoder, decoder, and the bottleneck layer that divides the network symmetrically with respect to the number of hidden layers and the number of neurons in each layers. However, they differ from traditional DAE in that they are not trained to reconstruct the input at their output layer. Rather, w-DAE takes a window of consecutive samples as input and attempts to reconstruct the last sample of the window in the output layer with the smallest reconstruction error possible. w-DAE employs a sliding-window that covers *n* samples, the encoder takes this input x_n and compresses it to get a representation of the time window y_n such that

$$y_n = \phi(x_n) = \sigma(Wx_n + b) \tag{11}$$

where $\sigma()$ is the activation function used, *W* is the weight matrix and *b* is the bias vector of the encoder.

The decoder takes the bottleneck layer and is trained to reconstruct the last sample of the sliding-window such that

$$\hat{x_i} = \psi(y_n) = \hat{\sigma}(\hat{W}y_n + c) \tag{12}$$

where $\hat{x_i}$ is the prediction of the last sample of the sliding window, $\hat{\sigma}()$ is the activation function used, $\hat{W}$ is the weight matrix and *c* is the bias vector of the decoder. Parameters *W*, *b*, $\hat{W}$ and *c* are regulated during training in order to find a set that minimizes the reconstruction error such that

$$\phi, \psi = arg\min_{\phi,\psi} \mathcal{L}(x_i, \hat{x_i}) \tag{13}$$

where $\mathcal{L}(x, \hat{x})$ is the reconstruction error. Similarly to DAE, an instance is considered an anomaly if its reconstruction error is higher than the set threshold. Fig. 15 shows an overview of the architecture of a windowed-autoencoder.

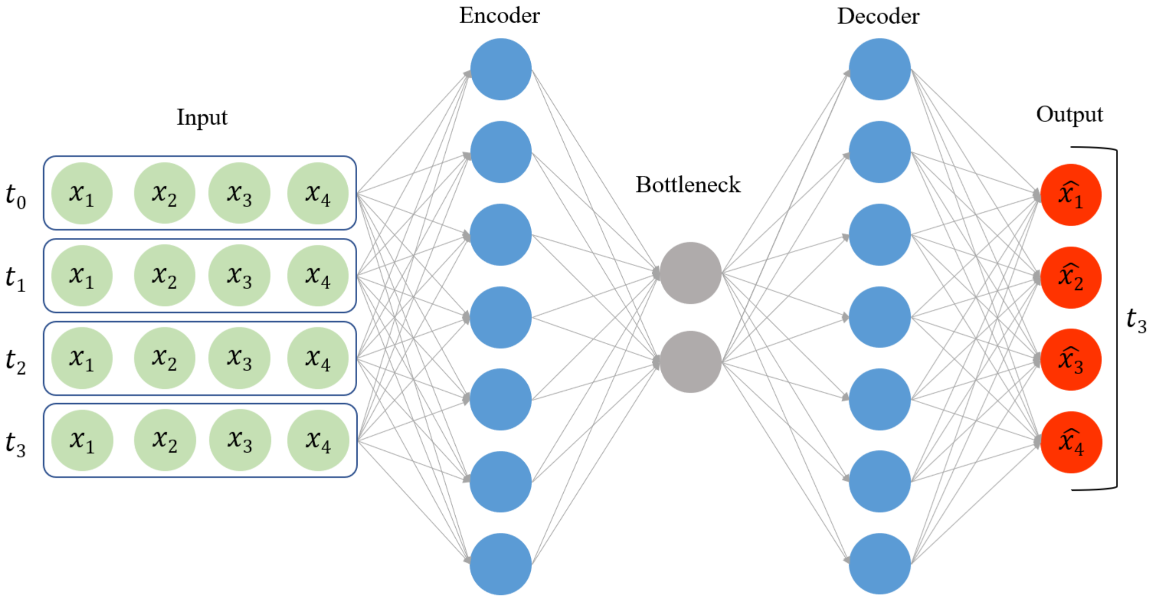


Figure 15: Windowed Deep Autoencoder

4.6 Long Short-Term Memory

RNNs [163] are a subdivision of neural networks that specialize in processing sequential data i.e. they base their prediction on a sequence of consecutive past events. They differ from traditional neural networks in that they handle time-series variables x_0, x_1 ... x_{t-1}, x_t. RNN predict the hidden states using the following formula:

$$h(t) = f(h(t-1), x(t)) \tag{14}$$

where *h* represents the state, *h(t-1)* represents the past states, and *x(t)* represents the input at time *t*. At each time step, RNNs take input $x(t)$ and compute a new state $h(t)$ by concatenating the previous state $h(t-1)$ with the input, applying a linear map to the concatenation, and passing the result through a logistic Sigmoid function.

However, RNNs face serious limitations when handling long-rage sequences because of the repeated application of Sigmoid functions that causes a large decay in the error signal over time [164]. This problem is termed as the vanishing gradient problem.

LSTM neural networks [165] are a subdivision of RNNs designed to overcome the shortcomings of traditional RNNs, most notably the vanishing gradient problem. LSTM has an additional memory cell c_t which is a linear combination of the previous state and the input. In addition, LSTMs have 3 multiplicative gates that regulate the proportion of the input that is passed to the memory cell i_t, and the proportion of the previous memory cell to ignore f_t. The memory cell value for input x_t is computed as:

$$i_t = \sigma(W_{ix}x_t + W_{ih}h_{t-1} + W_{ic}c_{t-1} + b_i) \tag{15}$$

$$f_t = \sigma(W_{fx}x_t + W_{fh}h_{t-1} + W_{fc}c_{t-1} + b_f) \tag{16}$$

$$c_t = f_t \otimes c_{t-1} + i_t \otimes tanh(W_{cx}x_t + W_{ch}h_{t-1} + b_c) \tag{17}$$

where σ is the component-wise logistic Sigmoid function, and $\otimes$ is the component-wise Hadamard product.

Finally, the current state h_t at each time step is governed by the third gate o_t that is calculated by:

$$o_t = \sigma(W_{ox}x_t + W_{oh}h_{t-1} + W_{oc}c_{t-1} + b_o) \tag{18}$$

$$h_t = o_t \otimes tanh(c_t) \tag{19}$$

Fig. 16 shows an LSTM cell adapted from [166].

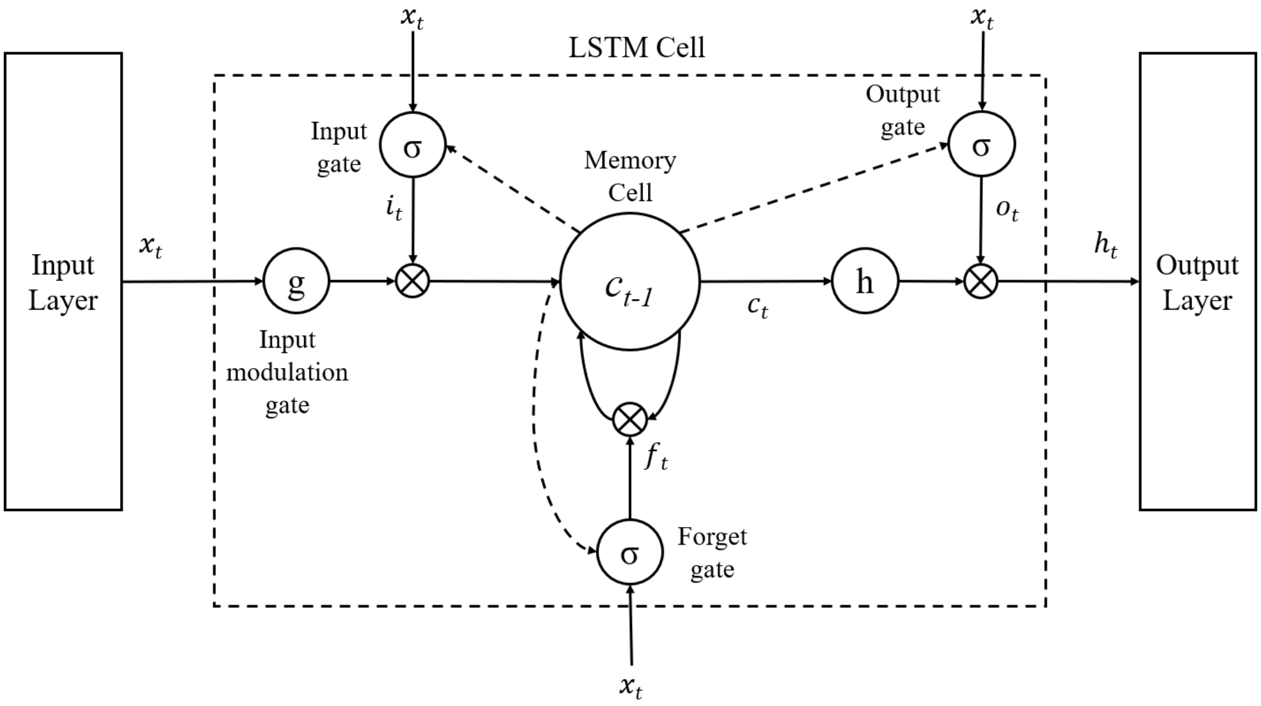


Figure 16: Structure of LSTM Cell

4.7 One-Class SVM

SVM is a supervised learning technique that separates the data instances by a hyperplane or a set of hyperplanes. The hyperplane is constructed in a way that provides the greatest margin of separation among the classes of the data. The margin is the sum of the shortest distances from the nearest data point of each class to the hyperplane. This design of the hyperplane, that underlines the differences between the categories, helps the model generalize better when classifying unseen data, thus doing so correctly. Equation 20 shows how the margin is calculated in order to construct the optimal hyperplane:

$$f(x) = \beta_0 + \sum_{i=1}^{n} \alpha_i(x, x_i) \tag{20}$$

where β_0 is the bias term, x is the new instance, x_i is an instance from the training set, and α_i with $i = 1, ...n$ are the set parameters.

In addition, SVM is effective in handling nonlinearly separable datasets because it maps the data points (which are represented by vectors), from the input space to a higher dimensional feature space where they become linearly separable. This is done by using a kernel function that takes two vectors from the input space and projects the resulting vector to the feature space. Some popular kernel functions are polynomial kernel, radial basis function kernel and sigmoid kernel [167].

OC-SVM is a version of SVM that is used for unsupervised learning. OC-SVM trains on one class label only and it aims to find a boundary that separates the instances of that one class from everything else. Thus it is considered an anomaly detection technique because it separates instances belonging to the only class it was trained on, from all other instances which will be considered abnormal with respect to the learned class. Fig. 17 shows a two dimensional example of anomaly detection using OC-SVM.

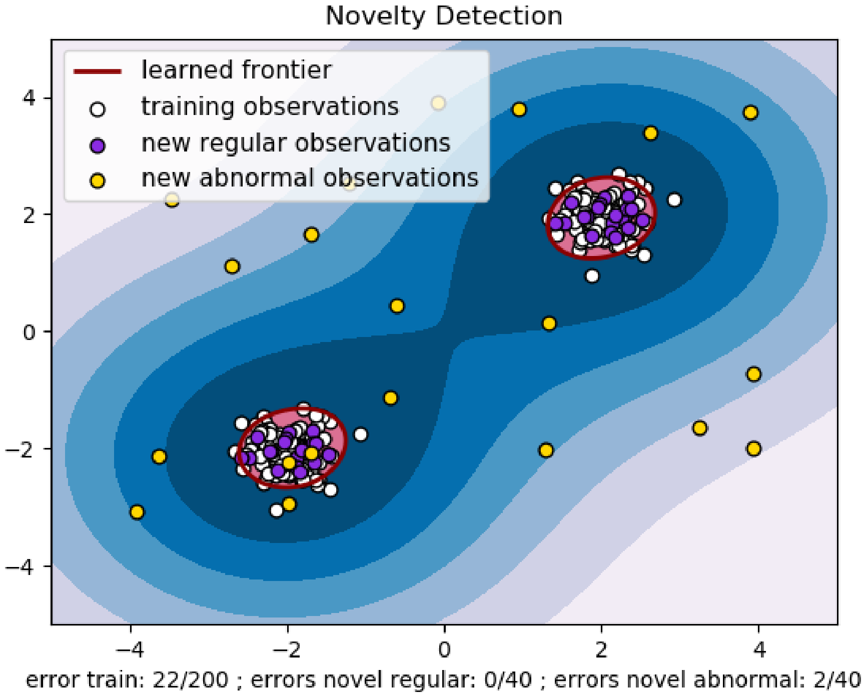


Figure 17: Two Dimensional Representation of OC-SVM [1]

Chapter 5

Experimental Results and Analysis

In this chapter, we explain the experimental setup used and we give details regarding the datasets collected from our testbed. Furthermore, we explain the evaluation metrics used to validate the anomaly detection methods and we present the results of the anomaly detection techniques tested on the 6 FDI scenarios we implemented. Finally, we end this chapter with an analysis of the experimental results.

5.1 Experimental Setup

We develop a HIL testbed to simulate the real-time behaviour of the power grid. We focus on having different hardware coming from actual vendors, and a real-time aspect to our experiments in order to have a simulation that is as close to real world smart grid operations as possible. We implement our power model in Hypersim [155], the physical measurements in the simulation are transported using the IEEE C37.118 protocol [19] over a network emulated using OpenStack [158], where they are ultimately captured and decoded using Wireshark [168] before further analysis.

We train our anomaly detection models on a dedicated server with Intel(R) Xeon(R) CPU E5-2630 v3 @ 2.40GHz, 300 GB RAM, and Nvidia Titan X GPU. The implementation of

WAMS applications, and the anomaly detection models is done using Python programming language [169]. In addition we use Elasticsearch [170] as a database for data analytics. Kibana [171] is used in addition to Elasticsearch for visualization on the dashboard.

5.1.1 Datasets

The training, validation, and testing datasets collected from the testbed have the same size for both the IEEE 9-bus system and the IEEE 39-bus system. The training dataset is made up of 35,000 normal samples and the validation set is made up of 24,000 samples. The testing dataset is imbalanced with 75% normal and 25% attack, because of the difficulty of collection of FDI attack instances in realistic setups. Furthermore, we take into consideration different attack capabilities by testing the performance of the techniques for different number of PMUs attacked ranging from just 1 attacked PMU to all possible compromised PMUs. As explained in Section 4.2, the features extracted include voltage, current, frequency and ROCOF measurements collected by the PMUs. These measurements are preprocessed and normalized to the range of [0, 1] to account to the different magnitudes and avoid misleading the training algorithms. Figures 18, 19, 20 and 21 show the raw voltage, current, frequency and ROCOF measurements respectively, collected from a PMU. From the figures we can see that the variability of the values of these features differs, for examples, the values of frequency are mainly constricted in the range of 60 as opposed to voltage where the values vary between 136,000 and 139,000 volts over time. Moreover, figures show that the relation between certain features is visible whereas other features don't show such characteristic. For example, we see that current increases when voltage decreases and vice versa, however we don't see such a relation between voltage and frequency. Similarly, Figures 22, 23, 24 and 25 show the corresponding normalized voltage, current, frequency and ROCOF measurements from the same PMU.

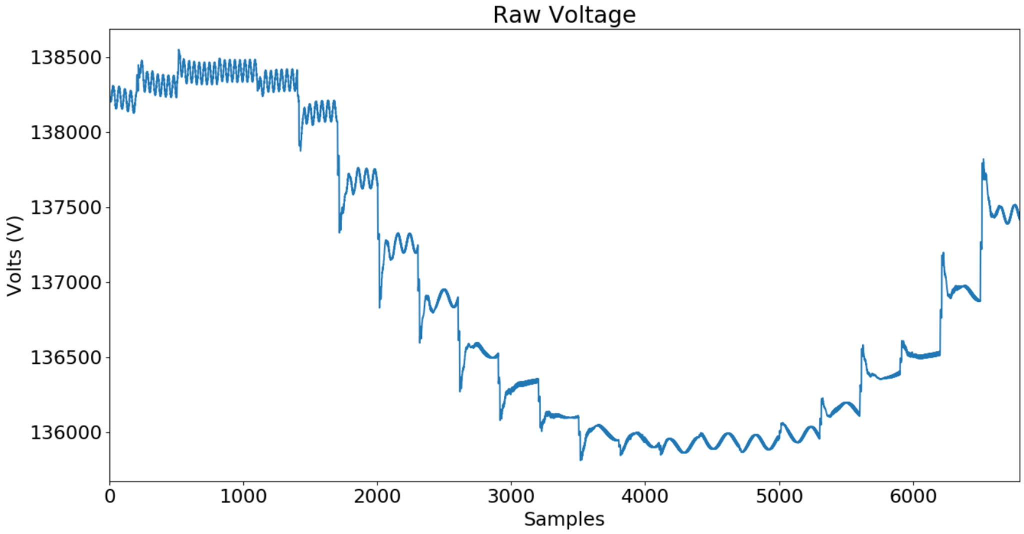


Figure 18: Raw Voltage Measurements

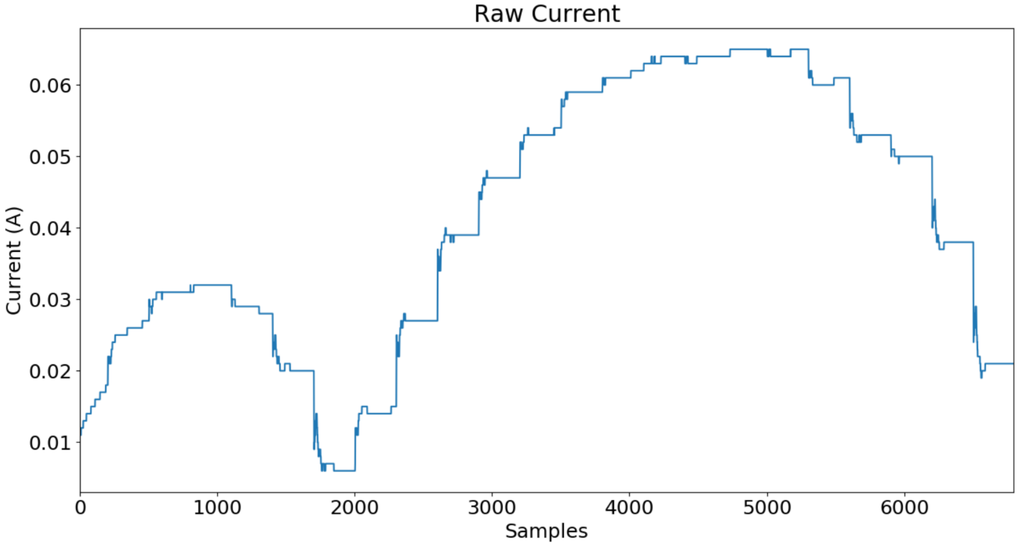


Figure 19: Raw Current Measurements

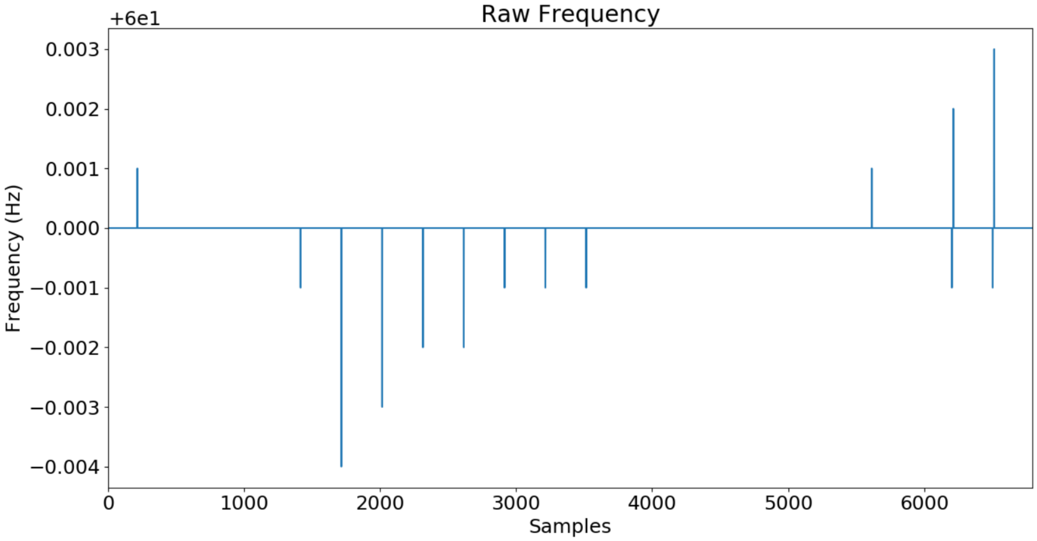


Figure 20: Raw Frequency Measurements

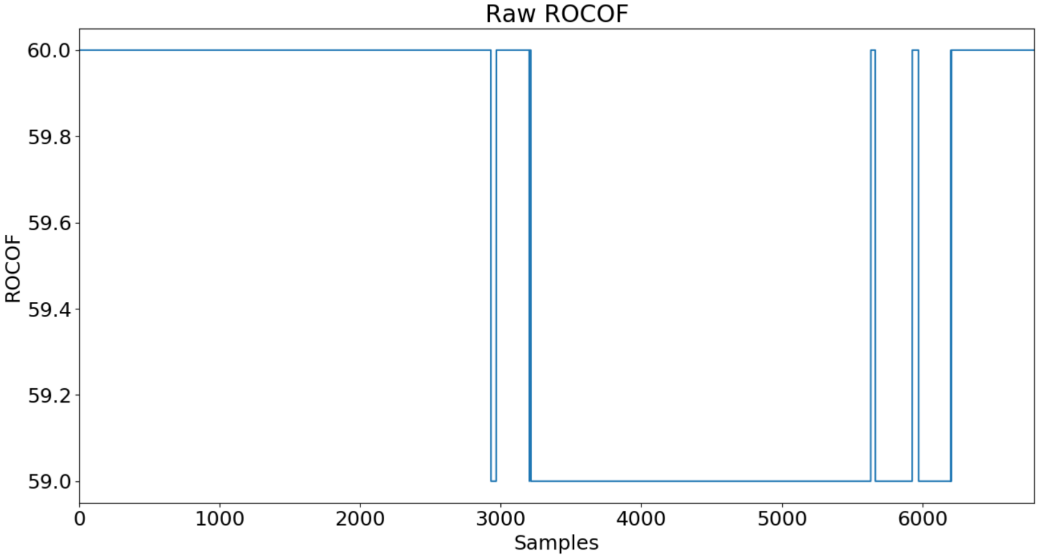


Figure 21: Raw ROCOF Measurements

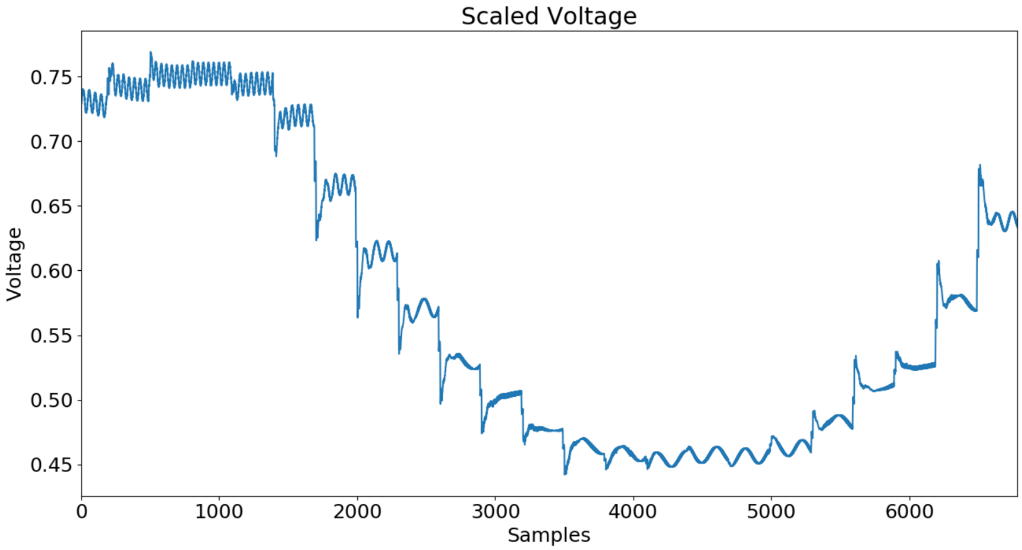


Figure 22: Scaled Voltage Measurements

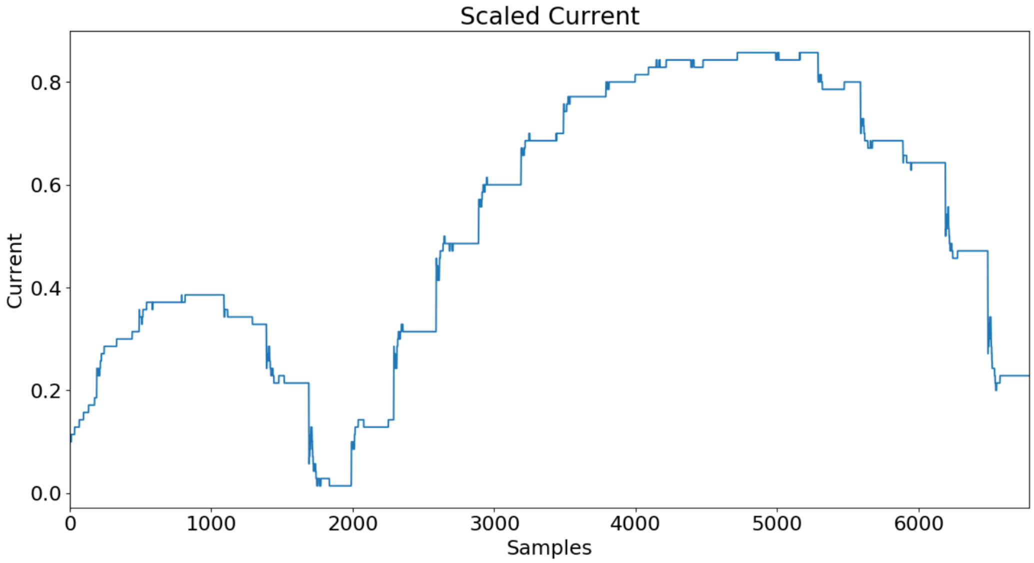


Figure 23: Scaled Current Measurements

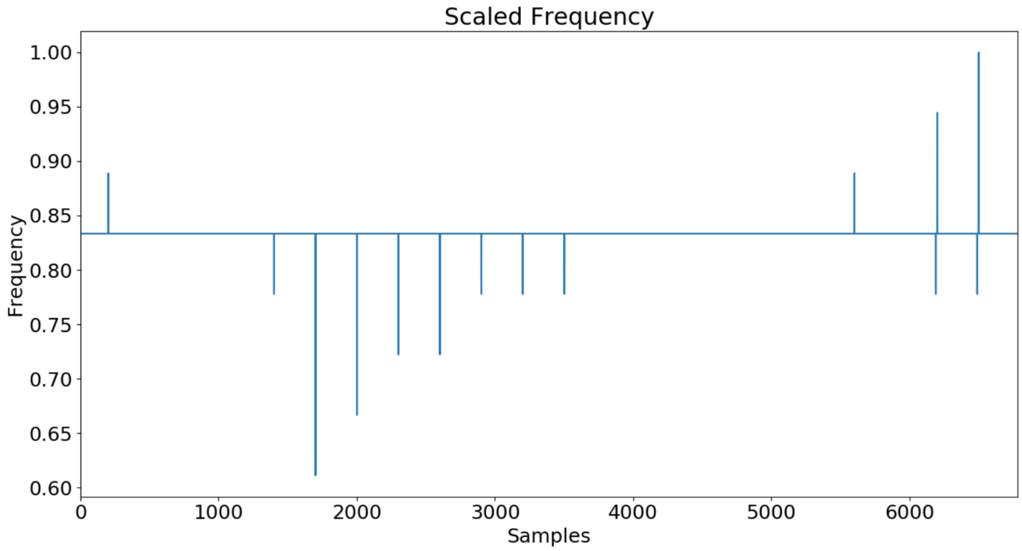


Figure 24: Scaled Frequency Measurements

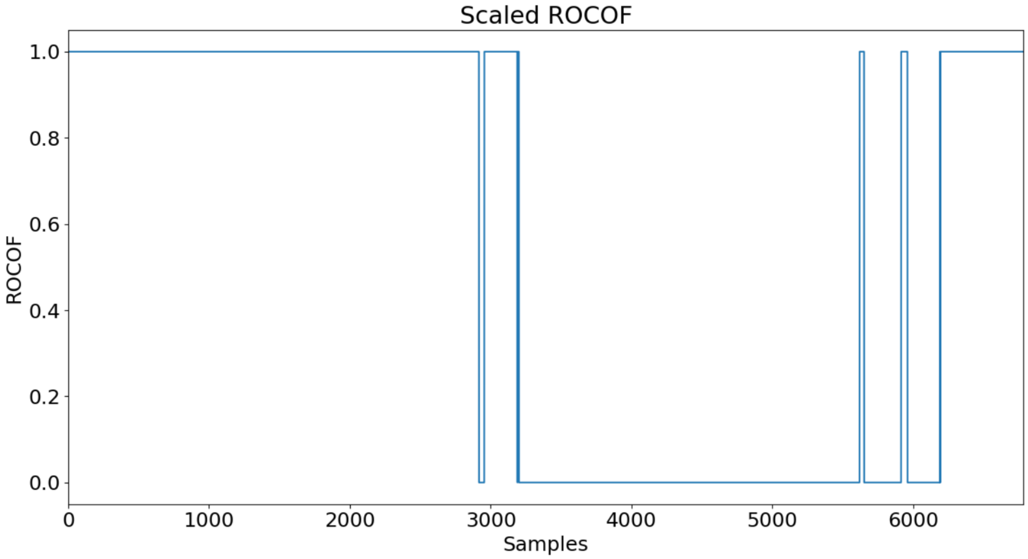


Figure 25: Scaled ROCOF Measurements

To further explore these relationships, we plot the correlation matrix of these features. Fig. 26 shows the correlation matrix of measurements collected from the same PMU. We see that there is a strong correlation between measurements coming from same PMU like voltage and current where the correlation measure reaches about -0.75. This shows a strong negative relationship between the 2 measurements, which means that these features vary inversely consistently. On the other hand, we notice a correlation measure close to 0 between voltage and frequency which asserts that these features don't exhibit a strong relationship.

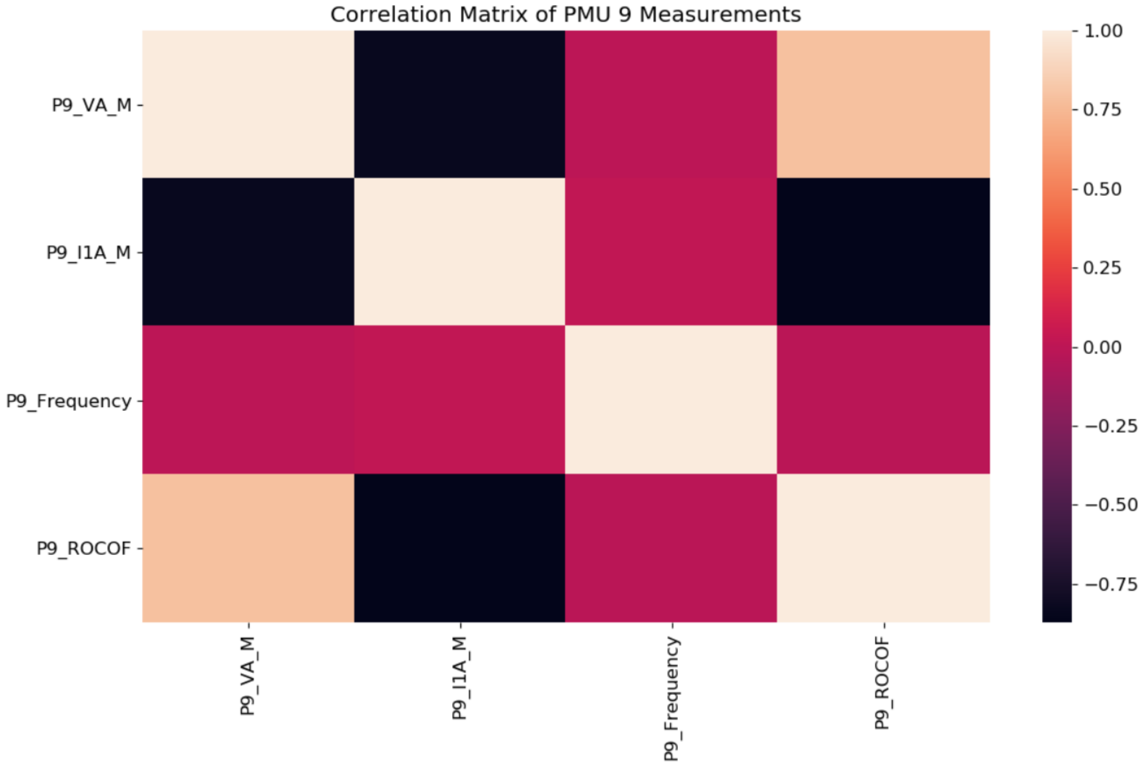


Figure 26: Correlation Matrix of PMU 9 Measurements

Furthermore, we investigate the correlation of measurements coming from different PMUs in the same system. Fig. 27 shows the correlation of measurements between 2 PMUs in the 9-bus system. We notice that there are also correlations between measurements coming from different PMUs. Voltage measurements coming from different PMUs show a strong positive correlation among themselves and voltage and current measurements exhibit a strong negative correlation. Furthermore we notice that there is a weak correlation between voltage and frequency coming from different PMUs.

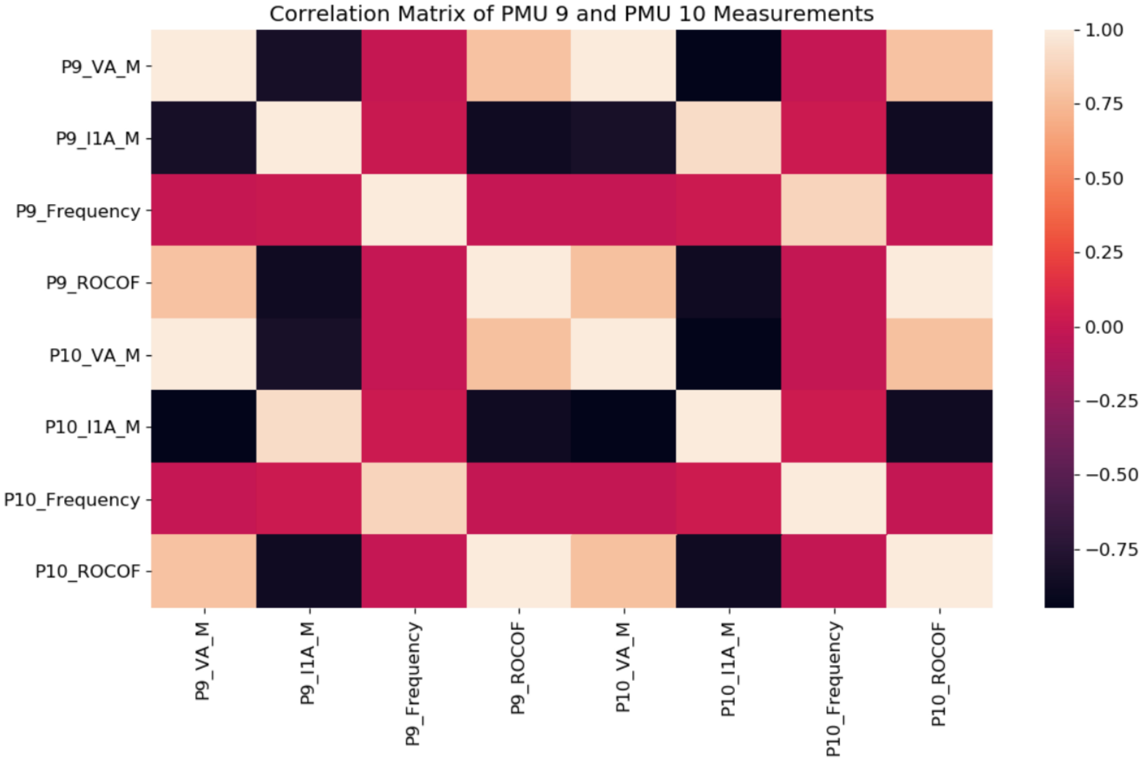


Figure 27: Correlation Matrix of PMU 9 and PMU 10 Measurements

5.2 Parameter Tuning

Hyperparameters play an important role when developing machine learning algorithms. They are the parameters that govern the training process of the algorithm. Usually, machine learning algorithms depend on multiple hyperparamteres that need to be tuned in order to achieve optimal results. In this work, we perform hyperparameter tuning on the tested techniques in order to find the set of hyperparamters that results in the best outcome.

Next, we will showcase the hyperparameter tuning process and present the set of hyperparamters chosen for each used method. We test the DAE with 1, 3, 5, 7, 9, 11, 13 and 15 hidden layers, and for different activation functions that include Tanh, Sigmoid, Relu, Elu, Softsign, Linear, and Selu functions. Finally, we pick the architecture-activation function combination that performs best on the validation set. The same process is followed for the other algorithms. First we train a DAE with one hidden layer with the different activation function. Fig. 28 shows the reconstruction error for the different activation functions. Fig. 29 shows the log of the error in order to get a clearer view of the results.

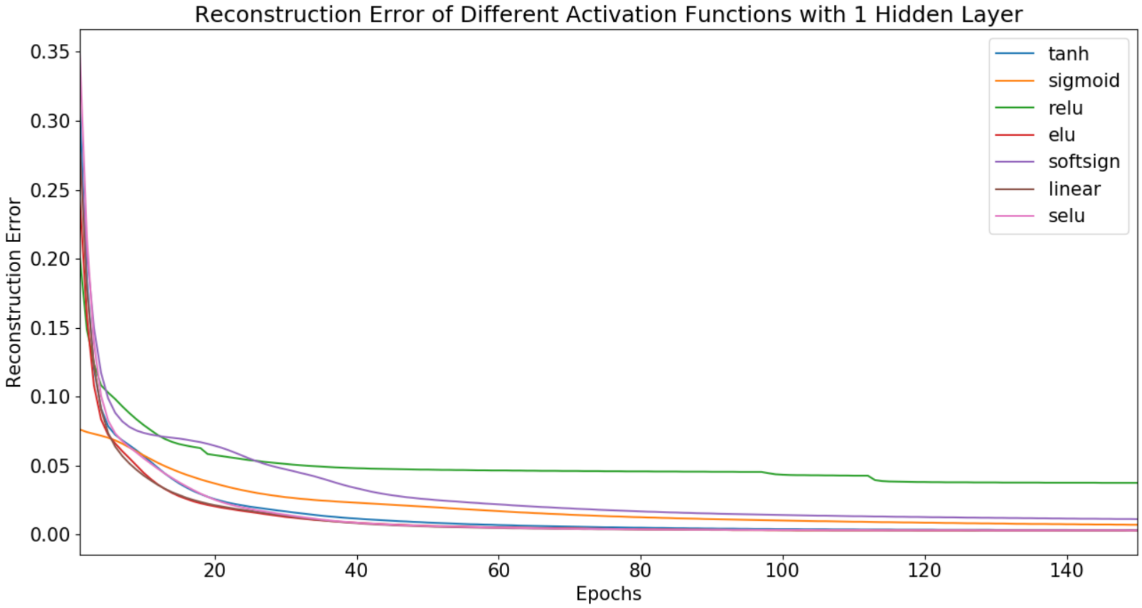


Figure 28: Reconstruction Error of Different Functions with 1 Hidden Layer

We then train a DAE with 5, 11, and 15 hidden layer with the different activation function. Figures 30, 31 and 32 shows the log of the reconstruction error for the different architectures respectively.

From the previous experiments Tanh, Selu, and Elu functions have consistently outperformed the rest of the other activation functions and have showed similar reconstruction errors. To choose between them we compare the run time for each activation function for different network architectures. Fig. 33 shows a comparison of the run-time of the 3

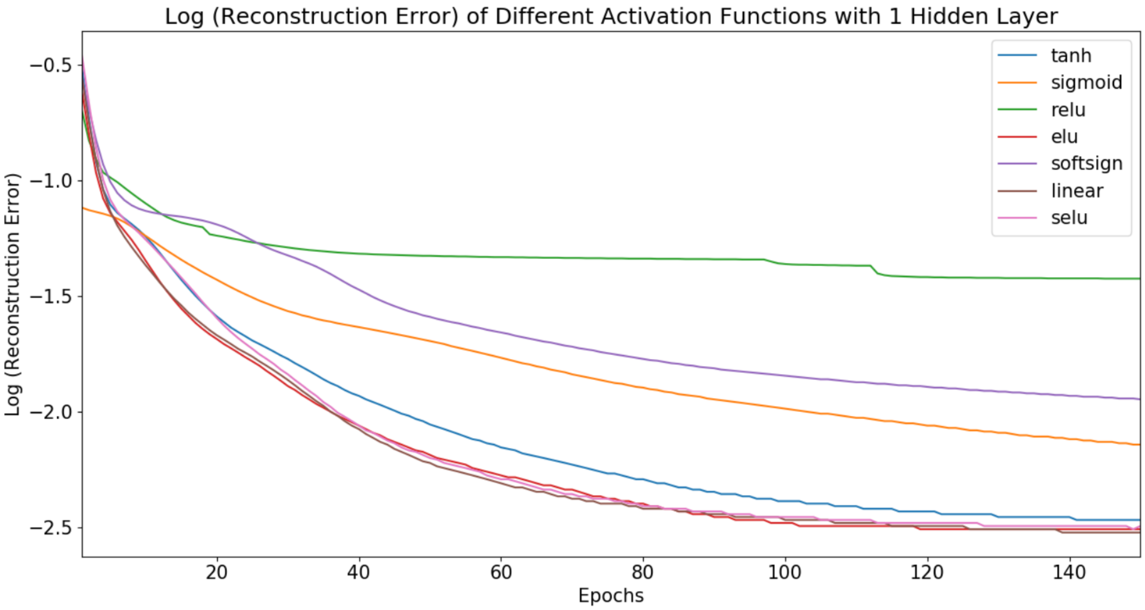


Figure 29: Log (Reconstruction Error) of Different Functions with 1 Hidden Layer

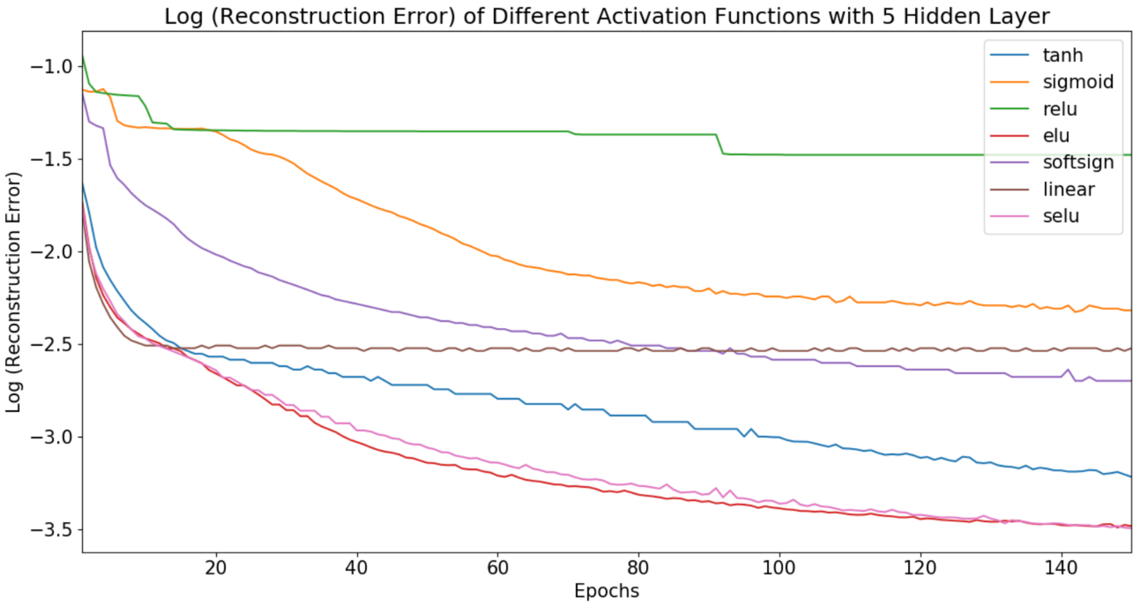


Figure 30: Log (Reconstruction Error) of Different Functions with 5 Hidden Layers

activation functions for different network architectures.

Based on the previous experiments we conclude that Tanh, Selu, and Elu activation functions have similar performance and that Tanh is faster than Selu and Elu across different network architectures

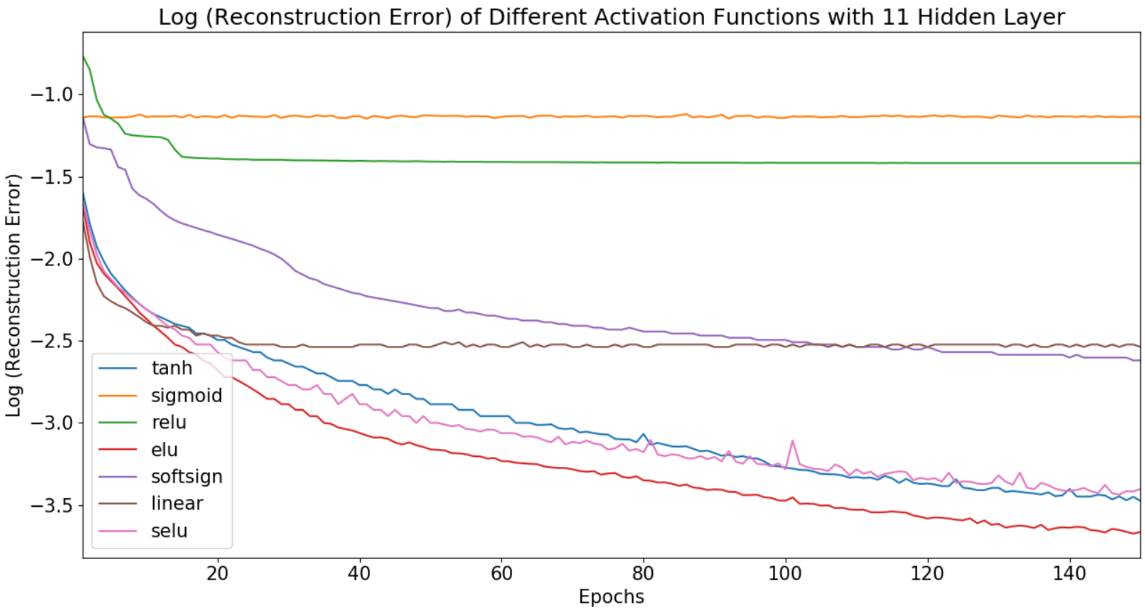


Figure 31: Log (Reconstruction Error) of Different Functions with 11 Hidden Layers

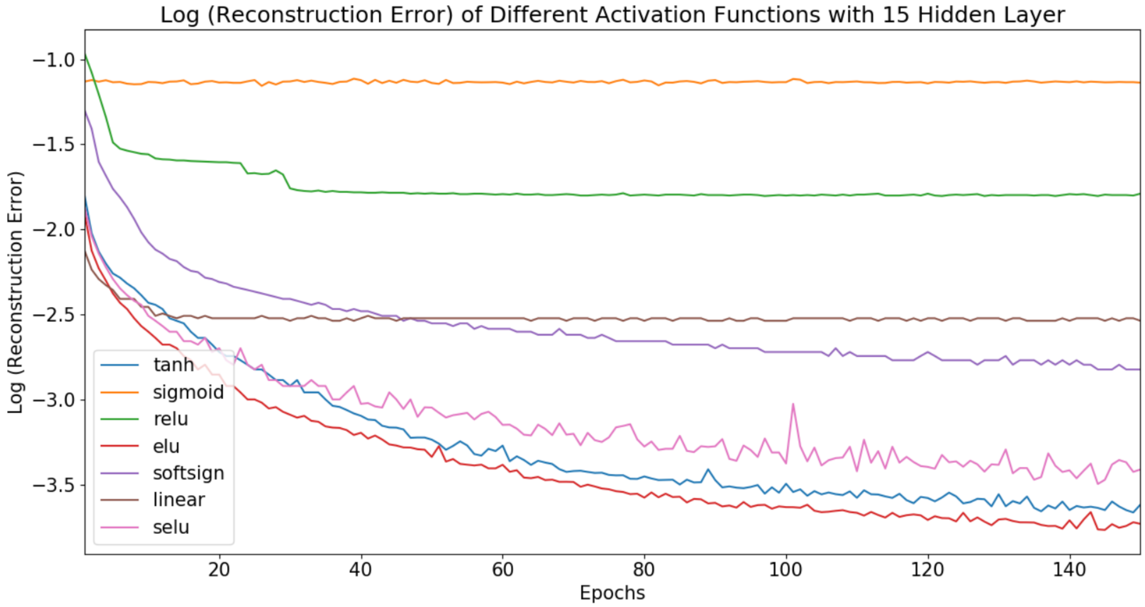


Figure 32: Log (Reconstruction Error) of Different Functions with 15 Hidden Layers

Next, we test the Tanh function with more network architectures. Fig. 34 shows the result of this experiment.

From Fig. 34 we see that the performance doesn't ameliorate by going from 11 to 13 or 15 hidden layers (~2.5e-04). To choose between them we compare the run time of Tanh

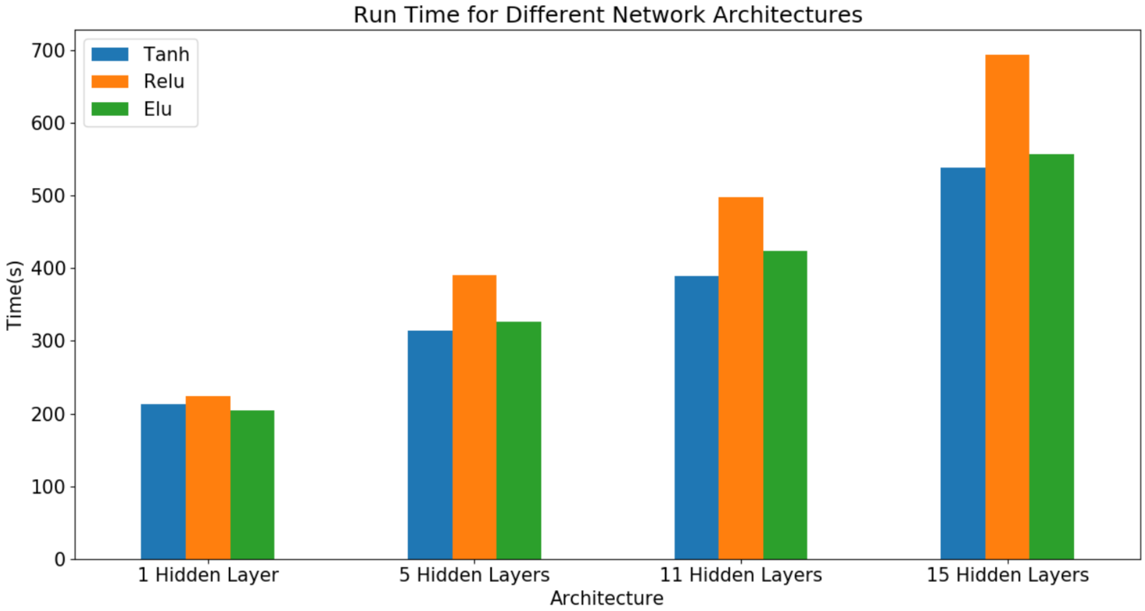


Figure 33: Run Time for Different Network Architectures

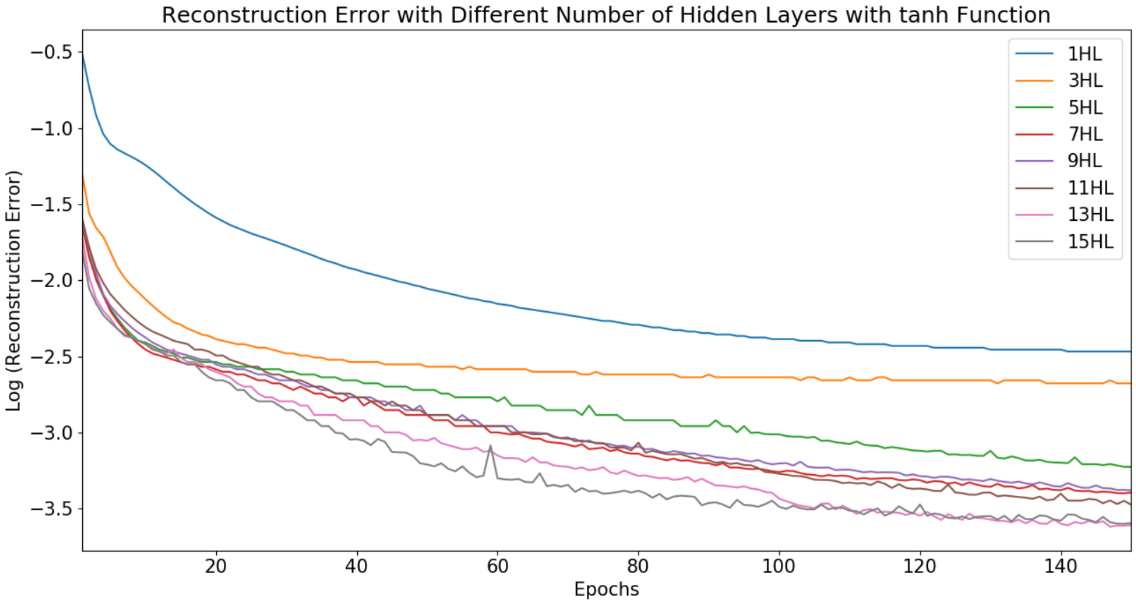


Figure 34: Reconstruction Error with Different Number of Hidden Layers

for 11, 13, and 15 hidden layers. Fig. 35 shows the result of this time comparison.

Finally, based on all the previous experiments, the best parameter combination for DAE is 11 hidden layers with Tanh activation function since it balances between performance and running time.

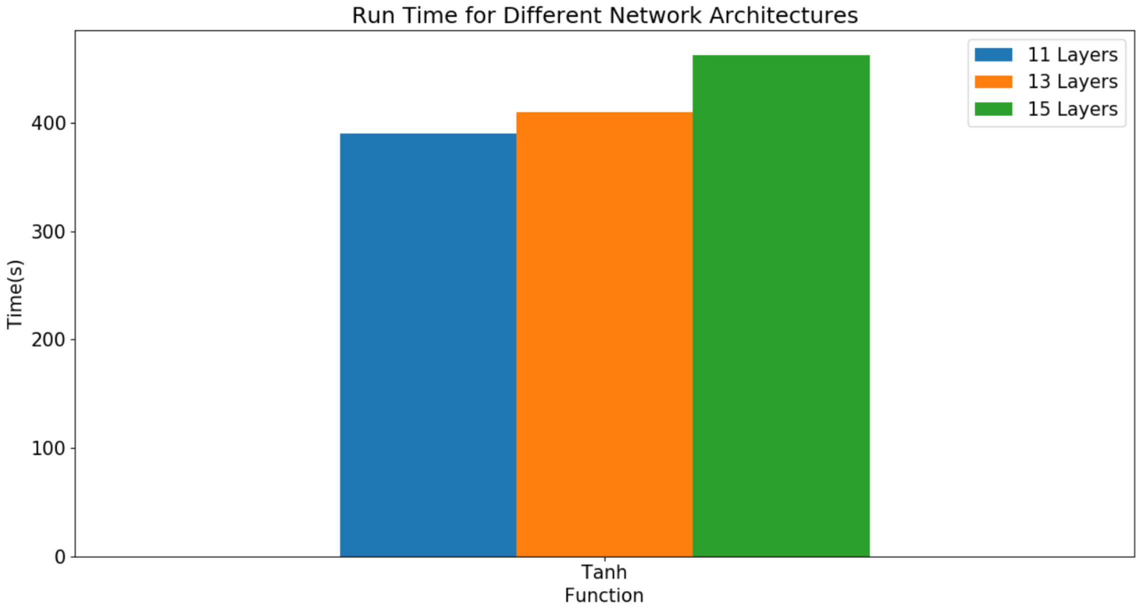


Figure 35: Run Time for Different Network Architectures

The same process is repeated for the other techniques to reach the optimal set of hyperparamaters. Table 6 shows the hyperparamaters of the implemented DAE, w-DAE and LSTM models. Table 7 shows the hyperparamaters of the implemented OC-SVM models

Table 6: Hyperparameters of DAE, w-DAE, and LSTM models

Model	Hidden Layers	Activation Function	Optimizer
9-bus DAE	11	Tanh	Adam
9-bus w-DAE	11	Tanh	Adam
39-bus DAE	11	Tanh	Adam
39-bus w-DAE	13	Tanh	Adam
9-bus LSTM	4	Tanh	Adam
39-bus LSTM	8	Tanh	Adam

Table 7: Hyperparameters of OC-SVM models

Model	Kernel	Gamma	Nu
9-bus OC-SVM	RBF	0.1	0.01
39-bus OC-SVM	RBF	0.1	0.01

5.2.1 Evaluation Metrics

To evaluate the performance of detection techniques, a confusion matrix is calculated. A confusion matrix is a table that summarizes the prediction results of a technique. Confusion matrices generally have two rows and two columns: the columns represent the actual class and the rows represent the predicted class. Furthermore, they portray the total number of errors made by the model, and it highlights the types of the made errors. Table 8 shows an example of a confusion matrix.

Table 8: Generic Confusion Matrix

	Class 0 Actual	**Class 1 Actual**
Class 0 Predicted	TN	FN
Class 1 Predicted	FP	TP

Four counts are calculated in a confusion matrix: True positive (TP), true negative (TN), false positive (FP) and false negative (FN):

- TP indicates when an instance is positive and it is predicted to be positive.
- TN indicates when an instance is negative and it is predicted to be negative.
- FP indicates when an instance is negative and it is predicted to be positive.
- FN indicates when an instance is positive and it is predicted to be negative.

Different evaluation metrics can be derived from a confusion matrix. In this research work, we evaluate the performance of our proposed techniques using 4 metrics: Accuracy, False Positive Rate, False Negative Rate, and F_1. These metrics defined next.

Accuracy

Accuracy is calculated by dividing the number of correct predictions over the total number of predictions as defined in Equation 21. Accuracy gives the same weight to both FPs and FNs which can mislead the interpretation of the result. This is especially important in cases of unbalanced datasets where one class occurs significantly more than the other because errors in the minority class might get overshadowed by the majority class.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{21}$$

False Positive Rate

FPR is calculated by dividing the number of false positives over all the negative cases in the dataset as defined in equation 22. In other words, *FPR* is the probability of false alerts being raised.

$$FPR = \frac{FP}{FP + TN} \tag{22}$$

False Negative Rate

FNR is calculated by dividing the number of false negatives over all the positive cases in the dataset as defined in equation 23. In other words, *FNR* is the probability of missing actual positive events.

$$FNR = \frac{FN}{FN + TP} \tag{23}$$

$\boldsymbol{F}_1$

F_1 is the weighted average of recall and precision. F_1 takes into account both FPs and FNs while giving them different weights as opposed to accuracy where both errors have the same weight. In order to calculate F_1, precision and recall should be calculated first. Precision is the number of TPs divided by all the predicted positive cases as defined in Equation 24. Precision shows how often the model is correct when predicting a positive class.

$$precision = \frac{TP}{TP + FP} \tag{24}$$

Recall is the number of TPs divided by all the actual positive cases as defined in Equation 25. Recall shows how many of the actual positive cases are predicted by the model.

$$recall = \frac{TP}{TP + FN} \tag{25}$$

Finally, F_1 is calculated using equation 26

$$F_1 = \frac{2 \cdot precision \cdot recall}{precision + recall} \tag{26}$$

5.3 Results

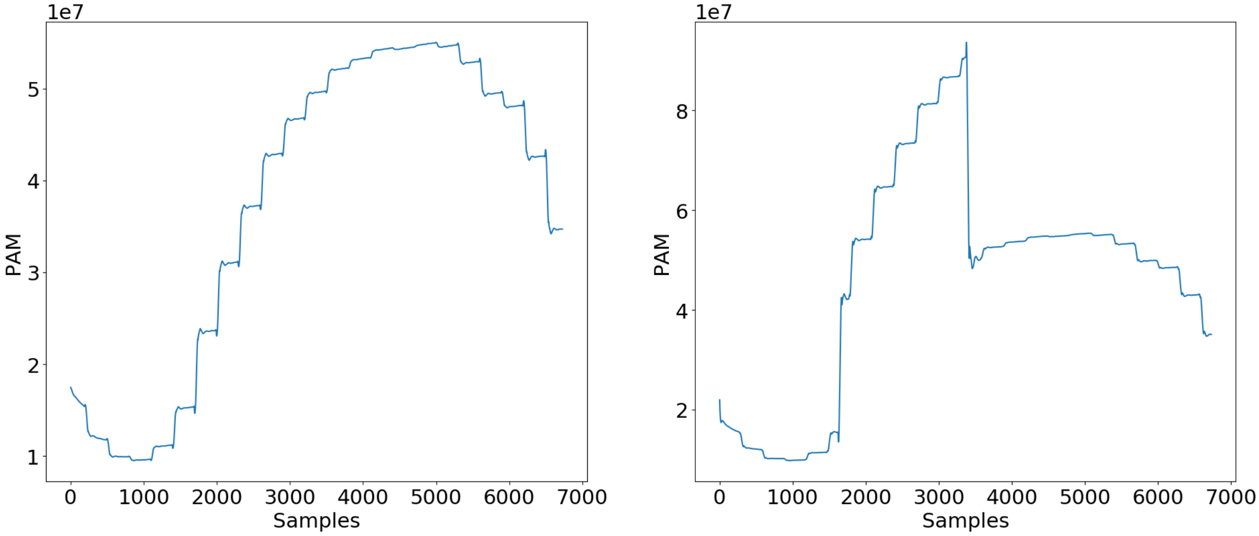
In this section, we will discuss each attack individually, we will show the WAMS application index under normal conditions and under FDI attack, and finally we will present the detection results for different number of compromised PMUs.

5.3.1 IEEE 9-bus System

In this section we discuss the attacks and detection results for all the tested models in the IEEE 9-bus system. In the tables we present all 4 metrics for the different number of compromised PMUs. Table 9 presents the results for the FDI attacks on the IEEE 9-bus applications, and Table 10 presents the results for the masking attacks in the IEEE 9-bus system. Next we detail attacks on each application with figures showing their impact and the detection results.

Attack on PAM

The stealthy FDI attack on the PAM application in the 9-bus system targets line 2. Fig. 36a shows the PAM index of line 2 under normal conditions and Fig. 36b shows the same index under FDI attack. The attacker modifies the measurements to gradually increase the perceived transferred power by 2 MW. Fig. 37 presents the performance, evaluated using the F_1 measure, of the studied anomaly detection algorithms in detecting this attack.



(a) Line 2 PAM Index Under Normal Conditions

(b) Line 2 PAM Index Under FDI Attack

Figure 36: PAM Experiment on Line 2 of IEEE 9-bus System

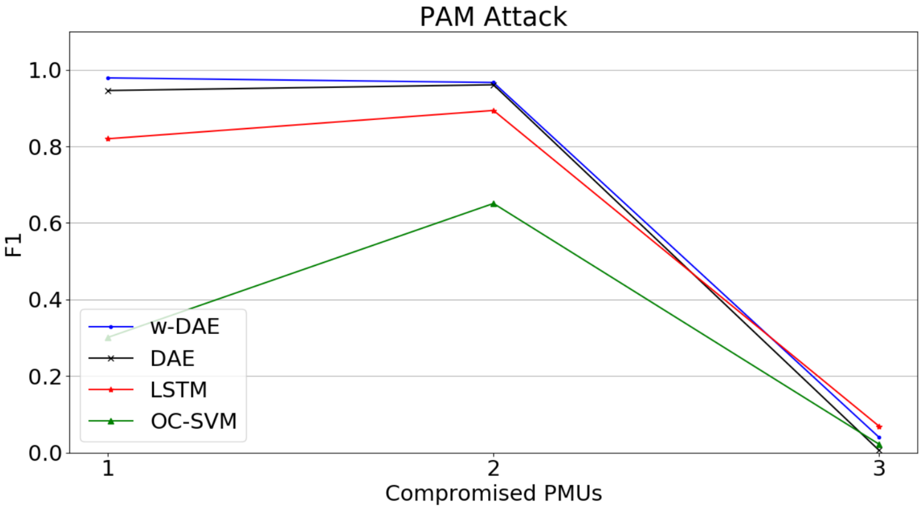
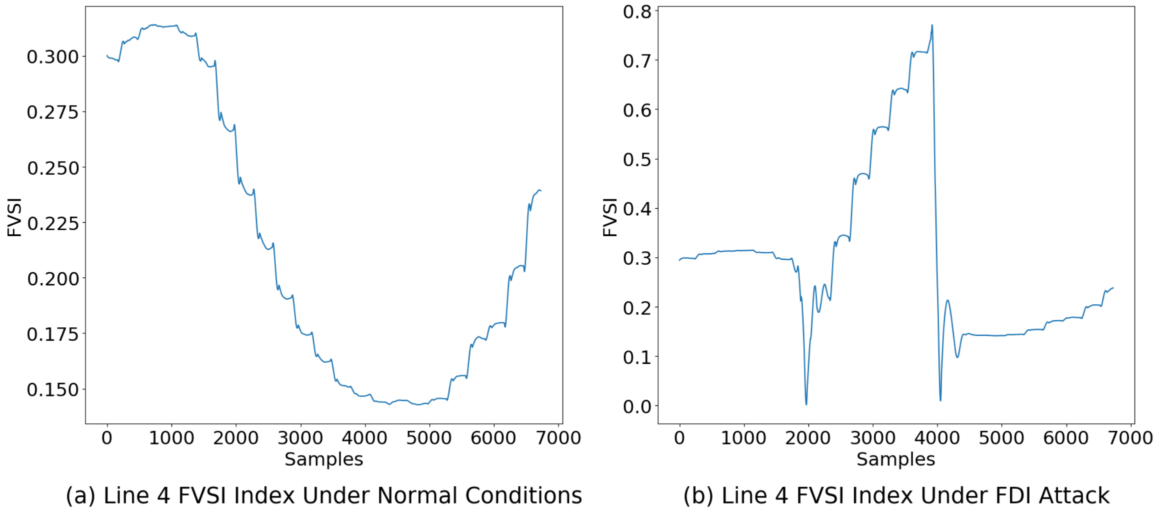


Figure 37: F_1 for Different Number of Compromised PMUs

Attack on FVSI

The stealthy FDI attack on the FVSI application in the 9-bus system targets line 4. Fig. 38a shows the FVSI index of line 4 under normal conditions and Fig. 38b shows the same index under FDI attack. The attacker modifies the measurements to gradually increase the perceived FVSI until it reaches a critical value (0.8). Fig. 39 presents the performance, evaluated using the F_1 measure, of the studied anomaly detection algorithms in detecting this attack.



(a) Line 4 FVSI Index Under Normal Conditions (b) Line 4 FVSI Index Under FDI Attack

Figure 38: FVSI Experiment on Line 4 of IEEE 9-bus System

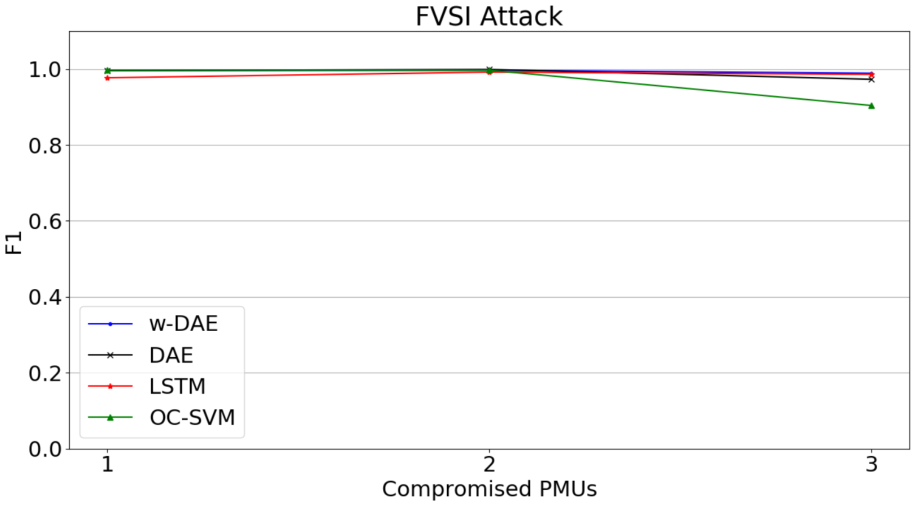


Figure 39: F_1 for Different Number of Compromised PMUs

Attack on ISI

The stealthy FDI attack on the ISI application in the 9-bus system targets bus 6. Fig. 40a shows the ISI index of bus 6 under normal conditions and Fig. 40b shows the same index under FDI attack. The attacker modifies the measurements to gradually decrease the perceived ISI until it reaches a critical value (0.2). Fig. 41 presents the performance, evaluated using the F_1 measure, of the studied anomaly detection algorithms in detecting this attack.

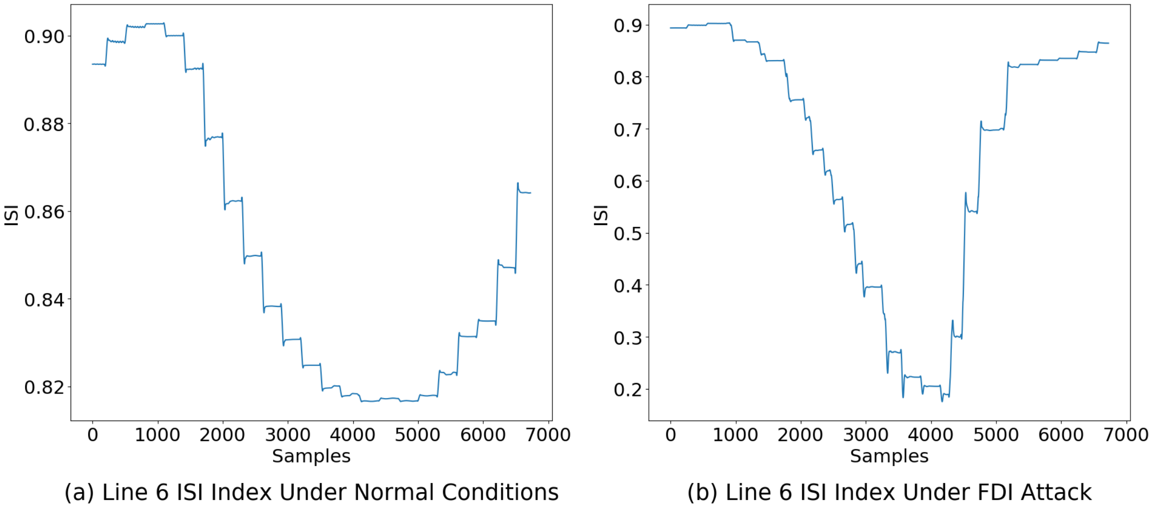


Figure 40: ISI Experiment on Bus 6 of IEEE 9-bus System

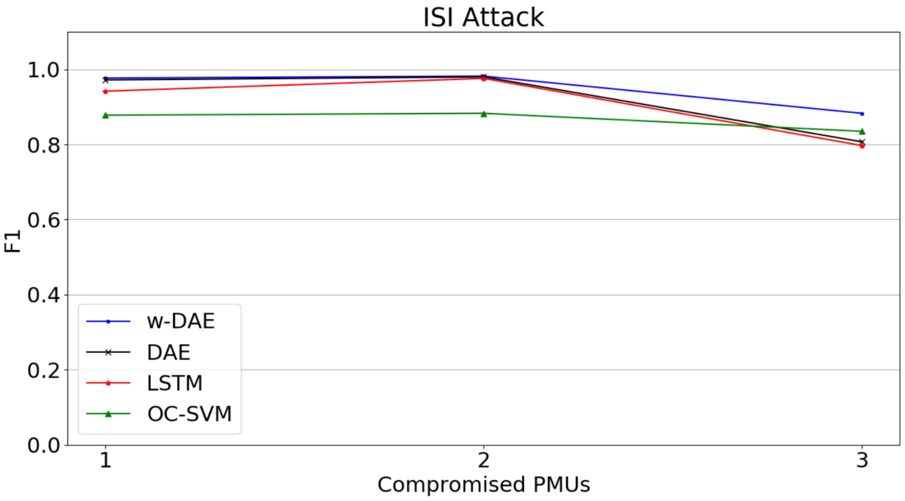


Figure 41: F_1 for Different Number of Compromised PMUs

Masking Attack on PAM

In the masking FDI attack against PAM in the 9-bus system, the attacker hides an instability on line 2 where the transferred power increases by 2 MW. When the attacker notices this instability in the system, he starts modifying the reported measurements to display normal operation, thus hiding the instability from the controller. This attack is the opposite of the previous attack on the PAM application. Fig. 42 presents the F_1 performance of the studied anomaly detection algorithms in detecting this attack.

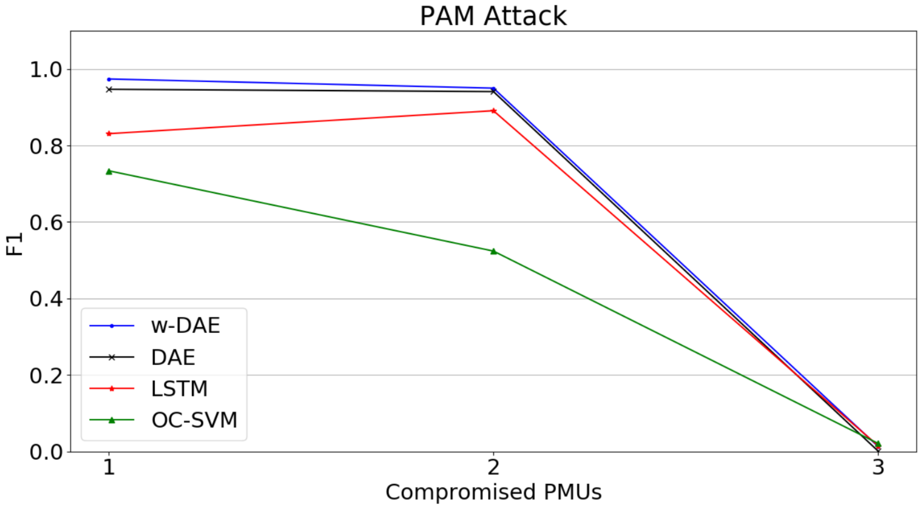


Figure 42: F_1 for Different Number of Compromised PMUs

Masking attack on FVSI

In the masking FDI attack against FVSI in the 9-bus system, the attacker hides an instability on line 4 where the index increase to 0.8. When the attacker notices this instability in the system, he starts gradually modifying the reported measurements to display normal operation, thus hiding the instability from the controller. This attack is the opposite of the previous attack on the FVSI application. Fig. 43 presents the performance, evaluated using the F_1 measure, of the studied anomaly detection algorithms in detecting this attack.

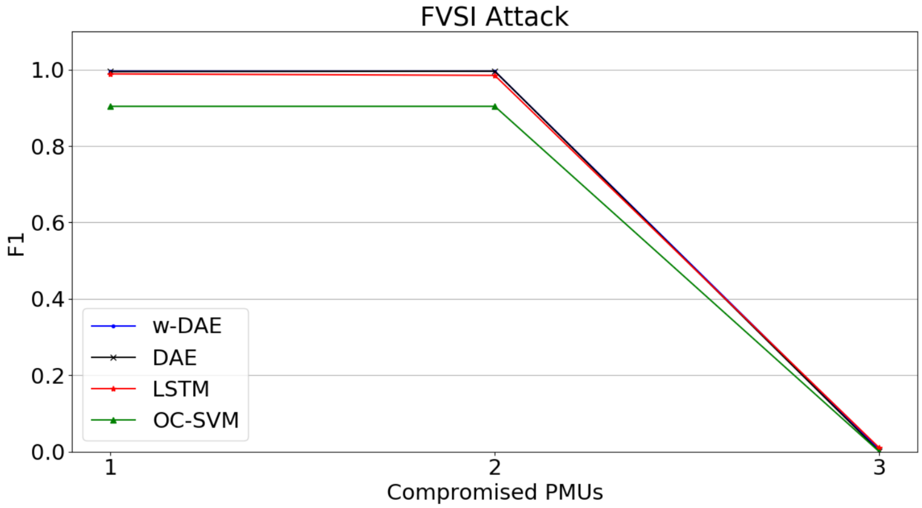


Figure 43: F_1 for Different Number of Compromised PMUs

Masking attack on ISI

In the masking FDI attack against ISI in the 9-bus system, the attacker hides an instability on bus 6 where the index decreases to 0.2. When the attacker notices this instability in the system, he starts gradually modifying the reported measurements to display normal operation, thus hiding the instability from the controller. This attack is the opposite of the previous attack on the ISI application. Fig. 44 presents the performance, evaluated using the F_1 measure, of the studied anomaly detection algorithms in detecting this attack.

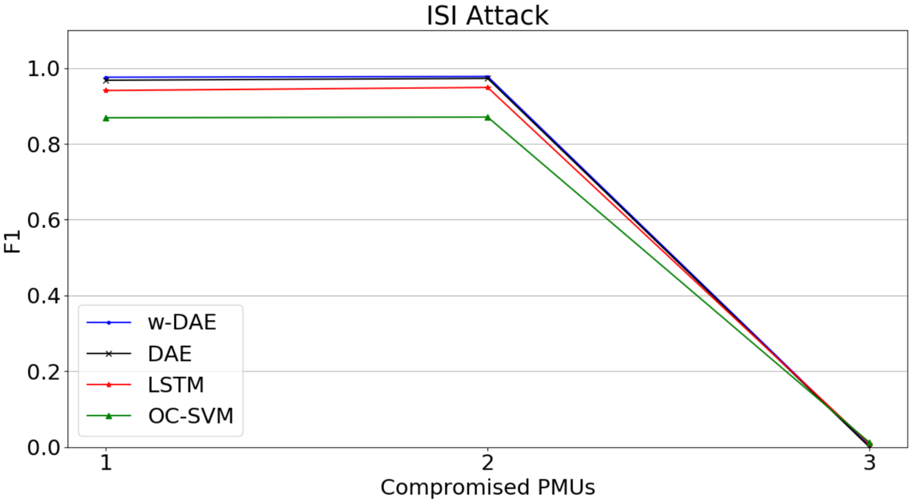


Figure 44: F_1 for Different Number of Compromised PMUs

Table 9: Detection Results for FDI Against Applications in the IEEE 9-bus System.

		PAM				FVSI				ISI			
Metrics	**# of Compromised PMUs**	**w-DAE**	**DAE**	**LSTM**	**OC-SVM**	**w-DAE**	**DAE**	**LSTM**	**OC-SVM**	**w-DAE**	**DAE**	**LSTM**	**OC-SVM**
Accuracy	1	0.986	0.973	0.922	0.886	0.997	0.997	0.992	0.922	0.971	0.961	0.929	0.848
	2	0.975	0.97	0.947	0.824	0.997	0.997	0.989	0.922	0.973	0.966	0.938	0.849
	3	0.732	0.734	0.734	0.731	0.632	0.634	0.634	0.557	0.362	0.365	0.364	0.346
F_1	1	0.974	0.947	0.831	0.734	0.996	0.995	0.989	0.904	0.976	0.968	0.941	0.869
	2	0.95	0.941	0.891	0.524	0.996	0.996	0.985	0.904	0.978	0.973	0.949	0.8708
	3	0.013	0.001	0.015	0.021	0.006	0.001	0.01	0	0.003	0	0.008	0.0121
FPR	1	0.001	0.0006	0.004	0.0086	0.0002	0.0002	0.0037	0.1197	0.0004	0.0004	0.0082	0.0614
	2	0.001	0.0006	0.0042	0.0086	0.0002	0.0002	0.0037	0.1197	0.0004	0.0004	0.0082	0.0614
	3	0.001	0.0006	0.0016	0.0086	0.0002	0.0002	0.0009	0.1197	0.0004	0.0004	0.0049	0.0614
FNR	1	0.0477	0.0995	0.2808	0.4063	0.0084	0.0088	0.0161	0.00321	0.0457	0.0611	0.107	0.2032
	2	0.0922	0.1106	0.1874	0.6368	0.0068	0.0072	0.0225	0.00321	0.0427	0.0529	0.0929	0.20143
	3	0.9934	0.9994	0.9923	0.9889	0.9972	0.9996	0.9952	1	0.9984	0.9998	0.9958	0.9936

Table 10: Detection Results for Masking FDI Attacks in the IEEE 9-bus System.

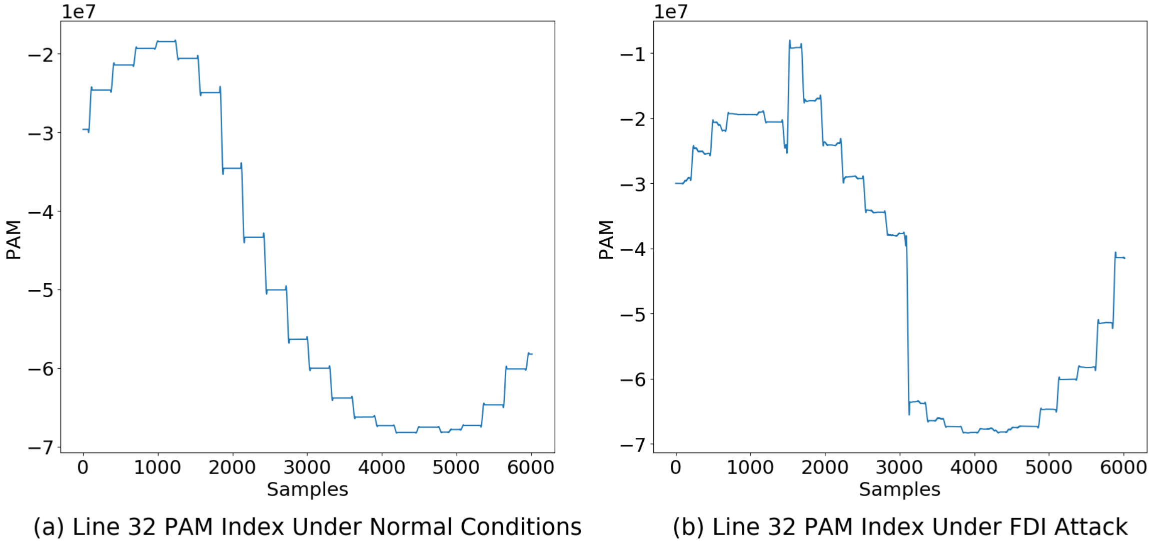
		PAM				FVSI				ISI			
Metrics	**# of Compromised PMUs**	**w-DAE**	**DAE**	**LSTM**	**OC-SVM**	**w-DAE**	**DAE**	**LSTM**	**OC-SVM**	**w-DAE**	**DAE**	**LSTM**	**OC-SVM**
Accuracy	1	0.986	0.973	0.922	0.886	0.997	0.997	0.992	0.922	0.971	0.961	0.929	0.848
	2	0.975	0.97	0.947	0.824	0.997	0.997	0.989	0.922	0.973	0.966	0.938	0.849
	3	0.732	0.734	0.734	0.731	0.632	0.634	0.634	0.557	0.362	0.365	0.364	0.346
F_1	1	0.974	0.947	0.831	0.734	0.996	0.995	0.989	0.904	0.976	0.968	0.941	0.869
	2	0.95	0.941	0.891	0.524	0.996	0.996	0.985	0.904	0.978	0.973	0.949	0.8708
	3	0.013	0.001	0.015	0.021	0.006	0.001	0.01	0	0.003	0	0.008	0.0121
FPR	1	0.001	0.0006	0.004	0.0086	0.0002	0.0002	0.0037	0.1197	0.0004	0.0004	0.0082	0.0614
	2	0.001	0.0006	0.0042	0.0086	0.0002	0.0002	0.0037	0.1197	0.0004	0.0004	0.0082	0.0614
	3	0.001	0.0006	0.0016	0.0086	0.0002	0.0002	0.0009	0.1197	0.0004	0.0004	0.0049	0.0614
FNR	1	0.0477	0.0995	0.2808	0.4063	0.0084	0.0088	0.0161	0.00321	0.0457	0.0611	0.107	0.203
	2	0.0922	0.1106	0.1874	0.6368	0.0068	0.0072	0.0225	0.00321	0.0427	0.0529	0.0929	0.2014
	3	0.9934	0.9994	0.9923	0.9889	0.9972	0.9996	0.9952	1	0.9984	0.9998	0.9958	0.9936

5.3.2 IEEE 39-bus System

In this section we discuss the attacks and detection results for all the tested models in the IEEE 39-bus system. In the tables we present all 4 metrics for the different number of compromised PMUs. Table 11 presents the results for the FDI attacks on the IEEE 39-bus applications, and Table 12 presents the results for the masking attacks in the IEEE 39-bus system. Next we detail attacks on each application with figures showing their impact and the detection results.

Attack on PAM

The stealthy FDI attack on the PAM application in the 39-bus system targets line 32. Fig. 45a shows the PAM index of line 32 under normal conditions and Fig. 45b shows the same index under FDI attack. The attacker modifies the measurements to gradually increase the perceived transferred power by 1 MW. Fig. 46 presents the performance, evaluated using the F_1 measure, of the studied anomaly detection algorithms in detecting this attack.



(a) Line 32 PAM Index Under Normal Conditions

(b) Line 32 PAM Index Under FDI Attack

Figure 45: PAM Experiment on Line 32 of IEEE 39-bus System

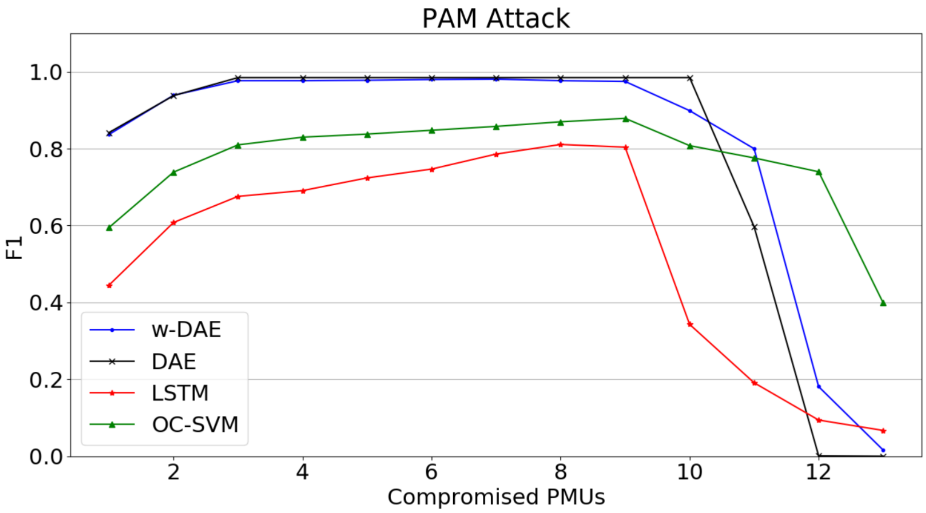
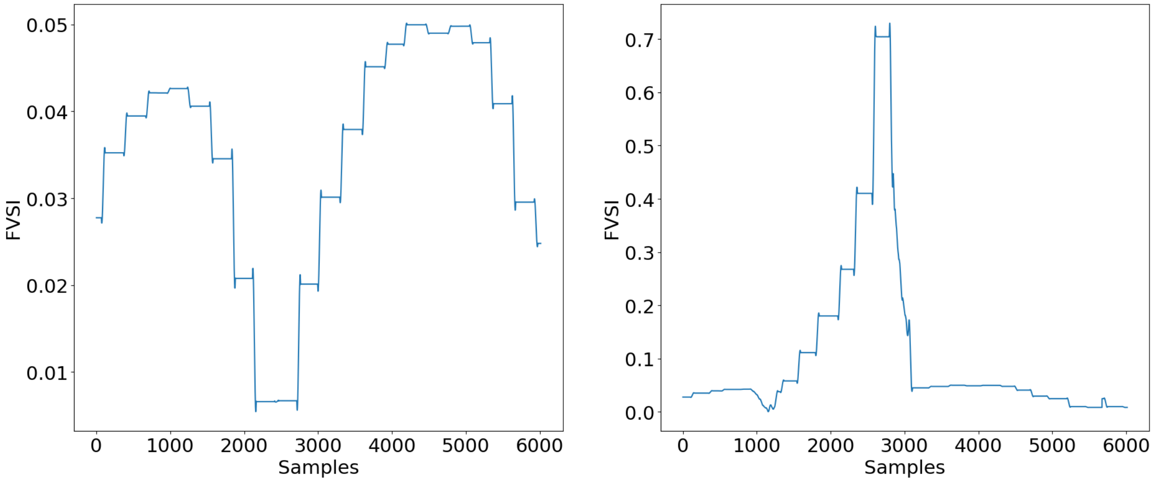


Figure 46: F_1 for Different Number of Compromised PMUs

Attack on FVSI

The stealthy FDI attack on the FVSI application in the 39-bus system targets line 27. Fig. 47a shows the FVSI index of line 27 under normal conditions and Fig. 47b shows the same index under FDI attack. The attacker modifies the measurements to gradually increase the perceived FVSI until it reaches a critical value (0.7). Fig. 48 presents the performance, evaluated using the F_1 measure, of the studied anomaly detection algorithms in detecting this attack.



(a) Line 27 FVSI Index Under Normal Conditions (b) Line 27 FVSI Index Under FDI Attack

Figure 47: FVSI Experiment on Line 27 of IEEE 39-bus System

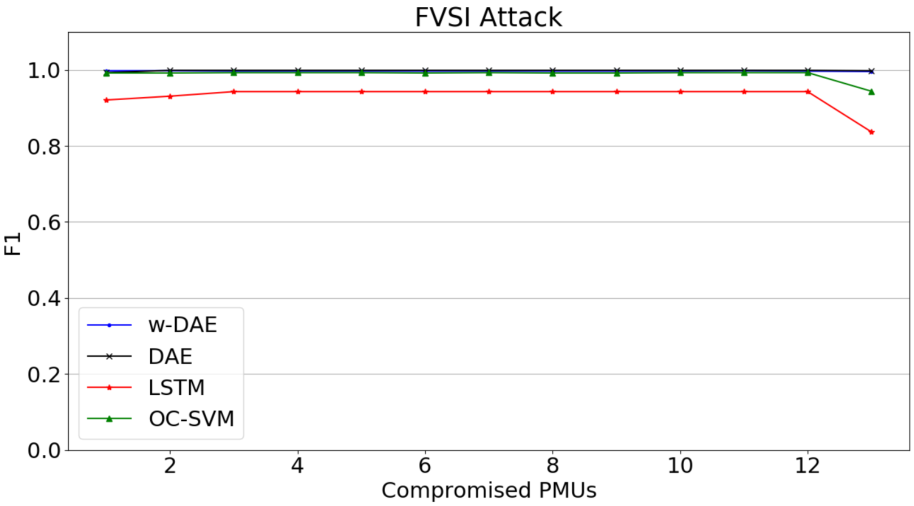
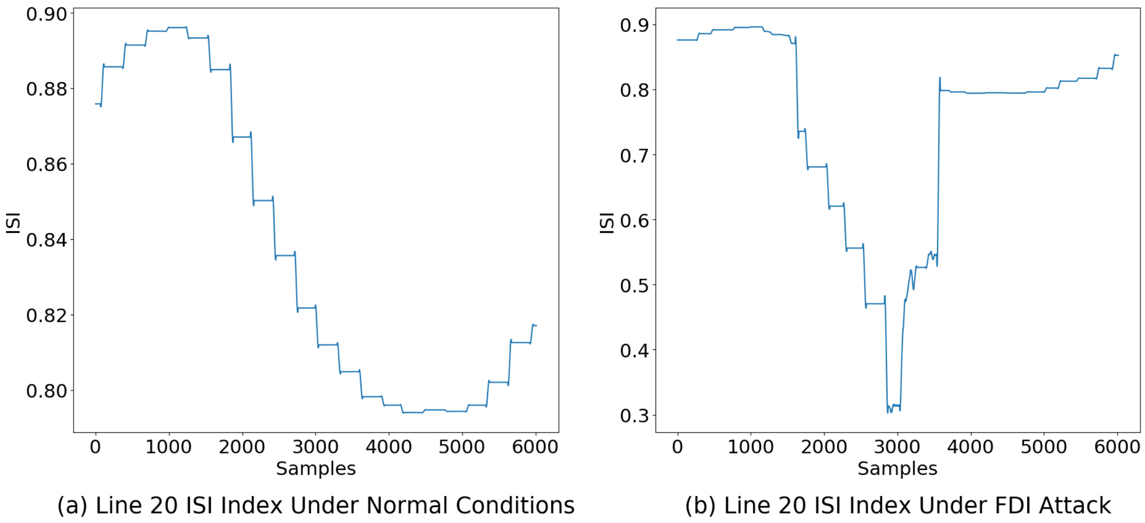


Figure 48: F_1 for Different Number of Compromised PMUs

Attack on ISI

The stealthy FDI attack on the ISI application in the 39-bus system targets bus 20. Fig. 49a shows the ISI index of bus 20 under normal conditions and Fig. 49b shows the same index under FDI attack. The attacker modifies the measurements to gradually decrease the perceived ISI until it reaches a critical value (0.3). Fig. 50 presents the performance, evaluated using the F_1 measure, of the studied anomaly detection algorithms in detecting this attack.



(a) Line 20 ISI Index Under Normal Conditions

(b) Line 20 ISI Index Under FDI Attack

Figure 49: ISI Experiment on Bus 20 of IEEE 39-bus System

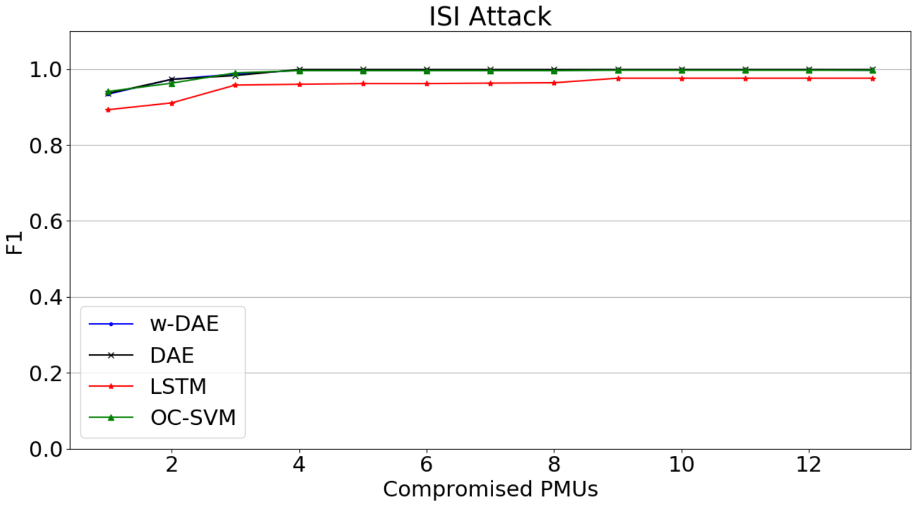


Figure 50: F_1 for Different Number of Compromised PMUs

Masking Attack on PAM

In the masking FDI attack against PAM in the 39-bus system, the attacker hides an instability on line 32 where the transferred power increases by 1 MW. When the attacker notices this instability in the system, he starts gradually modifying the reported measurements to display normal operation, thus hiding the instability from the controller. This attack is the opposite of the previous attack on the PAM application. Fig. 51 presents the performance, evaluated using the F_1 measure, of the anomaly detection algorithms in detecting this attack.

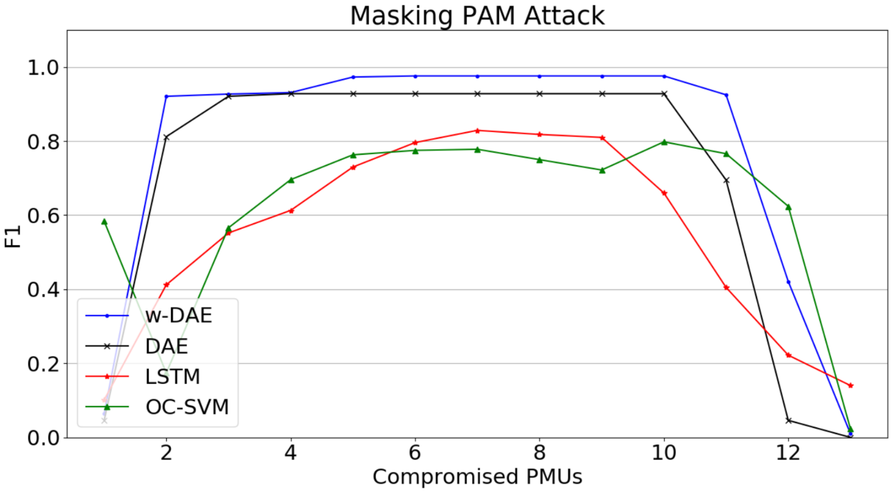


Figure 51: F_1 for Different Number of Compromised PMUs

Masking attack on FVSI

In the masking FDI attack against FVSI in the 39-bus system, the attacker hides an instability on line 27 where the index increase to 0.7. When the attacker notices this instability in the system, he starts gradually modifying the reported measurements to display normal operation, thus hiding the instability from the controller. This attack is the opposite of the previous attack on the FVSI application. Fig. 52 presents the performance, evaluated using the F_1 measure, of the studied anomaly detection algorithms in detecting this attack.

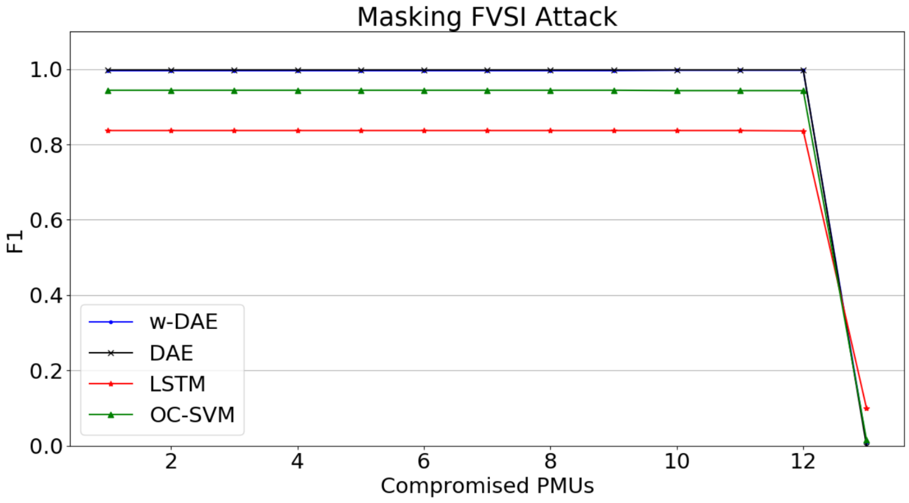


Figure 52: F_1 for Different Number of Compromised PMUs

Masking attack on ISI

In the masking FDI attack against ISI in the 39-bus system, the attacker hides an instability on bus 20 where the index decreases to 0.3. When the attacker notices this instability in the system, he starts gradually modifying the reported measurements to display normal operation, thus hiding the instability from the controller. This attack is the opposite of the previous attack on the ISI application. Fig. 53 presents the performance, evaluated using the F_1 measure, of the studied anomaly detection algorithms in detecting this attack.

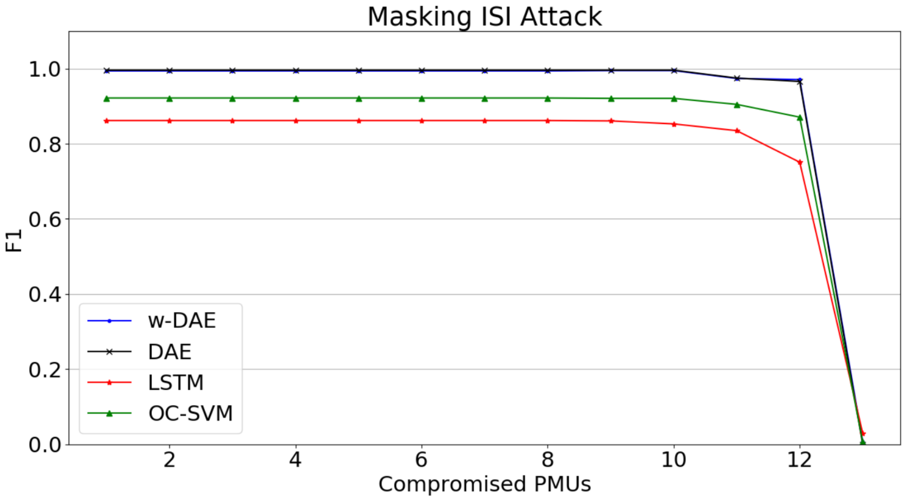


Figure 53: F_1 for Different Number of Compromised PMUs

Table 11: Detection Results for FDI Against Applications in the IEEE 39-bus System.

		PAM				FVSI				ISI			
Metrics	**# of Compromised PMUs**	**w-DAE**	**DAE**	**LSTM**	**OC-SVM**	**w-DAE**	**DAE**	**LSTM**	**OC-SVM**	**w-DAE**	**DAE**	**LSTM**	**OC-SVM**
Accuracy	1	0.933	0.935	0.804	0.859	0.999	0.996	0.948	0.995	0.956	0.957	0.928	0.96
	2	0.973	0.972	0.846	0.899	0.999	0.999	0.954	0.995	0.981	0.981	0.939	0.974
	3	0.989	0.993	0.859	0.922	0.998	0.999	0.962	0.995	0.991	0.988	0.97	0.993
	4	0.989	0.993	0.864	0.929	0.998	0.999	0.961	0.995	0.998	0.999	0.971	0.997
	5	0.99	0.993	0.876	0.932	0.998	0.999	0.961	0.995	0.998	0.999	0.973	0.997
	6	0.99	0.993	0.884	0.935	0.998	0.999	0.961	0.995	0.998	0.999	0.973	0.997
	7	0.991	0.993	0.899	0.939	0.998	0.999	0.961	0.995	0.998	0.999	0.974	0.997
	8	0.989	0.993	0.909	0.944	0.998	0.999	0.961	0.995	0.998	0.999	0.974	0.997
	9	0.988	0.993	0.905	0.947	0.998	0.999	0.961	0.995	0.998	0.999	0.983	0.998
	10	0.955	0.993	0.771	0.921	0.998	0.999	0.962	0.995	0.998	0.999	0.982	0.998
	11	0.918	0.86	0.742	0.91	0.999	0.999	0.962	0.995	0.998	0.999	0.982	0.998
	12	0.779	0.756	0.726	0.899	0.998	0.999	0.962	0.995	0.998	0.999	0.982	0.998
	13	0.761	0.761	0.734	0.816	0.997	0.998	0.852	0.955	0.998	0.999	0.982	0.998
F_1	1	0.837	0.842	0.445	0.595	0.998	0.993	0.921	0.992	0.934	0.936	0.893	0.941
	2	0.939	0.938	0.608	0.739	0.998	0.999	0.931	0.992	0.973	0.973	0.911	0.963
	3	0.977	0.985	0.676	0.81	0.997	0.999	0.943	0.993	0.987	0.983	0.958	0.99
	4	0.977	0.985	0.691	0.83	0.997	0.999	0.943	0.993	0.997	0.999	0.96	0.996
	5	0.978	0.985	0.724	0.838	0.997	0.999	0.943	0.993	0.997	0.999	0.962	0.996
	6	0.98	0.985	0.747	0.848	0.997	0.999	0.943	0.992	0.997	0.999	0.962	0.996
	7	0.981	0.985	0.786	0.858	0.997	0.999	0.943	0.993	0.997	0.999	0.963	0.996
	8	0.977	0.985	0.811	0.87	0.997	0.999	0.943	0.992	0.997	0.999	0.964	0.996
	9	0.975	0.985	0.804	0.879	0.997	0.999	0.943	0.992	0.998	0.999	0.976	0.997
	10	0.899	0.985	0.343	0.808	0.997	0.999	0.943	0.993	0.998	0.999	0.976	0.997
	11	0.8	0.597	0.191	0.776	0.998	0.999	0.943	0.993	0.998	0.999	0.976	0.997
	12	0.181	0.001	0.094	0.74	0.997	0.999	0.943	0.993	0.998	0.999	0.976	0.997
	13	0.016	0	0.067	0.399	0.996	0.998	0.837	0.944	0.997	0.999	0.976	0.997
FPR	1	0.00057	0	0.04563	0.0029	0.00065	0	0.05378	0.00629	0.00161	0.0001	0.02479	0.00343
	2	0.00057	0	0.04563	0.0029	0.00065	0	0.05378	0.00629	0.00252	0.0001	0.02479	0.00343
	3	0.00059	0	0.05709	0.0029	0.00131	0	0.0553	0.00629	0.00252	0.0001	0.02479	0.00343
	4	0.00059	0	0.05709	0.0029	0.00174	0	0.05595	0.00629	0.0023	0.0001	0.02479	0.00343
	5	0.00059	0	0.05729	0.0029	0.00174	0	0.05595	0.00629	0.0023	0.0001	0.02502	0.00343
	6	0.00059	0	0.05729	0.0029	0.00174	0	0.05595	0.00629	0.0023	0.0001	0.02502	0.00343
	7	0.00059	0	0.05729	0.0029	0.00174	0	0.05595	0.00629	0.0023	0.0001	0.02502	0.00343
	8	0.00059	0	0.05729	0.0029	0.00174	0	0.05595	0.00629	0.0023	0.0001	0.02502	0.00343
	9	0.00059	0	0.05807	0.0029	0.00174	0	0.05595	0.00629	0.00252	0.0001	0.0264	0.00343
	10	0.00157	0	0.05886	0.002923	0.00239	0	0.05595	0.00629	0.00252	0.0001	0.0264	0.00343
	11	0.00157	0	0.05866	0.0029	0.00218	0	0.05595	0.00629	0.00275	0.0001	0.0264	0.00343
	12	0.00157	0	0.05866	0.0029	0.00261	0	0.05595	0.00629	0.00275	0.0001	0.0264	0.00343
	13	0.00191	0	0.04754	0.0029	0.00399	0.00142	0.2381	0.0724	0.00298	0.0001	0.0264	0.00343
FNR	1	0.27869	0.273	0.67274	0.5732	0.00232	0.01302	0.04928	0.00232	0.12085	0.12085	0.15698	0.10507
	2	0.11293	0.117	0.4997	0.4086	0.00232	0.00232	0.02929	0.00232	0.04859	0.05233	0.12542	0.06645
	3	0.0425	0.029	0.39891	0.3127	0.00232	0.00232	0.00186	0.00139	0.02076	0.03281	0.04028	0.01453
	4	0.0425	0.029	0.37948	0.2848	0.00232	0.00232	0.00186	0.00139	0.00249	0.00249	0.03571	0.00249
	5	0.04068	0.029	0.33212	0.272	0.00232	0.00232	0.00186	0.00139	0.00249	0.00249	0.03198	0.00208
	6	0.03825	0.029	0.29751	0.2568	0.00232	0.00232	0.00139	0.00186	0.00249	0.00249	0.03032	0.00208
	7	0.03461	0.029	0.2374	0.2417	0.00232	0.00232	0.00139	0.00139	0.00249	0.00249	0.02865	0.00208
	8	0.04311	0.029	0.19672	0.2228	0.00232	0.00232	0.00139	0.00186	0.00249	0.00249	0.02824	0.00208
	9	0.04675	0.029	0.20765	0.2095	0.00186	0.00232	0.00139	0.00186	0	0.00249	0.00125	0
	10	0.18033	0.029	0.75531	0.316333	0	0.00232	0.00046	0.00093	0	0.00208	0.00166	0
	11	0.3303	0.575	0.87553	0.3607	0	0.00232	0.00046	0.00093	0	0.00208	0.00208	0
	12	0.89982	0.999	0.94171	0.4074	0	0.00232	0.00046	0.00139	0	0.00208	0.00208	0
	13	0.99211	1	0.95993	0.7486	0.00186	0.00232	0.00139	0.00093	0	0.00208	0.00208	0

Table 12: Detection Results for Masking FDI Attacks in the IEEE 39-bus System.

		PAM				FVSI				ISI			
Metrics	**# of Compromised PMUs**	**w-DAE**	**DAE**	**LSTM**	**OC-SVM**	**w-DAE**	**DAE**	**LSTM**	**OC-SVM**	**w-DAE**	**DAE**	**LSTM**	**OC-SVM**
Accuracy	1	0.738	0.737	0.725	0.833	0.997	0.998	0.852	0.955	0.995	0.997	0.872	0.933
	2	0.96	0.915	0.785	0.743	0.997	0.998	0.852	0.955	0.996	0.997	0.872	0.933
	3	0.963	0.961	0.82	0.828	0.997	0.998	0.852	0.955	0.996	0.997	0.872	0.933
	4	0.965	0.964	0.838	0.867	0.997	0.998	0.852	0.955	0.996	0.997	0.872	0.933
	5	0.986	0.964	0.876	0.891	0.997	0.998	0.852	0.955	0.996	0.997	0.872	0.933
	6	0.988	0.964	0.902	0.896	0.997	0.998	0.852	0.955	0.996	0.997	0.872	0.933
	7	0.988	0.964	0.915	0.897	0.997	0.998	0.852	0.955	0.996	0.997	0.872	0.933
	8	0.988	0.964	0.91	0.886	0.997	0.998	0.852	0.955	0.996	0.997	0.872	0.933
	9	0.987	0.964	0.907	0.876	0.997	0.998	0.852	0.955	0.996	0.997	0.871	0.932
	10	0.987	0.964	0.852	0.904	0.998	0.998	0.852	0.954	0.996	0.997	0.865	0.932
	11	0.962	0.874	0.782	0.892	0.998	0.998	0.852	0.954	0.98	0.981	0.85	0.919
	12	0.801	0.737	0.745	0.845	0.998	0.998	0.852	0.954	0.977	0.973	0.789	0.893
	13	0.73	0.73	0.73	0.719	0.62	0.62	0.5	0.579	0.596	0.598	0.479	0.534
F_1	1	0.064	0.045	0.101	0.584	0.996	0.998	0.837	0.944	0.994	0.996	0.862	0.922
	2	0.921	0.812	0.412	0.174	0.996	0.998	0.837	0.944	0.994	0.996	0.862	0.922
	3	0.927	0.921	0.552	0.566	0.996	0.998	0.837	0.944	0.994	0.996	0.862	0.922
	4	0.931	0.928	0.613	0.696	0.996	0.998	0.837	0.944	0.994	0.996	0.862	0.922
	5	0.973	0.928	0.73	0.763	0.996	0.998	0.837	0.944	0.994	0.996	0.862	0.922
	6	0.976	0.928	0.796	0.775	0.996	0.998	0.837	0.944	0.994	0.996	0.862	0.922
	7	0.976	0.928	0.829	0.778	0.996	0.998	0.837	0.944	0.994	0.996	0.862	0.922
	8	0.976	0.928	0.818	0.75	0.996	0.998	0.837	0.944	0.994	0.996	0.862	0.922
	9	0.976	0.928	0.81	0.722	0.996	0.998	0.837	0.944	0.995	0.996	0.861	0.921
	10	0.976	0.928	0.66	0.798	0.997	0.998	0.837	0.943	0.995	0.996	0.853	0.921
	11	0.925	0.695	0.405	0.766	0.997	0.998	0.837	0.943	0.974	0.975	0.835	0.905
	12	0.421	0.046	0.222	0.624	0.997	0.998	0.836	0.943	0.971	0.966	0.751	0.871
	13	0.01	0	0.14	0.023	0.009	0	0.1	0.016	0.007	0	0.029	0.006
FPR	1	0.0009	0	0.02742	0.02016	0.00399	0.00142	0.2381	0.0724	0.0064	0.0036	0.21242	0.11228
	2	0.0009	0	0.02742	0.02016	0.00399	0.00142	0.2381	0.0724	0.00612	0.0036	0.21242	0.11228
	3	0.0009	0	0.02742	0.02016	0.00399	0.00142	0.23838	0.0724	0.00612	0.0036	0.21242	0.11228
	4	0.0009	0	0.02742	0.02016	0.00399	0.00142	0.23867	0.0724	0.00612	0.0036	0.21242	0.11228
	5	0.0009	0	0.02742	0.02016	0.00399	0.00142	0.23838	0.0724	0.00612	0.0036	0.21242	0.11228
	6	0.0009	0	0.02742	0.02016	0.00399	0.00142	0.23838	0.0724	0.00612	0.0036	0.21242	0.11228
	7	0.0009	0	0.02742	0.02016	0.00371	0.00142	0.23838	0.0724	0.00612	0.0036	0.21269	0.11228
	8	0.0009	0	0.02742	0.02016	0.00371	0.00142	0.23867	0.0724	0.00612	0.0036	0.21269	0.11228
	9	0.0009	0	0.02742	0.02016	0.00371	0.00142	0.23895	0.0724	0.0064	0.0036	0.21242	0.11228
	10	0.00202	0	0.02944	0.02016	0.00371	0.00142	0.23895	0.0724	0.0064	0.0036	0.21242	0.11228
	11	0.00202	0	0.02944	0.02016	0.00371	0.00142	0.23895	0.0724	0.00612	0.0036	0.21242	0.11228
	12	0.00202	0	0.02944	0.02016	0.00371	0.00142	0.23838	0.0724	0.00612	0.0036	0.21242	0.11228
	13	0.00202	0	0.02944	0.02016	0.00285	0.00142	0.23838	0.0724	0.00612	0.0036	0.21242	0.11228
FNR	1	0.96661	0.97693	0.94293	0.56466	0.00186	0.00232	0.00093	0.00093	0.00208	0.00208	0.00208	0
	2	0.14511	0.31694	0.72131	0.89982	0.00186	0.00232	0.00046	0.00046	0.00208	0.00208	0.00208	0
	3	0.13358	0.14572	0.59077	0.58349	0.00232	0.00232	0.00046	0.00046	0.00208	0.00208	0.00166	0
	4	0.12629	0.13418	0.5258	0.43716	0.00232	0.00232	0.00046	0.00046	0.00208	0.00208	0.00166	0
	5	0.04979	0.13418	0.38312	0.34973	0.00232	0.00232	0.00046	0.00046	0.00208	0.00208	0.00166	0
	6	0.04372	0.13418	0.29022	0.33273	0.00232	0.00232	0.00046	0	0.00208	0.00208	0.00166	0
	7	0.04372	0.13418	0.23983	0.32908	0.00232	0.00232	0.00046	0	0.00208	0.00208	0.00166	0
	8	0.04372	0.13418	0.25744	0.36733	0.00232	0.00232	0.00046	0	0.00208	0.00208	0.00166	0
	9	0.04432	0.13479	0.26897	0.40437	0.00232	0.00232	0.00046	0	0.00042	0.00208	0.00374	0.00208
	10	0.04129	0.13479	0.46873	0.29994	0.00046	0.00232	0.00093	0.00232	0.00083	0.00249	0.02035	0.00249
	11	0.13479	0.46691	0.72617	0.34487	0.00046	0.00232	0.00093	0.00232	0.04153	0.04319	0.05606	0.03447
	12	0.73163	0.97632	0.86521	0.52155	0.00046	0.00232	0.00186	0.00232	0.04776	0.06146	0.20764	0.09884
	13	0.99514	1	0.91864	0.98786	0.99535	1	0.92701	0.9907	0.99668	1	0.98048	0.99668

5.4 Result Analysis

From the presented results, we can see that DAE has the best performance across all experiments, followed by w-DAE, then LSTM and OC-SVM. LSTM and OC-SVM performed similarly in most cases with some instances where LSTM outperformed OC-SVM and others where OC-SVM outperforming LSTM. In particular, we notice that LSTM's performance slightly deteriorate on the IEEE 39-bus system where it falls below OC-SVM which was able to scale better on the bigger system.

Additionally, we notice that including time information in the feature vector does not improve the detection results: DAE and w-DAE had almost the same performance, and they both had better results than LSTM in all test cases.

Furthermore, we see that the detection performance increases when more PMUs are compromised. This is especially evident in the 39-bus system where the number of PMUs is bigger. Such a limited attack will not be capable of showing an effect on the targeted application serious enough to illicit a reaction from the controller or that is consistent across different areas in the grid. The tested methods perform worse on these limited attacks than more dangerous attacks because the subtle alterations to the small number of measurements results in a reconstruction error that may not be big enough to cross the threshold in most instances of the attack. This is caused by the fact that the reconstruction errors of all features are summed and averaged which can lead to suppressing errors coming from the small number of subtle variations.

Moreover, we notice low FPR especially for DAE and w-DAE. Low FPR shows a low number of false alerts raised. False alerts are a significant problem that cyberattack detection teams face because, when numerous, false alerts can become overwhelming and time-costly and subsequently they will lower the confidence of the operators in the detection models. As a result, operators will start to ignore raised alarms which can be very dangerous in case the alarm is accurate and corresponds to a real cyberattack. Therefore, low FPR is a very important indicator of the good performance of the detection model. On the other hand, we see in attacks on the PAM application that once the attacker has control of most of the system, the detection performance deteriorates until it reaches almost 0 when all PMUs are compromised. This is due to the fact that increasing the load by 50% can lead to an increase in PAM indices of some lines. Therefore if the attacker alters most or all measurements in the system to show an increase in PAM indices, he will be portraying to the controller an operational scenario where there is a 50% increase in some loads, which is a scenario that is included in the training set. To this point, we also notice similar behavior with the masking attacks because in those scenarios, the attacker is altering the measurements to show the normal behavior of the grid, effectively portraying a normal scenario that was also included in the training set. This shows that the techniques avoid over-fitting and are able to generalize. However, we don't see this pattern of behavior for attacks on FVSI and ISI because the scenario that shows an instability in these applications is not included in the training scenarios, thus the models won't recognize it and will flag it. Most notably, the detection results are consistent for the 9 and 39-bus systems which attests for the scalability of the proposed technique, and the robustness of the results. In addition, we measure the required detection time for each incoming packet and the results show that it is in the order of milliseconds, varying between 0.06 seconds and 0.15 seconds for the different models. This shows that the detection process doesn't cause any significant delay on the communication and is suitable for high-rate protocols used in WAMS.

Chapter 6

Conclusion

Smart Grid security is a crucial research topic that is always evolving and attracting more research effort due to the importance of protecting critical infrastructures against the new threat of cyberattacks. In this research work, we present a comparative study of data driven anomaly detection techniques for identifying stealthy FDI attacks in WAMS. We design, implement, and evaluate a new platform for WAMS security monitoring that utilizes DPI and anomaly detection methods in order to identify cyberattacks. We formulate the FDI problem as an anomaly detection problem to account for the sparsity of attack data in realistic setups. Furthermore, we focus on linking the attacks to specific WAMS applications in order to observe the impact such attacks can have on the grid. The features used for anomaly detection are extracted from WAMS-specific protocols via DPI. We emphasise on performing the experiments in a realistic environment by incorporating real hardware in the simulations, and by limiting the number of PMUs in the system. The studied techniques proved to be effective in detecting FDI attacks under different attacker conditions. Moreover, the techniques demonstrated that they are scalable by exhibiting consistent performance on both the 9-bus and the 39-bus systems. By accomplishing this work, our research contributions consist of:

1. Building a realistic WAMS testbed that utilizes hardware from commercial vendors, simulates different operational scenarios, and monitors multiple stability indices.

2. Developing FDI attacks that target WAMS applications and showing the impact that those attacks can have on the grid.

3. Formulating the FDI attack detection problem as an anomaly detection problem in order to account for the lack of FDI attack data found in the real facilities thus aligning the solution with realistic setups.

4. Testing and comparing the performance and scalability of four anomaly detection techniques in identifying FDI attacks by analysing DPI-based features.

Our work can be improved in the future from different aspects. First, FNR is significantly higher than FPR, this is due to the fact that the attacker modifies the measurements gradually to achieve the ultimate goal so when the attack is launched there is a phase where the measurements are being modified but they are still very similar to the normal measurements. Although this slight variation in the measurements is not enough to portray an instability to the controller, it is nevertheless considered as an attack instance and the proposed algorithms are not able to flag such subtle changes. Further experimentation can help in resolving this issue and lowering the FNR. Second, supplementing DPI-based features with other sources of knowledge such as network system management (NSM) information and device logs can possibly improve the detection performance because it provides a holistic view of the network behavior. For example, in the FDI attack tree presented, the attacker can either infiltrate the network or take control of the PMU. Including NSM features in the attack detection model would provide more information on the communication network such as packet interarrival time and number of opened and closed connections. This information can be leveraged to detect rogue devices and MITM setups in the network which are used to launch FDI attacks. In addition, including device logs can detect when a PMU in the field is compromised, physically or via malware, by monitoring the processes running on the PMU and this could convey to the detection model that the measurements received are modified at the level of the PMU. Third, combining anomaly detection and classification can help in identifying the anomalous behavior and eradicating it. The anomaly detection model would flag any abnormal behavior and pass it to the classification model in order to determine the exact nature of the attack. Furthermore, this approach can be expanded to differentiate between zero-day attacks and known attacks: zero-day attacks would be flagged by the anomaly detection model but the classification model would not be able to confidently associate it with a know attack, while known attacks would be flagged as anomalous and classified with high confidence. This would enhance the security of WAMS by providing the operator with more information regarding the event taking place however it requires the simulation and collection of numerous attack scenarios. Fourth, combining rule-based and data-driven anomaly detection to monitor the different protocol frames can enhance the security of WAMS communications. For example, IEEE C37.118 has four different frames that are used to establish the connection between the IEDs, set/change the configuration of the packets, and carry the measurements. In this work we focused on monitoring the data frames that carry the measurements using data-driven techniques. However, future work can expand on this effort by monitoring the configuration, command, and header frames using rule-based anomaly detection, because the behavior of these frames is simpler and the information they carry can be modeled using rules developed based on the specifications in the protocol and the sequential behavior of these frames. Fifth, to ensure the safe deployment of the SG, research effort should focus on monitoring the security of the different SG domains such as substations, distribution systems, microgirds, etc. The security monitoring approaches of the different domains would compliment each other and ensure a more secure SG. For example, an attack on the transmission system can be linked to another attack on the distribution system launched by the same cyberattackers. By monitoring both systems, the controller can draw a link between both cyberattacks, increasing the controller's awareness of the situation and facilitating the response and recovery process.

Bibliography

[1] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, 12:2825–2830, 2011.

[2] Hao Li, Gary W Rosenwald, Juhwan Jung, and Chen-Ching Liu. Strategic power infrastructure defense. *Proceedings of the IEEE*, 93(5):918–933, 2005.

[3] Prabha Kundur, Neal J Balu, and Mark G Lauby. *Power system stability and control*, volume 7. McGraw-hill New York, 1994.

[4] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke. Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics*, 7(4):529–539, Nov 2011.

[5] M. Zima, M. Larsson, P. Korba, C. Rehtanz, and G. Andersson. Design aspects for wide-area monitoring and control systems. *Proceedings of the IEEE*, 93(5):980–996, May 2005.

[6] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. Begovic, and A. Phadke. Wide-area monitoring, protection, and control of future electric power networks. *Proceedings of the IEEE*, 99(1):80–93, Jan 2011.

[7] N. Komninos, E. Philippou, and A. Pitsillides. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Communications Surveys & Tutorials*, 16(4):1933–1954, Fourthquarter 2014.

[8] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong. The 2015 ukraine blackout: Implications for false data injection attacks. *IEEE Transactions on Power Systems*, 32(4):3317–3318, July 2017.

[9] Anton Cherepanov and Robert Lipovsky. Blackenergy–what we really know about the notorious cyber attacks. *Virus Bulletin October*, 2016.

[10] Anton Cherepanov and Robert Lipovsky. Industroyer: Biggest threat to industrial control systems since stuxnet. *WeLiveSecurity, ESET*, 12, 2017.

[11] Boldizsár Bencsáth, Gábor Pék, Levente Buttyán, and Márk Félegyházi. Duqu: A stuxnet-like malware found in the wild. *CrySyS Lab Technical Report*, 14:1–60, 2011.

[12] R. Langner. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security Privacy*, 9(3):49–51, May 2011.

[13] J. Liang, L. Sankar, and O. Kosut. Vulnerability analysis and consequences of false data injection attack on power system state estimation. *IEEE Transactions on Power Systems*, 31(5):3864–3872, 2016.

[14] Stuart A Boyer. *SCADA: supervisory control and data acquisition*. International Society of Automation, 2009.

[15] Mini S Thomas and John Douglas McDonald. *Power system SCADA and smart grids*. CRC press, 2015.

[16] Keith Stouffer, Joe Falco, and Karen Scarfone. Guide to industrial control systems (ics) security. *NIST special publication*, 800(82):16–16, 2011.

[17] H. Bentarzi, M. Tsebia, and A. Abdelmoumene. Pmu based scada enhancement in smart power grid. In *2018 IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering (CPE-POWERENG 2018)*, pages 1–6, 2018.

[18] ALI Ikbal, Mohd Asim Aftab, and SM Suhail Hussain. Performance comparison of IEC 61850-90-5 and IEEE c37. 118.2 based wide area PMU communication networks. *Journal of Modern Power Systems and Clean Energy*, 4(3):487–495, 2016.

[19] Ieee standard for synchrophasor data transfer for power systems. *IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005)*, pages 1–53, Dec 2011.

[20] Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118. Standard, International Electrotechnical Commission, Geneva, CH, 2012.

[21] KE Martin, Gustavo Brunello, MG Adamiak, Galina Antonova, M Begovic, G Benmouyal, PD Bui, H Falk, V Gharpure, A Goldstein, et al. An overview of the IEEE standard c37. 118.2—synchrophasor data transfer for power systems. *IEEE Transactions on Smart Grid*, 5(4):1980–1984, 2014.

[22] Communication networks and systems for power utility automation. Standard, International Electrotechnical Commission, Geneva, CH, 2004.

[23] R. E. Mackiewicz. Overview of iec 61850 and benefits. In *2006 IEEE PES Power Systems Conference and Exposition*, pages 623–630, Oct 2006.

[24] T. S. Sidhu and Y. Yin. Modelling and simulation for performance evaluation of iec61850-based substation communication systems. *IEEE Transactions on Power Delivery*, 22(3):1482–1489, July 2007.

[25] M. G. Kanabar and T. S. Sidhu. Performance of iec 61850-9-2 process bus and corrective measure for digital relaying. volume 26, pages 725–735, April 2011.

[26] Carl Kriger, Shaheen Behardien, and John-Charly Retonda-Modiya. A detailed analysis of the GOOSE message structure in an IEC 61850 standard-based substation automation system. *International Journal of Computers Communications & Control*, 8(5):708–721, 2013.

[27] Q Yang, D Keckalo, D Dolezilek, and E Cenzon. Testing iec 61850 merging units. In *proceedings of the 44th Annual Western Protective Relay Conference, Spokane, WA*, 2017.

[28] Mini S Thomas, Ikbal Ali, and Nitin Gupta. Interoperable framework for IEC 61850-compliant ieds and noncompliant energy meters with SCADA. *Energy Technology & Policy*, 2(1):73–81, 2015.

[29] Jan Tore Sørensen and Martin Gilje Jaatun. An analysis of the manufacturing messaging specification protocol. In *International Conference on Ubiquitous Intelligence and Computing*, pages 602–615. Springer, 2008.

[30] Phase angle monitoring - naspi.org, Jun 2016.

[31] Ismail Musirin and TK Abdul Rahman. Novel fast voltage stability index (fvsi) for voltage stability analysis in power transmission system. In *Student Conference on Research and Development*, pages 265–268. IEEE, 2002.

[32] Andrzej Wiszniewski. New criteria of voltage stability margin for the purpose of load shedding. *IEEE Transactions on Power Delivery*, 22(3):1367–1371, 2007.

[33] H. He and J. Yan. Cyber-physical attacks and defences in the smart grid: a survey. *IET Cyber-Physical Systems: Theory Applications*, 1(1):13–27, 2016.

[34] Yao Liu, Peng Ning, and Michael K Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security (TISSEC)*, 14(1):13, 2011.

[35] Mohammad Esmalifalak, Zhu Han, and Lingyang Song. Effect of stealthy bad data injection on network congestion in market based power system. In *2012 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 2468–2472, 2012.

[36] Michael Sutton, Adam Greene, and Pedram Amini. *Fuzzing: brute force vulnerability discovery*. Pearson Education, 2007.

[37] Andrew Nicholson, Stuart Webber, Shaun Dyer, Tanuja Patel, and Helge Janicke. SCADA security in the light of cyber-warfare. *Computers & Security*, 31(4):418–436, 2012.

[38] Russian government cyber activity targeting energy and other critical infrastructure sectors. Technical report, The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 2018.

[39] 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*, 21(2):1851–1877, Secondquarter 2019.

[40] S. Torabi, E. Bou-Harb, C. Assi, M. Galluscio, A. Boukhtouta, and M. Debbabi. Inferring, characterizing, and investigating internet-scale malicious iot device activities: A network telescope perspective. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 562–573, June 2018.

[41] Keke Gai, Meikang Qiu, Zhong Ming, Hui Zhao, and Longfei Qiu. Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks. *IEEE Transactions on Smart Grid*, 8(5):2431–2439, 2017.

[42] Q. Yan, F. R. Yu, Q. Gong, and J. Li. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE Communications Surveys & Tutorials*, 18(1):602–622, Firstquarter 2016.

[43] N. Hoque, D. Bhattacharyya, and J. Kalita. Botnet in ddos attacks: Trends and challenges. *IEEE Communications Surveys & Tutorials*, 17(4):2242–2270, Fourthquarter 2015.

[44] F. M. Cleveland. Cyber security issues for advanced metering infrasttructure (ami). In *2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century*, pages 1–5, July 2008.

[45] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. Ddos in the iot: Mirai and other botnets. *Computer*, 50(7):80–84, 2017.

[46] Mauro Conti, Nicola Dragoni, and Viktor Lesyk. A survey of man in the middle attacks. *IEEE Communications Surveys & Tutorials*, 18(3):2027–2051, 2016.

[47] C. Xu, S. Chen, J. Su, S. M. Yiu, and L. C. K. Hui. A survey on regular expression matching for deep packet inspection: Applications, algorithms, and hardware platforms. *IEEE Communications Surveys & Tutorials*, 18(4):2991–3029, Fourthquarter 2016.

[48] Ying-Dar Lin, Po-Ching Lin, Viktor K Prasanna, H Jonathan Chao, and John W Lockwood. Guest editorial deep packet inspection: Algorithms, hardware, and applications. *IEEE Journal on Selected Areas in Communications*, 32(10):1781–1783, 2014.

[49] Adam Hahn. Operational technology and information technology in industrial control systems. In *Cyber-security of SCADA and other industrial control systems*, pages 51–68. Springer, 2016.

[50] H. Lin, A. Slagell, Z. Kalbarczyk, P. W. Sauer, and R. Iyer. Runtime semantic security analysis to detect and mitigate control-related attacks in power grids. *IEEE Transactions on Smart Grid*, 9(1):163–178, Jan 2018.

[51] V Chandala, A Banerjee, and V Kumar. Anomaly detection: A survey, acm computing surveys. *University of Minnesota*, 2009.

[52] Anna L Buczak and Erhan Guven. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications surveys & tutorials*, 18(2):1153–1176, 2015.

[53] Stuart J Russell and Peter Norvig. Artificial intelligence: a modern approach. malaysia. *Pearson Education Limited. Rycroft-Malone, J.(2004). The PARIHS framework—A framework for guiding the implementation of evidenceǦ based practice. Journal of nursing care quality*, 19(4):297–304, 2016.

[54] Thomas Morris, Rayford Vaughn, and Yoginder Dandass. A retrofit network intrusion detection system for modbus RTU and ASCII industrial control systems. In *2012 45th Hawaii International Conference on System Sciences*, pages 2338–2345, 2012.

[55] Georgia Koutsandria, Vishak Muthukumar, Masood Parvania, Sean Peisert, Chuck McParland, and Anna Scaglione. A hybrid network ids for protective digital relays in the power transmission grid. In *2014 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 908–913, 2014.

[56] Yi Yang, Kieran McLaughlin, Tim Littler, Sakir Sezer, Bernardi Pranggono, and HF Wang. Intrusion detection system for IEC 60870-5-104 based SCADA networks. In *2013 IEEE power & energy society general meeting*, pages 1–5, 2013.

[57] Shengyi Pan, Thomas Morris, and Uttam Adhikari. A specification-based intrusion detection framework for cyber-physical environment in electric power system. *IJ Network Security*, 17(2):174–188, 2015.

[58] Junho Hong, Chen-Ching Liu, and Manimaran Govindarasu. Integrated anomaly detection for cyber security of the substations. *IEEE Transactions on Smart Grid*, 5(4):1643–1653, 2014.

[59] Rong Jiang, Rongxing Lu, Ye Wang, Jun Luo, Changxiang Shen, and Xuemin Sherman Shen. Energy-theft detection issues for advanced metering infrastructure in smart grid. *Tsinghua Science and Technology*, 19(2):105–120, 2014.

[60] James Christopher Foreman and Dheeraj Gurugubelli. Cyber attack surface analysis of advanced metering infrastructure. *arXiv preprint arXiv:1607.04811*, 2016.

[61] Gaoqi Liang, Junhua Zhao, Fengji Luo, Steven R Weller, and Zhao Yang Dong. A review of false data injection attacks against modern power systems. *IEEE Transactions on Smart Grid*, 8(4):1630–1638, 2016.

[62] Ruilong Deng, Gaoxi Xiao, Rongxing Lu, Hao Liang, and Athanasios V Vasilakos. False data injection on state estimation in power systems—attacks, impacts, and defense: A survey. *IEEE Transactions on Industrial Informatics*, 13(2):411–423, 2016.

[63] Po-Yu Chen, Shusen Yang, Julie A McCann, Jie Lin, and Xinyu Yang. Detection of false data injection attacks in smart-grid systems. *IEEE Communications Magazine*, 53(2):206–213, 2015.

[64] Ahmed S Musleh, Guo Chen, and Zhao Yang Dong. A survey on the detection algorithms for false data injection attacks in smart grids. *IEEE Transactions on Smart Grid*, 2019.

[65] Jun Yan, Bo Tang, and Haibo He. Detection of false data attacks in smart grid with supervised learning. In *2016 International Joint Conference on Neural Networks (IJCNN)*, pages 1395–1402, 2016.

[66] Dongchan Lee and Deepa Kundur. Cyber attack detection in PMU measurements via the expectation-maximization algorithm. In *2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pages 223–227, 2014.

[67] J. Wang, D. Shi, Y. Li, J. Chen, H. Ding, and X. Duan. Distributed framework for detecting PMU data manipulation attacks with deep autoencoders. *IEEE Transactions on Smart Grid*, 2018.

[68] Alfonso Valdes, Richard Macwan, and Matthew Backes. Anomaly detection in electrical substation circuits via unsupervised machine learning. In *2016 IEEE 17th International Conference on Information Reuse and Integration (IRI)*, pages 500–505, 2016.

[69] Mohamad El Hariri, Tarek A Youssef, Hany F Habib, and Osama Mohammed. Online false data detection and lost packet forecasting system using time series neural networks for IEC 61850 sampled measured values. In *2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–5, 2017.

[70] Lanchao Liu, Mohammad Esmalifalak, Qifeng Ding, Valentine A Emesih, and Zhu Han. Detecting false data injection attacks on power grid by sparse optimization. *IEEE Transactions on Smart Grid*, 5(2):612–621, 2014.

[71] Xiangyu Niu, Jiangnan Li, Jinyuan Sun, and Kevin Tomsovic. Dynamic detection of false data injection attack in smart grid using deep learning. In *2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–6. IEEE, 2019.

[72] Kebina Manandhar, Xiaojun Cao, Fei Hu, and Yao Liu. Detection of faults and attacks including false data injection attack in smart grid using kalman filter. *IEEE transactions on control of network systems*, 1(4):370–379, 2014.

[73] Danda B Rawat and Chandra Bajracharya. Detection of false data injection attacks in smart grid communication systems. *IEEE Signal Processing Letters*, 22(10):1652–1656, 2015.

[74] Qingyu Deng and Jian Sun. False data injection attack detection in a power grid using rnn. In *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*, pages 5983–5988. IEEE, 2018.

[75] Mustafa Faisal, Alvaro A Cardenas, and Avishai Wool. Modeling modbus TCP for intrusion detection. In *2016 IEEE Conference on Communications and Network Security (CNS)*, pages 386–390, 2016.

[76] Dong Wei, Florin Darie, and Ling Shen. Application layer security proxy for smart grid substation automation systems. In *2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–6, 2013.

[77] Yi Yang, Kieran McLaughlin, Lei Gao, Sakir Sezer, Yubo Yuan, and Yanfeng Gong. Intrusion detection system for IEC 61850 based smart substations. In *2016 IEEE Power and Energy Society General Meeting (PESGM)*, pages 1–5, 2016.

[78] YooJin Kwon, Huy Kang Kim, Yong Hun Lim, and Jong In Lim. A behavior-based intrusion detection technique for smart grid infrastructure. In *2015 IEEE Eindhoven PowerTech*, pages 1–6, 2015.

[79] Thomas Morris, Bryan Jones, Rayford Vaughn, and Yoginder Dandass. Deterministic intrusion detection rules for modbus protocols. In *2013 46th Hawaii International Conference on System Sciences*, pages 1773–1781, 2013.

[80] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, B. Pranggono, P. Brogan, and H. F. Wang. Intrusion detection system for network security in synchrophasor systems. In *IET International Conference on Information and Communications Technologies (IETICT 2013)*, pages 246–252, April 2013.

[81] Yi Yang, Keiran McLaughlin, Sakir Sezer, Tim Littler, Eul Gyu Im, Bernardi Pranggono, and HF Wang. Multiattribute scada-specific intrusion detection system for power networks. *IEEE Transactions on Power Delivery*, 29(3):1092–1102, 2014.

[82] U. K. Premaratne, J. Samarabandu, T. S. Sidhu, R. Beresh, and J. Tan. An intrusion detection system for IEC 61850 automated substations. *IEEE Transactions on Power Delivery*, 25(4):2376–2383, Oct 2010.

[83] Thomas Morris, Shengyi Pan, Uttam Adhikari, Nicolas Younan, Roger King, and Vahid Madani. Cyber security testing and intrusion detection for synchrophasor systems. *International Journal of Network Science*, 1(1):28–52, 2016.

[84] Robin Berthier and William H Sanders. Specification-based intrusion detection for advanced metering infrastructures. In *2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing*, pages 184–193, 2011.

[85] Read Sprabery, Thomas Morris, Shengyi Pan, Uttam Adhikari, and Vahid Madani. Protocol mutation intrusion detection for synchrophasor communications. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, page 41. ACM, 2013.

[86] Hui Lin, Adam Slagell, Catello Di Martino, Zbigniew Kalbarczyk, and Ravishankar K Iyer. Adapting Bro into SCADA: building a specification-based intrusion detection system for the DNP3 protocol. In *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, page 5. ACM, 2013.

[87] Yi Yang, Hai-Qing Xu, Lei Gao, Yu-Bo Yuan, Kieran McLaughlin, and Sakir Sezer. Multidimensional intrusion detection system for IEC 61850-based SCADA networks. *IEEE Transactions on Power Delivery*, 32(2):1068–1078, 2016.

[88] Haiyong Bao, Rongxing Lu, Beibei Li, and Ruilong Deng. Blithe: Behavior rule-based insider threat detection for smart grid. *IEEE Internet of Things Journal*, 3(2):190–205, 2015.

[89] P. Jokar and V. C. M. Leung. Intrusion detection and prevention for zigbee-based home area networks in smart grids. *IEEE Transactions on Smart Grid*, 9(3):1800–1811, May 2018.

[90] O. A. Beg, T. T. Johnson, and A. Davoudi. Detection of false-data injection attacks in cyber-physical dc microgrids. *IEEE Transactions on Industrial Informatics*, 13(5):2693–2703, Oct 2017.

[91] Paria Jokar, Nasim Arianpoo, and Victor CM Leung. Electricity theft detection in AMI using customers' consumption patterns. *IEEE Transactions on Smart Grid*, 7(1):216–226, 2015.

[92] Manali Chakraborty. Advanced monitoring based intrusion detection system for distributed and intelligent energy theft: Diet attack in advanced metering infrastructure. In *Transactions on Computational Science XXXI*, pages 77–97. Springer, 2018.

[93] Masood Parvania, Georgia Koutsandria, Vishak Muthukumary, Sean Peisert, Chuck McParland, and Anna Scaglione. Hybrid control network intrusion detection systems for automated power distribution systems. In *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, pages 774–779, 2014.

[94] Rafiullah Khan, Abdullah Albalushi, Kieran McLaughlin, David Laverty, and Sakir Sezer. Model based intrusion detection system for synchrophasor applications in smart grid. In *2017 IEEE Power & Energy Society General Meeting*, pages 1–5, 2017.

[95] Rafiullah Khan, Kieran McLaughlin, John Hastings David Laverty, Hastings David, and Sakir Sezer. Demonstrating cyber-physical attacks and defense for synchrophasor technology in smart grid. In *2018 16th Annual Conference on Privacy, Security and Trust (PST)*, pages 1–10, 2018.

[96] Shengyi Pan, Thomas Morris, and Uttam Adhikari. Developing a hybrid intrusion detection system using data mining for power systems. *IEEE Transactions on Smart Grid*, 6(6):3104–3113, 2015.

[97] Hyunguk Yoo and Taeshik Shon. Novel approach for detecting network anomalies for substation automation based on IEC 61850. *Multimedia Tools and Applications*, 74(1):303–318, 2015.

[98] Saranya Parthasarathy and Deepa Kundur. Bloom filter based intrusion detection for smart grid SCADA. In *2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1–6, 2012.

[99] Mahmoud El Chamie, Kin Gwn Lore, Devu Manikantan Shila, and Amit Surana. Physics-based features for anomaly detection in power grids with micro-pmus. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–7, 2018.

[100] Seemita Pal and Biplab Sikdar. A mechanism for detecting data manipulation attacks on PMU data. In *2014 IEEE International Conference on Communication Systems*, pages 253–257, 2014.

[101] Yacine Chakhchoukh, Song Liu, Masashi Sugiyama, and Hideaki Ishii. Statistical outlier detection for diagnosis of cyber attacks in power state estimation. In *2016 IEEE Power and Energy Society General Meeting (PESGM)*, pages 1–5, 2016.

[102] Mohammad Esmalifalak, Lanchao Liu, Nam Nguyen, Rong Zheng, and Zhu Han. Detecting stealthy false data injection using machine learning in smart grid. *IEEE Systems Journal*, 11(3):1644–1652, 2014.

[103] C. Gu, P. Jirutitijaroen, and M. Motani. Detecting false data injection attacks in ac state estimation. *IEEE Transactions on Smart Grid*, 6(5):2476–2483, Sep. 2015.

[104] Shang Li, Yasin Yılmaz, and Xiaodong Wang. Quickest detection of false data injection attack in wide-area smart grids. *IEEE Transactions on Smart Grid*, 6(6):2725–2735, 2014.

[105] Yi Huang, Mohammad Esmalifalak, Huy Nguyen, Rong Zheng, Zhu Han, Husheng Li, and Lingyang Song. Bad data injection in smart grid: attack and defense mechanisms. *IEEE Communications Magazine*, 51(1):27–33, 2013.

[106] Yun Gu, Ting Liu, Dai Wang, Xiaohong Guan, and Zhanbo Xu. Bad data detection method for smart grids based on distributed state estimation. In *2013 IEEE International Conference on Communications (ICC)*, pages 4483–4487, 2013.

[107] Yi Huang, Husheng Li, Kristy A Campbell, and Zhu Han. Defending false data injection attack on smart grid network using adaptive cusum test. In *2011 45th Annual Conference on Information Sciences and Systems*, pages 1–6, 2011.

[108] Mi Wen, Donghuan Yao, Beibei Li, and Rongxing Lu. State estimation based energy theft detection scheme with privacy preservation in smart grid. In *2018 IEEE International Conference on Communications (ICC)*, pages 1–6, 2018.

[109] Sandeep Kumar Singh, Ranjan Bose, and Anupam Joshi. Energy theft detection in advanced metering infrastructure. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pages 529–534, 2018.

[110] Jaime Yeckle and Bo Tang. Detection of electricity theft in customer consumption using outlier detection algorithms. In *2018 1st International Conference on Data Intelligence and Security (ICDIS)*, pages 135–140, 2018.

[111] Marcelo Zanetti, Edgard Jamhour, Marcelo Pellenz, Manoel Penna, Voldi Zambenedetti, and Ivan Chueiri. A tunable fraud detection system for advanced metering infrastructure using short-lived patterns. *IEEE Transactions on Smart Grid*, 2017.

[112] Muhammad Qasim Ali, Reza Yousefian, Ehab Al-Shaer, Sukumar Kamalasadan, and Quanyan Zhu. Two-tier data-driven intrusion detection for automatic generation control in smart grid. In *2014 IEEE Conference on Communications and Network Security*, pages 292–300, 2014.

[113] Anish Jindal, Amit Dua, Kuljeet Kaur, Mukesh Singh, Neeraj Kumar, and S Mishra. Decision tree and svm-based data analytics for theft detection in smart grid. *IEEE Transactions on Industrial Informatics*, 12(3):1005–1016, 2016.

[114] Sergio A Salinas and Pan Li. Privacy-preserving energy theft detection in microgrids: A state estimation approach. *IEEE Transactions on Power Systems*, 31(2):883–894, 2015.

[115] Varun Badrinath Krishna, Kiryung Lee, Gabriel A Weaver, Ravishankar K Iyer, and William H Sanders. F-deta: A framework for detecting electricity theft attacks in smart grids. In *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 407–418, 2016.

[116] Stephen McLaughlin, Brett Holbert, Ahmed Fawaz, Robin Berthier, and Saman Zonouz. A multi-sensor energy theft detection framework for advanced metering infrastructures. *IEEE Journal on Selected Areas in Communications*, 31(7):1319–1330, 2013.

[117] Xinyu Yang, Peng Zhao, Xialei Zhang, Jie Lin, and Wei Yu. Toward a gaussian-mixture model-based detection scheme against data integrity attacks in the smart grid. *IEEE Internet of Things Journal*, 4(1):147–161, 2016.

[118] Saurabh Amin, Galina A Schwartz, Alvaro A Cardenas, and S Shankar Sastry. Game-theoretic models of electricity theft detection in smart utility networks: Providing new capabilities with advanced metering infrastructure. *IEEE Control Systems Magazine*, 35(1):66–81, 2015.

[119] Jorge Valenzuela, Jianhui Wang, and Nancy Bissinger. Real-time intrusion detection in power system operations. *IEEE Transactions on Power Systems*, 28(2):1052–1062, 2012.

[120] Oliver Kosut, Liyan Jia, Robert J Thomas, and Lang Tong. Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures. In *2010 First IEEE International Conference on Smart Grid Communications*, pages 220–225, 2010.

[121] Kedi Zheng, Qixin Chen, Yi Wang, Chongqing Kang, and Qing Xia. A novel combined data-driven approach for electricity theft detection. *IEEE Transactions on Industrial Informatics*, 15(3):1809–1819, 2018.

[122] Meng Wu and Le Xie. Online detection of false data injection attacks to synchrophasor measurements: A data-driven approach. In *Proceedings of the 50th Hawaii international conference on system sciences*, 2017.

[123] Uttam Adhikari, Thomas Morris, and Shengyi Pan. Applying hoeffding adaptive trees for real-time cyber-power event and intrusion classification. *IEEE Transactions on Smart Grid*, 9(5):4049–4060, 2017.

[124] Raymond Hink, Justin Beaver, Mark Buckner, Tommy Morris, Uttam Adhikari, and Shengyi Pan. Machine learning for power system disturbance and cyber-attack discrimination. In *2014 7th international symposium on resilient control systems (ISRCS)*, pages 1–8, 2014.

[125] Shengyi Pan, Thomas Morris, and Uttam Adhikari. Classification of disturbances and cyber-attacks in power systems using heterogeneous time-synchronized data. *IEEE Transactions on Industrial Informatics*, 11(3):650–662, 2015.

[126] Uttam Adhikari, Thomas Morris, and Shengyi Pan. Applying non-nested generalized exemplars classification for cyber-power event and intrusion detection. *IEEE Transactions on Smart Grid*, 9(5):3928–3941, 2016.

[127] Jingyu Wang and Dongyuan Shi. Learning from time-synchronized power system measurements with rare anomalous event records to detect PMU data manipulation attacks. In *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pages 1–6, 2017.

[128] Youbiao He, Gihan J Mendis, and Jin Wei. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. *IEEE Transactions on Smart Grid*, 8(5):2505–2516, 2017.

[129] Mete Ozay, Inaki Esnaola, Fatos Tunay Yarman Vural, Sanjeev R Kulkarni, and H Vincent Poor. Machine learning methods for attack detection in the smart grid. *IEEE Transactions on Neural Networks and Learning Systems*, 27(8):1773–1786, 2015.

[130] Kian Hamedani, Lingjia Liu, Rachad Atat, Jinsong Wu, and Yang Yi. Reservoir computing meets smart grids: Attack detection using delayed feedback networks. *IEEE Transactions on Industrial Informatics*, 14(2):734–743, 2017.

[131] David Wilson, Yufei Tang, Jun Yan, and Zhuo Lu. Deep learning-aided cyber-attack detection in power transmission systems. In *2018 IEEE Power & Energy Society General Meeting (PESGM)*, pages 1–5, 2018.

[132] Wang Jiao and Victor OK Li. Support vector machine detection of data framing attack in smart grid. In *2018 IEEE Conference on Communications and Network Security (CNS)*, pages 1–5, 2018.

[133] Jin Wei and Gihan J Mendis. A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids. In *2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*, pages 1–6, 2016.

[134] Xiayang Chen, Lei Zhang, Yi Liu, and Chaojing Tang. Ensemble learning methods for power system cyber-attack detection. In *2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, pages 613–616, 2018.

[135] Qian Chen, Hisham A Kholidy, Sherif Abdelwahed, and John Hamilton. Towards realizing a distributed event and intrusion detection system. In *International Conference on Future Network Systems and Security*, pages 70–83. Springer, 2017.

[136] I. Kamwa, S. R. Samantaray, and G. Joos. Compliance analysis of PMU algorithms and devices for wide-area stabilizing control of large power systems. *IEEE Transactions on Power Systems*, 28(2):1766–1778, May 2013.

[137] Don Johnson, Alfred Menezes, and Scott Vanstone. The elliptic curve digital signature algorithm (ecdsa). *International journal of information security*, 1(1):36–63, 2001.

[138] A. L. Buczak and E. Guven. A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys Tutorials*, 18(2):1153–1176, Secondquarter 2016.

[139] Burton H Bloom. Space/time trade-offs in hash coding with allowable errors. *Communications of the ACM*, 13(7):422–426, 1970.

[140] F. Simmross-Wattenberg, J. I. Asensio-Perez, P. Casaseca-de-la-Higuera, M. Martin-Fernandez, I. A. Dimitriadis, and C. Alberola-Lopez. Anomaly detection in network traffic based on statistical inference and α-stable modeling. *IEEE Transactions on Dependable and Secure Computing*, 8(4):494–509, July 2011.

[141] Yong Wang. Gauss–newton method. *Wiley Interdisciplinary Reviews: Computational Statistics*, 4(4):415–420, 2012.

[142] Masashi Sugiyama, Taiji Suzuki, and Takafumi Kanamori. *Density ratio estimation in machine learning*. Cambridge University Press, 2012.

[143] Daphne Koller and Nir Friedman. *Probabilistic graphical models: principles and techniques*. MIT press, 2009.

[144] Nitesh V Chawla, Kevin W Bowyer, Lawrence O Hall, and W Philip Kegelmeyer. Smote: synthetic minority over-sampling technique. *Journal of artificial intelligence research*, 16:321–357, 2002.

[145] Tianqi Chen and Carlos Guestrin. Xgboost: A scalable tree boosting system. In *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining*, pages 785–794. ACM, 2016.

[146] Ian Jolliffe. *Principal component analysis*. Springer, 2011.

[147] Xavier Hinaut and Peter F Dominey. On-line processing of grammatical structure using reservoir computing. In *International Conference on Artificial Neural Networks*, pages 596–603. Springer, 2012.

[148] Robert E Schapire. Explaining adaboost. In *Empirical inference*, pages 37–52. Springer, 2013.

[149] William W Cohen. Fast effective rule induction. In *Machine learning proceedings 1995*, pages 115–123. Elsevier, 1995.

[150] Charles Wheelus, Elias Bou-Harb, and Xingquan Zhu. Tackling class imbalance in cyber security datasets. In *2018 IEEE International Conference on Information Reuse and Integration (IRI)*, pages 229–232, 2018.

[151] Jin Wei and Gihan J Mendis. A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids. In *2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG)*, pages 1–6. IEEE, 2016.

[152] Christine Rosinger and Mathias Uslar. Smart grid security: IEC 62351 and other relevant standards. In *Standardization in Smart Grids*, pages 129–146. Springer, 2013.

[153] Mehmet Hazar Cintuglu, Osama A Mohammed, Kemal Akkaya, and A Selcuk Uluagac. A survey on smart grid cyber-physical system testbeds. *IEEE Communications Surveys & Tutorials*, 19(1):446–464, 2016.

[154] Y. He, J. Guo, and X. Zheng. From surveillance to digital twin: Challenges and recent advances of signal processing for industrial internet of things. *IEEE Signal Processing Magazine*, 35(5):120–129, Sep. 2018.

[155] D Van Que, JC Soumange, G Sybille, G Turmel, P Giroux, G Cloutier, and S Poulin. Hypersim–an integrated real-time simulator for power networks and control systems. In *Proc. Int. Conf. Digital Power System Simulators, Vasteras, Sweden*, 1999.

[156] Ali R. Al-Roomi. Power Flow Test Systems Repository, 2015.

[157] T Athay, R Podmore, and S Virmani. A practical method for the direct analysis of transient stability. *IEEE Transactions on Power Apparatus and Systems*, (2):573–584, 1979.

[158] OpenStack Foundation. Openstack: Open source software for creating private and public clouds.

[159] William Yuill, A Edwards, S Chowdhury, and SP Chowdhury. Optimal pmu placement: A comprehensive literature review. In *2011 IEEE Power and Energy Society General Meeting*, pages 1–8. IEEE, 2011.

[160] V Vijaya Rama Raju and SV Jayarama Kumar. An optimal pmu placement method for power system observability. In *2016 IEEE Power and Energy Conference at Illinois (PECI)*, pages 1–5. IEEE, 2016.

[161] Saikat Chakrabarti and Elias Kyriakides. Optimal placement of phasor measurement units for power system observability. *IEEE Transactions on power systems*, 23(3):1433–1440, 2008.

[162] Marco Martinelli, Enrico Tronci, Giovanni Dipoppa, and Claudio Balducelli. Electric power system anomaly detection using neural networks. In *International Conference on Knowledge-Based and Intelligent Information and Engineering Systems*, pages 1242–1248. Springer, 2004.

[163] David E Rumelhart, Geoffrey E Hinton, and Ronald J Williams. Learning representations by back-propagating errors. *nature*, 323(6088):533–536, 1986.

[164] Chris Dyer, Miguel Ballesteros, Wang Ling, Austin Matthews, and Noah A Smith. Transition-based dependency parsing with stack long short-term memory. *arXiv preprint arXiv:1505.08075*, 2015.

[165] Sepp Hochreiter and Jürgen Schmidhuber. Long short-term memory. *Neural Computation*, 9(8):1735–1780, 1997.

[166] Rui Fu, Zuo Zhang, and Li Li. Using lstm and gru neural network methods for traffic flow prediction. In *2016 31st Youth Academic Annual Conference of Chinese Association of Automation (YAC)*, pages 324–328. IEEE, 2016.

[167] Hwanjo Yu and Sungchul Kim. Svm tutorial-classification, regression and ranking. *Handbook of Natural computing*, 1:479–506, 2012.

[168] Angela Orebaugh, Gilbert Ramirez, and Jay Beale. *Wireshark & Ethereal network protocol analyzer toolkit*. Elsevier, 2006.

[169] Guido Van Rossum and Fred L Drake Jr. *Python tutorial*. Centrum voor Wiskunde en Informatica Amsterdam, The Netherlands, 1995.

[170] Clinton Gormley and Zachary Tong. *Elasticsearch: the definitive guide: a distributed real-time search and analytics engine*. " O'Reilly Media, Inc.", 2015.

[171] Yuvraj Gupta. *Kibana essentials*. Packt Publishing Ltd, 2015.